Preface

In early 2013 the IQC and ETSI thought that it was the right time to start to bring together the conventional cryptography community and the quantum cryptography community and to develop a vision for how these communities could jointly make an effort to create a quantum-safe cryptographic environment. http://www.etsi.org/news-events/past-events/648-crypto-workshop2013.

For many years now there has been a separation between the research community working on quantum cryptography and the one working on cryptography unrelated to quantum mechanical effects.

This had led to an effective labeling between the 2 communities, where the quantum cryptographers referred to their non-quantum colleagues as “classical cryptographers”, referring to cryptography based in a classical versus quantum physical paradigm, while for their non-quantum colleagues the term “classical cryptography” summarizes historical encryption techniques that have been broken and are no longer in use. The community working on non-quantum based cryptography intended to be secure in an era with quantum technologies adopted the name of “post-quantum-cryptography” for their work.

It was the aim of the workshop to find out how the diverse communities will need to co-operate in order to standardize and deploy the next-generation cryptographic infrastructure, in particular, one that will be secure against emerging quantum computing technologies.

Some short and medium term objectives towards the long-term goal of a quantum-safe cryptographic infrastructure were set out. This led to the decision to produce a White Paper on Quantum-Safe Cryptography and to hold a 2nd Workshop on Quantum-Safe Cryptography in Ottawa in 2013. It was hoped that this would encourage all stakeholders to start new standardization work within ETSI either creating new groups and/or expanding the role of existing groups. This work could include, for example, a standard for combining a battle-tested conventional key-establishment algorithm with a quantum-safe key establishment protocol, other study items or pre-standards, etc.

The targeted audience consisted of the key players and decision makers in deploying a global quantum-safe cryptographic infrastructure. This included implementers of conventional post-quantum cryptography (i.e. crypto algorithms resistant to quantum computers), QKD implementers, implementers of cryptography and security tools and systems (which will need quantum-safe cryptographic primitives), first industry and government adopters of quantum-safe tools, standardization bodies, and anyone else interested in moving now to be a part of creating the quantum-safe cryptographic infrastructure for the future.

These conference proceedings contain most of the papers presented during the workshop and poster sessions. Many presenters also took the opportunity to back up their claims with scientific papers, which are published right below their presentation.
ETSI Quantum-Safe Cryptography 2013 Program Committee

We had the great honor and pleasure of being joined by the following people on our Program Committee:

- Charles Brookson, Chairman of ETSI OCG SEC, Zeata Security,
- Johannes Buchmann, Prof. of Informatics and Mathematics at TU Darmstadt, Deputy Director of CASED,
- Matthew Campagna, Director of Certicom Research, BlackBerry,
- Donna Dodson, Deputy Chief Cybersecurity Advisor & Division Chief for Computer Security Division at NIST,
- Gaby Lenhart, Senior Research Officer at ETSI,
- Michele Mosca, Director, CryptoWorks21 and Deputy Director, Institute for Quantum Computing, University of Waterloo,
- Mark Pecen, Senior Vice President R&D at BlackBerry,
- Bart Preneel, Professor, COSIC, KU Leuven, Belgium,
- Carmine Rizzo, Security Expert at ETSI,
- Masahide Sasaki, Director Quantum ICT Laboratory at NICT,
- Andrew Shields, Chairman of ETSI QKD, Toshiba,

whom we would like to thank for accepting the difficult challenge of selecting the topics to be presented from a vast number of submissions. All these submissions were of very high quality therefore the only selection-criterion we were able to apply was their relevance for the given sub-topics from the call for presentations.

Editors:
Michele Mosca, University of Waterloo
Gaby Lenhart, ETSI
Mark Pecen, BlackBerry
SESSION 1: INTRODUCTION AND KEYNOTE
Session chair: Gaby Lenhart, ETSI

Welcome and Workshop Introduction
Luis Jorge Romero, ETSI Director-General

KEYNOTE: Quantum and Quantum-Safe-Crypto: the Perspective of the European Commission’s Joint Research Centre
Vladimir Sucha, Deputy Director General of the European Commission’s Joint Research Center

KEYNOTE: Research, development, and perspective of Tokyo QKD network
Kiyoshi Tamaki, NTT

KEYNOTE: Is there a market for Quantum safe technologies in Canada’s cyber strategy?
Alan Jones, retired Assistant Deputy Minister in the Canadian government

SESSION 2: SETTING THE SCENE
Session Chair: Michele Mosca, Institute for Quantum Computing, University of Waterloo

Extensible standards and impact on technology switching costs
Mark Pecen, Blackberry

Towards quantum-safe cryptography
Michele Mosca, Institute for Quantum Computing, University of Waterloo

Overview of post-quantum cryptography
Daniel J. Bernstein, University of Illinois at Chicago and Technische Universiteit Eindhoven

Overview of quantum key distribution technology and introduction to the work of the ETSI QKD ISG
Martin Ward, Toshiba

Security perspectives for quantum key distribution
Norbert Luetkenhaus, University of Waterloo

SESSION 3: INDUSTRY SESSION
Session Chair: Mark Pecen, RIM

Quantum Key Distribution in the Real World
Grégoire Ribordy, ID Quantique

Kerberos Revisited
Léon Pintsov, Pitney Bowes
A roadmap to migrating the Internet to quantum-safe cryptography  
William Whyte, Security Innovation

Advances in the security analysis of CVQKD  
Sébastien Kunz Jacques, SeQureNet

Questions and Answers Session  
Panel Discussion

SESSION 4: METROLOGY SESSION  
Session chair: Grégoire Ribordy, ID Quantique

Quantum Cryptography Platform for Test & Evaluation for EU-relevant Deployment Scenarios  
Pravir Chawdhry, Joint Research Centre

Metrology for QKD – an industrial quantum optical communication technology  
Christopher Chunnilall, National Physic laboratory

Hash-based signature  
Johannes Buchmann, TU Darmstadt

Quantifying security in a quantum key distribution system  
Marco Lucamarini, Toshiba Research Europe Ltd

Questions and Answers Session  
Panel Discussion

SESSION 5: DEPLOYMENT  
Session chair: Donna Dodson, NIST

Practical impacts of Quantum Computing  
Lily Chen, National Institute of Standards & Technology (NIST)

Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel  
Romain Alleaume, Telecom ParisTech and SeQureNet

Quantum Metropolitan Area Network based on Wavelength Division Multiplexing  
Vicente Martin, Universidad Politécnica de Madrid

Securing Fiber Optic Communication against Unlimited Adversaries  
Rei Safavi-Naini, University of Calgary

Isogeny-Based Cryptography on Mobile Devices  
Dieter Fishbein, University of Waterloo
Benchmarking of post-quantum cryptography
Tanja Lange, Technische Universiteit Eindhoven

Questions and Answers Session
Panel Discussion

SESSION 6: SECURITY ISSUES
Session chair: Johannes Buchmann, Technische Universität Darmstadt

Implementation loopholes in quantum cryptography Institute for Quantum Computing
Vadim Makarov, Institute for Quantum Computing, University of Waterloo

Evaluating the security of post-quantum cryptosystems
Yi-kai Liu, National Institute of Standards & Technology (NIST)
Jintai Ding, University of Waterloo

Questions and Answers Session
Panel Discussion

PANEL DISCUSSION & WRAP-UP
Michele Mosca, Institute for Quantum Computing, University of Waterloo
& all programme committee members
Welcome and Workshop Introduction

Luis Jorge Romero Saro, Director General of ETSI has over 20 years international experience in the telecommunications sector. Previously he has held diverse Director positions in Spain, Morocco and Mexico, predominantly with Telefonica. As Global Director for International Roaming and Standards, and Director of Innovation and Standards, he oversaw Telefonica’s participation in global standardization activities, and participated directly in the work of the Next Generation Mobile Networks (NGMN) Alliance and in the GSM Association (GSMA). Before joining ETSI in July 2011, he held the position of Director General of Innosoft and was also a partner and board member of Madrid-based Innology Ventures.

Quantum and Quantum-Safe-Crypto: the Perspective of the European Commission’s Joint Research Centre

Vladimir Šucha, Joint Research centre of the European Commission, has been appointed Deputy Director-General of the Joint Research Centre of the European Commission in July 2012. He had previously spent 6 years in the position of director for culture and media in the Directorate-General for Education and Culture of the European Commission. Before joining the European Commission, he held various positions in the area of European and international affairs. Between 2005 and 2006, he was Director of the Slovak Research and Development Agency, national body responsible for funding research. He was principal advisor for European affairs to the minister of education of the Slovak Republic (2004-2005). He worked at the Slovak Representation to the EU in Brussels as research, education and culture counselor (2000-2004). In parallel, he has followed a long-term academic and research career, being a full professor in Slovakia and visiting professor/scientist at different academic institutions in many countries.

Research, development, and perspective of Tokyo QKD network

Kiyoshi Tamaki, NTT corporation, obtained in 2004 his Ph.D degree under the supervision by Prof. Masato Koashi at Prof. Nobuyuki Imoto’s group in the Graduate University for Advanced Studies (SOKENDAI), Japan. After getting his Ph.D degree, he worked at the Perimeter Institute for Theoretical Physics in Canada, under the support of Dr. Daniel Gottesman, and then he worked as a postdoctoral fellow for Prof. Hoi-Kwong Lo’s group in the University of Toronto in Canada. From January 2006, he joined the Quantum Optical State Control group at NTT basic research laboratories in Japan. His main research interest is security of QKD

Is there a market for Quantum safe technologies in Canada’s cyber strategy?

Alan Jones served for almost 32 years with the Government of Canada with the Royal Canadian Mounted Police and for over 28 years with the Canadian Security Intelligence Service. Alan spent many years in intelligence operations working in the counter-terrorism, counter-espionage and counter-proliferation programs. Alan was the Assistant Director, Operations which included the investigation of cyber espionage threats against Canada. He retired in June 2013 as the Assistant Director, Technology. Alan was responsible for building a new technology directorate from all the IT, operational technology and data exploitation programs in CSIS. Additionally, he led the creation of the CSIS Cyber Centre as part of the Government of Canada’s development of a national Cyber strategy. Alan sat on the Canadian Security Telecommunications Advisory Committee which is responsible for the development of guidelines and best practices for cyber security for the Canadian telecommunications industry. Alan was a Senior Policy Advisor in the Privy Council Office, Security Intelligence Directorate. He is a past Chair of the G8 Counter-terrorism practitioners group. Alan is now a contributor to the IQC at the University of Waterloo on the practical application of quantum cryptology and is a contributor to Carleton University’s Critical Infrastructure Resiliency Program. Alan holds a Bachelor of Arts degree in Law from Carleton University in Ottawa.
Extensible standards and impact on technology switching costs

Mark PECEN, RIM, serves as Sr. Vice President, R&D for BlackBerry, and is responsible for RIM’s Advanced Technology Research Centre and broad-based R&D strategy, and also serves as an advisor to the RIM Innovation Council of the board of directors.

He established RIM’s Research Centre in 2005. The centre’s focus is wireless communication research, including all aspects from radio frequency hardware and antennas to core network technology and wireless-specific services. Topics include signal processing, information theory, cryptography, audio/video codecs, data compression, radio system protocols, mobility control, electromagnetics, advanced services and application platforms, prototyping of hardware and software and new technology trials.

He is an inventor of a number of technologies adopted by global standards bodies, including the Global System for Mobile Telecommunication (GSM), Universal Mobile Telecommunication System (UMTS), High-Speed Packet Access (HSPA+), 4th Generation Long-Term Evolution (LTE/LTE-Advanced) and others. A past Distinguished Innovator with Motorola, Pecen also managed consultation work for firms in North America and Europe.

Pecen serves as an advisor to the Canadian government on wireless communication and research. He holds board positions on 4G Americas, École Polytechnique, Wilfred Laurier University School of Business, Quantum Works academic network for quantum information research, Canadian Digital Media Network, the Communication Research Centre (CRC) of Industry Canada and others.

As a veteran of the wireless industry, he holds more than 100 fundamental patents in areas of mobile communication, networking and computing, and is a graduate of the University of Pennsylvania, Wharton School of Business and the School of Engineering and Applied Sciences.

Towards quantum-safe cryptography

Michele MOSCA, Institute for Quantum Computing at the University of Waterloo

Michele Mosca (DPhil, Oxford) is co-founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, and a founding member of the Perimeter Institute for Theoretical Physics. He is co-founder and director of the NSERC CREATE Training Program in Building a Workforce for the Cryptographic Infrastructure of the 21st Century (CryptoWorks21.com). His current research interests include quantum algorithms and complexity, and the development of cryptographic tools that will be safe against quantum technologies.

Awards and honours include the 2010 Canada’s Top 40 Under 40 award, Canada Research Chair in Quantum Computation (2002-2012), Fellow of the Canadian Institute for Advanced Research (2010-present), University Research Chair (2012-present), and Queen Elizabeth II Diamond Jubilee Medal (2013).

Overview of post-quantum cryptography

Daniel J. Bernstein, University of Illinois at Chicago and Technische Universiteit Eindhoven, is the designer of the “qmail” software used to receive mail by more than one million of the Internet’s SMTP servers (for example, yahoo.com); the “tinydns” software that publishes four million of the Internet’s level-2.com domain names (for example, facebook.com); and the “Curve25519” cryptographic algorithm that Apple uses to protect files stored on hundreds of millions of iPhones. Bernstein coined the phrase “post-quantum cryptography” in 2003, is coeditor of a survey book on the topic, and is coauthor of the recent “McBits” software for high-speed high-security post-quantum cryptography.
Speakers

**Overview of quantum key distribution technology and introduction to the work of the ETSI QKD ISG**

**Martin Ward**, Toshiba

Martin Ward (DPhil, Oxford) is a Senior Research Scientist at Toshiba Research Europe in Cambridge, UK. He works on applications of quantum information including quantum cryptography and semiconductor devices for creating quantum photonic states. He participates in the ETSI ISG on Quantum Key Distribution.

**Security perspectives for quantum key distribution**

**Norbert Lütkenhaus**, University of Waterloo

Norbert Lütkenhaus studied at the RWTH Aachen and the LMU Munich, from which he graduated with a thesis in general relativity. Then he changed the field to study quantum optics and quantum cryptography under the supervision of Stephen M. Barnett at the University of Strathclyde, Scotland, UK. In 1996 he obtained his PhD. After postdoc positions in Innsbruck (Peter Zoller and Ignacio Cirac) and the Helsinki Institute of Physics (Kalle-Antti Suominen) he worked for MagiQ Technologies (New York) to initiate the project of commercial realisation of quantum key distribution. Returning to academia in 2001, he build up and lead an Emmy-Noether Research Group at the University of Erlangen-Nürnberg, during which time he did his habilitation (2004). Currently he is an Associate Professor in the Physics Department at the University of Waterloo and a member of the Institute of Quantum Computing.
Speakers

Quantum Key Distribution in the Real World

Grégoire Ribordy, ID Quantique, Switzerland, has over 15 years of experience in various R&D and management roles in the field of photonics and quantum technologies. He co-founded ID Quantique in 2001 and has managed the company since then. Prior to this, he was a research fellow at the Group of Applied Physics of the University of Geneva from 1997-2001. In this position, he actively developed quantum cryptography technology. In 1995-1996, Mr. Ribordy worked for one year in the R&D division of Nikon Corp. in Tokyo. Mr. Ribordy is the recipient of several awards such as the 2001 New Entrepreneurs in Science and Technology prize, the 2002 de Vigier Award for Entrepreneurship and the Swiss Society for Optics and Microscopy 1999 prize.

Kerberos Revisited

Dr. Leon Pintsov, Pitney Bowes, is an internationally recognized expert in the fields of information security, computer imaging and postal technology and economics. He created several techniques and algorithms in the field of information security including development (together with S. Vanstone) of Pintsov-Vanstone Digital Signature Scheme with Message Recovery. Dr. Pintsov authored and co-authored a book on computer modeling of imaging devices and over 40 scientific publications. He is inventor and co-inventor of 125 International patents in 16 countries. He is a Senior Member of the Institute of Electrical and Electronics Engineers and a member of Connecticut Academy of Science and Engineering. Dr. Pintsov is an active member of international standardization committees including European Standardizations Centre (CEN) Technical Committee 331 and Universal Postal Union Standards Board. Dr. Pintsov is a founding member of the Scientific Advisory Board of the Center for Applied Cryptographic Research at the University of Waterloo (Canada), a member of the Scientific Advisory Board of ONETS Corp (China), a member of the Board of Directors of Connecticut Technology Council and MIT Enterprise Forum and IP Factory (USA). Dr. Pintsov is also a member of Advisory Board of Axiom Venture Partners and a member of International Editorial Board of the International Journal of Advanced Logistics. Dr. Pintsov holds a M.S. degree in Mathematics (Magna Cum Laude) from the University of St. Petersburg (Russia), Executive M.S. degree in Management Science from the Hartford Graduate Center of the Rensselaer Polytechnic Institute (USA) and Ph.D. degree in Applied Mathematics from the Institute of Telecommunication Engineering in St. Petersburg.

A roadmap to migrating the Internet to quantum-safe cryptography

Dr. William Whyte, Security Innovation, is responsible for the strategy and research behind the company’s activities in vehicular communications security and cryptographic research. Before joining Security Innovation, he was CTO for NTRU Cryptosystems, a leading provider of embedded security solutions and previously served as Senior Cryptographer with Baltimore Technologies in Dublin, Ireland. Dr. Whyte is chair of the IEEE 1363 Working Group for new standards in public key cryptography and has served as technical editor of two published IEEE standards, IEEE Std 1363.1-2008 and IEEE Std 1609.2-2006, as well as the ASC X9 standard X9.98. He led the implementation of 1609.2 for the USDoT-sponsored VII Proof of Concept project and is responsible for development of the NTRU Aerolink™ product. Dr. Whyte holds a D. Phil from Oxford University on Statistical Mechanics of Neural Networks and a B.A. from Trinity College, Dublin, Ireland. He has presented on cryptography and security at numerous industry and government events on four continents.

Advances in the security analysis of CVQKD

Sébastien Kunz-Jacques, SeQureNet, was graduated from the ENS Paris in 2001 and from Télécom ParisTech in 2003. He then worked for four years in the cryptology laboratory of the ANSSI, the French national agency for the evaluation of the security of IT products. In this position, he participated in several Common Criteria evaluations of products involving cryptographic mechanisms. He contributed to several research publications and obtained a PhD in cryptography from the ENS Paris crypto laboratory and the University of Paris VII in 2007.
Speakers

Quantum Cryptography Platform for Test & Evaluation for EU-relevant Deployment Scenarios

Pravir Chawdhry is a senior scientist at the Joint Research Centre (JRC) of the European Commission. He is Action Leader for the research group CORSA, focusing on the Protection of Communications, Radio-navigation and Space Assets. In support to the Galileo project under the EU Space Policy and the Radio Spectrum Policy Programme under the Digital Agenda, his group hosts state-of-the-art JRC laboratories for the security of global satellite navigation systems and reference measurement test-beds for radio spectrum and communications systems. These laboratories are geared to provide practical support to regulatory and standardization activities on RFID, wireless communications, software defined radio and broadband radio networks. Since 2011, Pravir has worked at the JRC on cybersecurity, online trust and privacy, border security, electronic passports and cross-border identity management as enablers of critical infrastructure protection.

Metrology for QKD – an industrial quantum optical communication technology

Christopher Chunnilall is a Senior Research Scientist at the National Physical Laboratory (NPL), the UK’s National Measurement Institute. He received his Ph.D. from King’s College London and has worked at NPL since 1995. His research interests include the metrology of, and using, single and entangled photons and photon counting detectors, and developing measurements to validate technologies based on the production, manipulation, and detection of single and entangled photons. He is a member of the ETSI ISG in Quantum Key Distribution.

Hash-based signature

Johannes Buchmann, Professor, Department of Computer Science and CASED, Technische Universität Darmstadt, Germany.
1982: PhD Mathematics
1985/86: Postdoc Ohio State University, supported by Fellowship of the Alexander von Humboldt Foundation
1988 - 1996: Professor of Computer Science Universität des Saarlandes, Germany
1993: Leibniz Prize Deutsche Forschungsgemeinschaft
1996 - present: Professor of Computer Science and Mathematics Technische Universität Darmstadt
2001 - 2007: Vice President Research Technische Universität Darmstadt
2008 - 2011: Director Center of Advanced Security Research Darmstadt CASED.
2011 - present: Vice-Director CASED
2011: Member of German Academy of Science Leopoldina

Quantifying security in a quantum key distribution system

Marco Lucamarini is Research Scientist at the Cambridge Research Laboratory, within Toshiba Research Europe Ltd, since 2012.
He obtained his degree and Ph.D. in Physics at the University of Rome “Sapienza” working, for the former, in the experimental group of Prof. De Martini and Prof. Mataloni, and for the latter, in the theoretical groups of Prof. De Pasquale and Prof. Tombesi.
His current interest is the security of practical systems for quantum key distribution.
He has almost 10 years of post-doctoral research experience in quantum systems coherence, quantum information and quantum cryptography.
Speakers

Practical impacts of Quantum Computing

**Lily Chen**, NIST

Lily (Lidong) Chen is a mathematician and the acting manager of Cryptographic Technology Group of Computer Security Division, National Institute of Standards and Technology (NIST). She received her Ph.D degree from Aarhus University, Denmark in Applied Mathematics. Her research areas include cryptographic protocols and their applications in communication security.

Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel

**Romain Alléaume** is Assistant Professor at Telecom ParisTech and founder of a start-up company, SeQureNet, where he works as scientific advisor. His research is centered on quantum optics and quantum information and in particular on quantum key distribution where he made several contributions in the past 10 years. After graduating from Ecole Normale Supérieure of Paris and completed his PhD at University Paris VI and ENS Cachan in 2004, on experimental quantum cryptography with single-photon sources, he was co-recipient, together with 5 co-workers, of “magazine La Recherche” scientific prize 2004. He then joined Telecom ParisTech to coordinate the work on QKD networks performed in the framework of the FP6 project SECOQC that culminated by the first demonstration of a QKD network in Europe. Romain Alléaume co-founded the start-up company SeQureNet in 2008, who has developped the first commercial continuous-variable QKD product, Cygnus, released in 2012. Romain Alléaume is currently coordinating several national and european projects, with emphasis on QKD practical security (Q-CERT) and on the optical integration of QKD in telecommunications networks (Quantum-WDM).

Quantum Metropolitan Area Network based on Wavelength Division Multiplexing

**Prof. Vicente Martín**, Assoc. Prof. of Computational Science, Ph. D. Physics U. Autónoma de Madrid on the numerical simulation of quantum systems. Founding member of the “Specialized Group in Quantum Information and Computing” of the Spanish Royal Society of Physics and of the Quantum Industry Specification Group at ETSI, where he has participated in several group specifications. His main interests are the classical post processing in quantum cryptography protocols and the integration of QKD in conventional networks. Currently leads the Research group on Quantum Information and Computation Group (GIICC) at the Technical University of Madrid (UPM) and the effort to build a QKD network prototype, that was funded by Telefónica Research and Development. He is also director of CeSViMa —Centro de Supercomputación y Visualización de Madrid— one of the largest supercomputing centres in Spain.

Securing Fiber Optic Communication against Unlimited Adversaries

**Rei Safavi-Naini**, AITF Strategic Chair in Information Security and Professor, Department of Computer Science, University of Calgary

Before joining University of Calgary in 2007, Dr. Rei Safavi-Naini was a Professor of Computer Science, and the Director of the Telecommunication and Information Technology Research Institute and the Centre for Information Security at the University of Wollongong in Australia. She has served on the program committee of major conferences in cryptography and information security including Crypto, Eurocrypt and Asiacrypt and has worked on numerous industry collaborative research projects. Currently, she is director of the iCORE Information Security Lab (ICIS). She holds a PhD in Electrical and Computer Engineering (coding theory) from University of Waterloo, and her current research interest include information theoretic security, provable security, network security, digital and privacy rights management, and multimedia security.
Speakers

Isogeny-Based Cryptography on Mobile Devices

Dieter Fishbein, University of Waterloo
Dieter is a graduate student pursuing a Masters of Mathematics in the Department of Combinatorics and Optimization at the University of Waterloo, under the supervision of David Jao. His research interests are in number theory and cryptography with an emphasis on the efficient implementation of cryptographic protocols. Dieter is originally from Toronto, Canada and holds a Bachelor of Science in mathematics from McGill University.

Benchmarking of post-quantum cryptography

Tanja Lange, Technische Universiteit Eindhoven
Prof. Dr. Lange received her PhD in mathematics from the University of Essen. In 2006 she joined Technische Universiteit Eindhoven as Full Professor. Prof. Dr. Lange has published more than 50 research papers bridging the gaps between algebraic geometry, theoretical cryptography, and real-world information protection. She is an expert on curve-based cryptography and post-quantum cryptography.

Prof. Dr. Lange is on the editorial board for 2 journals and serves on 3 steering committees, including the workshop series on Post-Quantum Cryptography. She has organized around 20 conferences and workshops, has served on more than 40 program committees. She is coordinator of the EU-FP7 project PUFFIN -- Physically unclonable functions found in standard PC components.
Implementation loopholes in quantum cryptography Institute for Quantum Computing

Dr. Vadim Makarov, Institute for Quantum Computing, University of Waterloo, is one of world leaders in the practical security of quantum key distribution (QKD) systems. He obtained his PhD in 2007 from the Norwegian University of Science and Technology in Trondheim; his work had uncovered several practical attack methods against QKD systems. Postdoctoral work in South Korea followed, and in 2008 he returned to Norway to establish and run a quantum hacking laboratory under supervision of Prof. Johannes Skaar. Dr. Makarov moved to Canada in 2012 to start his own research group with a focus on practical QKD security, and create an advanced laboratory for security analysis http://www.vad1.com/lab/

Dr. Makarov has led international collaborations culminating in successful hacks of both commercial QKD systems on the market. He has demonstrated a full field implementation of an eavesdropper stealing the complete ‘secret’ key from a research prototype QKD system. Dr. Makarov’s work includes responsible disclosure, for the first time providing QKD companies advance information on security weaknesses in their products. Security patches have been issued, and close cooperation developed with manufacturers.

Evaluating the security of post-quantum cryptosystems

Yi-Kai Liu, NIST

Yi-Kai Liu is a staff scientist at the National Institute of Standards and Technology (NIST). He works on quantum algorithms, computational complexity theory and machine learning. He is currently involved with NIST projects on post-quantum cryptography and secure random number generation. He has previously worked on a variety of topics, including quantum state tomography, compressed sensing, quantum chemistry and peer-to-peer networks.

Before moving to NIST in 2011, Liu was a postdoctoral researcher at Caltech and UC Berkeley. He holds a PhD in computer science from UC San Diego, and a BA in mathematics from Princeton University.

Multi-variate function based quantum-safe crypto

Multi-variate Public Key Cryptography

Jintai Ding is a professor at the Department of Mathematical Sciences of the University of Cincinnati. He received his B.A. from Xian Jiaotong University in 1988, his M.A. in mathematics from the University of Science and Technology of China in 1990 and his Ph.D in mathematics from Yale in 1995. He was a lecturer at the Research Institute for Mathematical Sciences of Kyoto University from 1995 to 1998. He has been a faculty member at the University of Cincinnati since 1998. From 2006 to 2007, he was a visiting professor and Alexander Von Humboldt Fellow at Technical University of Darmstadt. From 2009 to 2012, he was a Distinguished Adjunct Professor at South China University of Technology. Since 2011, he has been an adjunct Professor at Chongqing University. He received the Zhong Jia Qing Prize from by the Chinese Mathematical Society in 1990. He was a Taft fellow at Taft Research Center in 2009-2010. His main research interests are in cryptography, computational algebra and information security. He hold patents in cryptographic algorithms in China and USA.
Research, development, and perspective of Tokyo QKD network

Kiyoshi Tamaki, NTT
From the users’ viewpoint, QKD network is no longer point-to-point link!

Overview of current Tokyo QKD Network project

What can be improved in Tokyo QKD network?
⇒ (1) Stability of key generation (used to last only few days)
⇒ (2) Theoretical investigation of the systems

Current missions:
- More stable key generation
- Develop theory accommodating imperfections of the devices
- Start test service of QKD at NICT (2015)
- We aim for making actual use cases of QKD
Main achievement of QKD systems

- Loss: 1.3dB
- More than 90% of the transmission is guaranteed.
- Polarization fluctuations in time (25ns - 31ns, Avg)
- Night, Daytime, Night

- NEC
- NICT

NEC’s QKD system

- We have implemented passive BB84 with WDM up to 8 channels
  - 1.25GHz clock x 8 channels = 10GHz system in total
  - It features some stabilization techniques

- A. Imamura et al., ECOC2009, 1-4, p.3009
**Key distillation hardware engine**

**Requirements**

- 50Gbps random number input
  - 10GHz photon transmission \times 5 \text{ bit}
  - 5 \text{ bits}: Basis (1\text{ bit}), Data (1\text{ bit}), Decoy (2\text{ bit}), EC&PA (1\text{ bit})
- Large size matrix multiplication for EC & PA processes in real time
  - code length: 1M bit

- Real-time processing

  Processing time \leq 300\text{ ms} for each 1Mbit block

---

**Maintenance-free long-term field demonstration**

- Degradation of the APD's cooling system due to imperfect sealing
  - Past: we worry about the stability.
  - Now, it is time to

  - Seriously investigate the life time of each component device to construct a reliable QKD system (QKD system is much more mature than it used to be)

  - Video meeting: 800kbps

  - K. Yoshino, et. al., arXiv:1308.1011
What has to be done?

For easy installation and better performance:
- Develop a QKD system that is easy to install and to do maintenance
- More efficient post-processing (more efficient finite size effect)

Compatibility with existing optical communication networks:
- More research on WDM between quantum channels and standard communication channels. (CV-QKD: OK. DV-QKD: a bit more research is needed)

Security:
- More research on side-channels.

Countermeasure against side-channel attacks

Real time and precise monitoring of PM

Countermeasure against bright pulse illumination attack

If more than 2 detectors click, then we discard the block, reset the SPDs and restart (8000 photons are needed to blind a SSPD*)

*F. Fujikura, et. al. Optics Express, 21, 5, pp. 6304 (2013)
Presentations

SESSION 1
INTRODUCTION AND KEYNOTESS

Phase encoding scheme for MDIQKD


Eve

Encoding: phase non-randomized BB84 state
\[ \{ |\alpha\rangle, -|\alpha\rangle, |\alpha\rangle, -|\alpha\rangle \} \]


\( M = 3111.3413 \)

- Completely free from detector-side-channels
- Essentially, no need of single-mode assumption
- Robust against PM fluctuations

Aiming for finding actual use cases of QKD

1. First of all, manage to meet potential users and talk with them.

2. How to attract them?
   - Present as many applications of QKD as possible, such as smart phone, internet-compatible applications, etc.
   - Cleaner explanation of QKD is needed
     - What kind of functionality QKD can provide? What’s the advantage of QKD over modern crypt and a trusted courier? -> Forward secrecy, ability to provide fresh keys anytime, etc.
     - What’s the disadvantage? -> Basically point to point, short distance, low key rate, high cost of renting an optical fiber etc.

3. Potential users worry about how to install QKD to their network and what kind of flaw QKD could possibly bring them
   - Compatibility with their network and easy installation

Implementing QKD correctly only increases the security of the network

\=> QKD only gives bonus to them
The security certificate of not only QKD layer, but also of whole QKD network is needed.

Such a certificate is very useful for willing users when they convince their bosses or budget authorities.

If it is possible, submit such documents to some crypto organizations.

We have to be well-prepared as much as possible in order to grasp the future big chance!
Good Morning

Thank you for the exceptional privilege of speaking to you today. My name is Alan Jones and my background is not as a physicist nor an engineer my experience has been as an intelligence professional; I retired this past May after almost 32 years with the Government of Canada, the past 28 years with the Canadian Security Intelligence Service. My last position was as the Assistant Director for Technology, prior to that I was the Assistant Director of Operations and spent most of my career investigating terrorist and spies in Canada and abroad. I started as a field officer and ended up as an executive leader. The difference being I moved from a world of individual investigations to being responsible for the strategies to solve problems on a large scale, at program levels.

The world changed a lot during my career and the term cyber went from science fiction to our everyday lexicon to describe the entanglement of our lives with computers and the internet. With those changes the threat environment developed another domain. Cyber space. In turn we need to develop new approaches to security in a domain that has a technical foundation largely incomprehensible to most of its users. Canada’s Cyber strategy, launched in 2010 focused on three pillars: securing Canadian Government Systems; securing vital systems outside Government and securing Canadians on-line. These areas are common themes in the cyber strategies of the EU and all of these areas are potential markets for Quantum based products particularly encryption.

Some might suggest that quantum encryption is a solution in search of a problem. Let’s talk about the IT security environment for a bit.

For many years, computer vendors and internet providers traditionally looked at security problems as user centric; You have a problem, you haven’t protected your computer, Todays reality is much different. We have a problem and telecommunications companies and enterprises - I include governments in this category - are having to shoulder an enormous amount of responsibility for the security of client user hardware and applications and user data. This is the result of the reality of large scale cyber attacks which can put entire networks at risk by using individual computers to propagate viruses or do tremendous damage to some end point system that controls a manufacturing process or the operations of critical infrastructure. These attacks are often at a scale and level of technical sophistication beyond what the average user could ever understand let alone control.

Enterprises have the authority and the need to exercise IT security management over all devices in the enterprise network - because they own the network and the devices and users sign on to terms and condition of use - which are enforced through system monitoring. At least that’s the theory. There are a few things working against enterprises:

Networks are designed to be as accessible as possible for users to do their work and share information. The world wide web is designed to be as open as possible and is very convenient and also cost effective for companies to connect employees around the world or to connect machines and devices – the internet of things. The www is also a virtually unguarded swamp of dangerous creatures. Viruses, hackers, hack-tivists, malicious individuals, vindictive employees, angry customers, industrial spies, state spies, terrorists, criminals of all kinds or simple cascading technical failure caused by a malfunction somewhere in the system.

The value proposition to use the www as the backbone of a corporate communication system, despite the risks, is usually overwhelmingly in favour of the www. That value proposition has extended to SCADA industrial controls that a everything from farms to food production to hydro-electric dams to the electricity grid to oil and gas production and distribution. The internet of things will access, manage or control devices ranging from insulin injectors carried by diabetics to your automobile or your refrigerator.

When we talk about data at rest public or private data centers hold many different types of data that should be protected and sometimes by law must be protected such as employee personal data, customer data, third party data
or national secrets. Companies also hold intellectual property, sensitive contract and financial data, sensitive legal data and often have significant potential liability if there is an unauthorized disclosure of data. Liability will also extend to SCADA or other industrial control systems which if fail will cause damage to the environment, the food chain, to public safety, to economic stability or the commercial viability of a client’s manufacturing process. These failures may happen through equipment malfunction, human error or as the result of a malicious act.

Modern workplaces involve work from home, mobile workers and pressures for employers to accommodate BYOD. All of these trends pose great challenges to have an enabled and nimble workforce but to do so securely and to do so affordably. Office tools are not viewed as profit centers - but neither are locks on doors...

The Public sector has very similar workforce issues: government departments are under pressure to provide service to both their employees and the public via e-services as the lowest cost to the taxpayer. Only agencies that operate at the Top Secret level: intelligence agencies, parts of defence organizations, perhaps parts of national police agencies and central government agencies with national security responsibilities can justify the cost of external proprietary networks and what in the trade is known as Type 1 crypto. These networks are very expensive to operate; the rule of thumb is minimum 1.5 times the cost of an unsecure network not including external leased lines or satellite communications. These networks also have many restrictions on users which often slows down work processes: add to this the additional cost of TS security clearances which can easily exceed $25,000 per person and also records management system with appropriate security features, and lets not forget the cost of archiving all that material for decades to meet access to information and other legal regimes. All of which must be done securely and may need to be retrieved remotely.

Governments are also expected to lead national cyber security strategies and to co-ordinate cyber security strategies nationally and with other nations; governments are expected to maintain appropriate legal frameworks to govern activity on the www within their borders or involving their citizens and for the protection of data - public or private. There is much discussion about the extent of liability for governments for the security of information travelling in or through its borders. Law and case law are still in the early days of development on these issues. 90% of telecommunications structure in Canada, like most countries, is owned and managed by the private sector but are the consequences of a disaster attributed to a cyber attack solely the responsibility of the private sector or is it shared by government? What if the threat came from an insider versus a foreign entity? What are the limits of active network defence for a private entity? How much does it matter if the attacker is a non-state actor versus a state-actor? What’s the default response in active defense if the defender is unable to attribute the origin of the attack? How are those limits affected by the fact that regardless of the attribution of the attack it is being carried out over private telecommunications networks that are supporting millions of other, innocent users who could become collateral damage in a cyber battle?

E-service providers such as financial institutions and governments as well as e-commerce providers have an enormous vested interest in the future health and viability the internet. Internet use is exponential in every sector, there is increasing dependency on it, internet capacity is increasing but telcos can hardly keep up to bandwidth demands and there are also increasing pressures in terms of security threats, legislation and regulation about data sharing and increasingly blurred lines between enterprise and personal devices.

Cloud services provided over the ‘net will continue to increase as will the complexity of governance around data stored in the cloud – how will privacy requirements be met? How do data owners ensure the confidentiality of their data if it is stored elsewhere? If a data owner decides to change cloud service providers what happens to their data? Is it completely retrievable and can it completely deleted? How can you be sure that all that you have stored is transferred to the new cloud service provider?

These are all areas where practical and reliable encryption can provide solutions to many of these challenges. Not just for the protection of state secrets but for many types of stored data or the protection of command an control mechanisms in SCADA systems.

Telecommunications providers, on-line service providers, software application vendors, computer vendors all are putting increasing effort into making their products more secure. It makes good business sense to do so, it makes good sense to try to keep the world wide web viable as a good value proposition for individuals and enterprises but the security
Challenge is daunting and requires many layers of security extending from individual users to telecommunications providers to enterprise network operators.

Regulatory bodies, standards writers, industry monitors and enforcement bodies all face significant challenges: Government imposed regulations are often viewed as market inhibitors or as leverage by large players over smaller ones. ITS monitoring systems that are real time to enable rapid response and with logs that are useful to enforcement bodies are not universal. There remains reluctance, often understandably for companies to report the extent of damage done in order to protect market share, share price and client interests. All enterprises are now having to perform a calculus around the threat risk profile of their information and their networks. The loss of low value information that is widely communicated over public networks with minimal security might be quite acceptable in a certain business model – on-line pizza delivery: The higher the value of the information the greater the security measures must be taken to protect it. If the pizza company is big enough maybe the details of its cash flow or corporate structure is a little more sensitive. If that pizza company is one of many diverse holdings in a larger multinational corporation the loss or unauthorized disclosure of the financial details of the holding company could effect many other companies in many countries.

It is as of yet, unclear as to how to articulate the value proposition of quantum encryption in the security architecture of an enterprise.

We also need to think about lawful access legislation. Most states will insist that any data or communication within its borders must be accessible under lawful order. Whether it’s a search warrant or some other mechanism. How will quantum based security providers accommodate lawful access? Can current approaches to lawful access be used for quantum encryption that has such unique anti-interception properties?

And have we thought about how we respond to our adversaries being equally equipped with quantum encryption or quantum based offensive tools? Counter quantum methodologies will become a requirement if we are faced with these challenges.

Outside of IT departments and Signal Intelligence programs few Executives, Government or private sector, particularly Chief Financial Officers, have very little interest in the actual internal workings of any machine helps them solve problems in a timely manner and does so at an affordable price. Any machine becomes more corporately popular if it helps save money or better yet increase profits. A liability for any organization is the cost of security and the higher the security the higher the cost. Technical complexity often equates to costly overhead and costly maintenance. If for example key management can be streamlined through reliable quantum technology resulting in fewer system devices and less human engagement both the costs and the number of potential points of failure will be reduced.

Quantum based security products have tremendous potential to meet an increasing market demand for better cyber security for data in motion and data at rest in both the public and private sectors – both sectors have increasing global networks and work forces that want and often need to be mobile. Quantum may also have the potential to be more economical than some traditional systems especially if it is able to streamline the current cryptologic infrastructure and physical security overhead, with all the related restrictions. If quantum based technology can potentially enable not just more secure but more efficient business activities it will be compellingly attractive to a wide variety of public and private sector consumers, especially those with national security, critical infrastructure, economic and privacy compliance responsibilities high security Government agencies would find such a possibility compelling.

But quantum technology must support and enable business process not the other way around. It must be affordable, scalable, data agnostic, it must have practical maintenance requirements, it must be robust and reliable. It must also be describable in ways that Boards of Directors can understand the value proposition as they make decisions around enterprise IT security.

Thank you for the opportunity to speak with you this morning, You are part of a fascinating new field of research that may improve parts of our world in the near future. Best of luck in your workshop.
There is a catastrophe looming for our information and communication infrastructure. Solutions to avert this catastrophe exist, but serious work needs to be done, starting immediately, to develop, deploy and standardize the solutions.

Mark Pecen nicely described in his presentation one of the unfortunate challenges – the problem of switching costs, which we often face when we want to replace one solution with a better one – and he outlined ways to mitigate this problem.

Let me outline the problem that needs a solution.

To appreciate the depth of the problem, we need to understand how profoundly our current ICT infrastructure, which is central to stability of the global economy, depends on cryptography. We necessarily start with some trust assumptions, and some physical security (at least at the end-points, for some period of time). Cryptography is what lets us leverage a relatively small amount of trust and physical security to take advantage of an untrusted ICT infrastructure. Without cryptography, we essentially need to “unplug” from the ICT infrastructure, and stop using untrusted parties and media. This is simply not practical for the majority of applications, including anything involving a financial transaction that uses real-time communication (credit card purchases, money transfers, online banking, etc), online communication (e-mail, texting, social media, etc), online advertising, e-health, and so on.

So reliable cryptography is fundamental to the global economy and our daily lives.

It is worth noting that cryptography is generally regarded as one of the strongest parts in the “chain” of tools that provide information security. The weak links we see today in cybersecurity are typically related to the other pieces of the chain. These urgent cyber-security challenges naturally distract from the need to act today to prevent a cyber catastrophe in the future if the cryptography link in the chain of tools is broken. This is another of the challenges to solving this problem.

The problem we discussed at this workshop is a well-defined catastrophe on the horizon for some critical parts of the cryptography infrastructure.

Peter Shor discovered in 1994 that quantum computers will break factoring and discrete-logarithm-based cryptosystems. Fortunately, we didn’t have quantum computers at the time. But 20 years later, the picture is becoming clearer. I’ll return to this shortly.

Of course, this quantum computing risk is on top of the daily risk we already face – that of an unexpected algorithmic advance. For example, it was once believed that discrete logarithms in GF(2^{127}) were intractable, and the method was even being implemented in hardware until my colleagues at Waterloo found a way to solve instances of this size. Coppersmith found a way to build on this work and take the exponent in the complexity of solving such discrete logarithms from $O(n^{1/2})$ to $O(n^{1/3})$, which was a major milestone that led to other
important advances in crytanalysis. More recently, our colleagues in France found another major weakness for discrete logarithms in fields with low characteristic. With regard to the specific threat of a quantum computer, one must ask: is this really something we need to worry about now?

Roughly speaking, this depends on three variables, X, Y and Z:

- X is the number of years you need your public-key cryptography to remain unbroken. For example, how long is it necessary to protect health information, or national security information, or trade secrets?
- Y is the number of years it will take to replace the current system with one that is quantum-safe.
- Z is the number of years it will take the break the current tools, using quantum computers or other means.

If X+Y>Z, then we have a problem now, and immediate action needs to be taken. This means that for the latter part of those Y years, we have to either stop doing business or continue using the tools we know will be broken in Z years. Either way, these will not be pleasant times for doing business.

So what is Z? We don’t know, but we can say something more useful.

Firstly, let me emphasize that the size of the number factored to date by quantum means is an essentially irrelevant metric. What we should ask is how close we are to meeting a meaningful fault-tolerance threshold. We do know that a scalable quantum computer is feasible (given reasonable error models and architectures) thanks to fault-tolerant quantum error correcting codes. If experimentalists can perform a handful of fundamental physical operations with precision better than a fault-tolerance threshold $\epsilon$, then they can perform large-scale quantum computations with efficient scaling. In the past 10 years, great advances have been made on all three of these fronts. The error models are more realistic and better understood. The architectures are more realistic and basic components are being implemented. And we have much more powerful families of fault-tolerant codes. The threshold $\epsilon$ has risen from $10^{-6}$ to roughly 1%. The experiments are starting to approach the threshold.

IBM states [1]: “We are still a long way from building a practical quantum computer, but the path toward this goal is becoming clearer. Rapid improvements in experimental quantum hardware suggest that a threshold for the design and construction of fault-tolerant systems may be reached in the next five years. At that point, the goal of building a useful and reliable quantum computer will be within our reach.” Note this was written in 2011.

Our colleagues at Yale [2] wrote a nice review in 2013 tracking relevant metrics, which seem to support the predictions made by IBM. For example, they show that qubit life-times have increased exponentially over the past 14 years. They nicely describe seven stages to building a fault-tolerant quantum computer, and point out that in the past 14 years, superconducting qubits have achieved the first three stages and are moving towards the fourth.

The bottom line is that progress toward building a quantum computer is measured in orders
of magnitude, and has been truly impressive over the past two decades, and will likely continue accelerating in pace. I personally would say the likelihood of a large quantum computer in the next 20 years is an order of magnitude higher than it was 10 years ago, and cannot be ignored.

Now on to the question of Y: the time required to transition from our current infrastructure to quantum-safe tools.

Cryptographers have been thinking of alternatives for many years; some of these proposed solutions are almost as old as public-key cryptography, others are much newer. Quantum algorithms experts are starting to look at these systems more and more, though still not enough. Standards organizations, including ETSI, NIST and NICT, have been looking at this space for many years. But I think it’s fair to say it would not be easy in the near future to change from the current cryptography algorithms to quantum-safe ones. The standards and practices are not ready.

Looking at past examples, we can ask how long it took for RSA to go from discovery to large-scale deployment. Or Elliptic Curve Cryptography (ECC)? Roughly 20 years.

What about the recent BEAST attacks? The vulnerability was known for nearly a decade, and a fix was available about five years prior to the attacks, but not widely deployed (and still not fully deployed).

The short answer is “a long time” — roughly a decade or two. The bottom line is that the “wait and see” approach is too risky. It’s optimistic to think we can wait until a point when people will know large quantum computers will be here in less than 20 years, and guarantee not less than, say, 15 years. Will anyone really be able to predict with this relative precision? Will organizations building quantum computers necessarily tell us when they are close?

Even 15 years doesn’t give us much time, given the broad range of work that needs to be done, including battle-testing these systems in the field for a number of years before people would really trust them. Not to mention that sometimes X>0.

We need alternatives, even just to protect against unexpected (classical) algorithmic advances, even modest ones. And these alternatives should also be quantum-safe in order to protect against the well-defined and emerging quantum threat.

We also need the infrastructure to have greater algorithmic agility, especially if it will contain computationally secure tools.

Fortunately, we have several solutions. There are two families of complementary solutions. The first class of solutions are often called “post-quantum,” though some use the term to encompass practical quantum cryptography as well. Here I refer to classical, mathematics-based codes deployable on the existing infrastructure, which are believed to be secure against quantum attacks. The key advantage of these solutions is that they don’t require new physical infrastructure. The downside is that we are still dealing with computational security, with the occasional unexpected advances that we may or may not learn about until it’s too late to avert a problem.

The other set of tools are quantum tools, requiring some amount of quantum technology. In general, however, this is available technology, such as fibre, free-space and single-photon
sources and detectors. The performance parameters (distance, rate, etc.) are an issue for many applications, but they will continue to improve. That’s the downside. The main upside is that for quantum key establishment we don’t have computational assumptions, such as assuming that factoring large integers is infeasible.

These two sets of tools are not mutually exclusive; in fact, they complement each other and work very well in combination to fill the spectrum of security needs.

Let me highlight two of the most important cryptographic primitives: signatures and key-establishment.

In an era with quantum computers, the quantum-safe alternatives for authentication or signatures include:

• Trapdoor-based public-key signatures
• Hash-based signatures, which have the advantage of not requiring a trapdoor
• Symmetric key authentication (if we are ready to leave the public-key setting in some circumstances).

Quantum-safe alternatives for key-establishment include:

• Key establishment via public-key encryption, which requires trapdoors
• Quantum key establishment.

We had several talks on both families of approaches throughout the first ETSI workshop on quantum-safe cryptography.

As I mentioned, the quantum and classical solutions can work very well together, achieving some things that they individually cannot. For example, one can use hash-based signatures to authenticate quantum key establishment, and thereby get long-term security not achievable using just public-key key establishment by only assuming the short-term security of a hash-function.

During the workshop we heard a number of presentations and had discussions that will help us answer the following questions:

• How ready are these potentially quantum-safe systems for widespread deployment?
• What gaps remain?
• What are the pitfalls we should avoid? For example, do we face the risk of standardizing too little or too late, or too much or too soon?
• Can we agree on some kind of roadmap, and identify meaningful next steps? If so, who will spearhead this effort?

This workshop was only a first step. We look forward to identifying the next steps and working on their implementation together.

References:


Extensible standards and impact on technology switching costs
Mark Pecen, BlackBerry
Presentations

SESSION 2
SETTING THE SCENE

Why Standardize?
We can learn from our experience in ETSI wireless

Equipment Interoperability
- The first mobile radio systems were proprietary (e.g. an Ericsson radio only talked to another Ericsson radio and only in areas having infrastructure)
- Single-source supplier has large monopoly power
- Proprietary technology tends to create smaller and more tightly segmented markets

Economies of Scale
- Standard technology enables large scale adoption, which fuels the learning curve
**Presentations**

**SESSION 2**

**SETTING THE SCENE**

---

**Economies of scope**
- Re-use of platform for multiple products – no need for special country-specific technologies

**Large-scale adoption potential**
- For example, 3GPP wireless technologies (GSM/GPRS/EDGE/UMTS) have 87% of global subscriber market share

---

**A wireless example: 3GPP technologies**

![Map showing wireless coverage](image_url)

**Legend**
- Live GSM
- Planned GSM
- No GSM

[Source: 4G Americas, 2012]
Standardization can create huge markets

- Positive network externalities can be created
  - The more a certain technology is in use, the greater further adoption potential
- Reasonable trade-offs possible
  - Give up certain proprietary advantages in exchange for the creation of large global markets

A double-edged sword

- Future innovation can be severely constrained
- Innovation produces Ricardian economic rents
- You may lose some competency-based rents as the price you pay for creation of large markets
- The large installed base of customers then becomes a constraint in itself
What does this mean for cryptography?

Impact of standardization on adoption of cryptographic solutions

Cryptographic solutions are highly dependent on network externalities (i.e. the ability for others to use the same solution)
Must be a mechanism for key exchange, an authority to authenticate identities, etc.
A proprietary cryptographic solution may be appropriate in some cases, but is likely to occupy a small and specialized market segment where scaling isn’t a problem. Such proprietary techniques generally have difficulty in scaling in deployment size, across national borders, etc.
Presentations

SESSION 2
SETTING THE SCENE

- Standardized cryptographic solutions anticipate market scale, scope and deployment scenarios.
- Standards tend to be defined that are simple to implement and deploy – the details of which are designed to mean the same thing to system designers in Beijing as they do to those in Paris.

Consider technology switching costs – Why so much legacy infrastructure still exists
### Setting the Scene

**More Practical View…**

- **Realistic switching cost:** Economically infeasible to switch to new technology

**Incremental cost**

<table>
<thead>
<tr>
<th>Old system</th>
<th>New system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Switching Costs</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Electric Power Generation in the United States**

- General Direct Current (DC) electric power distribution has been outdated in the United States since 1903.
- Nevertheless, the last Consolidated Edison DC power generation and distribution center in the state of New York was turned off in 2007 – customers still using DC were supplied with AC to DC rectifier units to ease switching costs.
Meanwhile in wireless...

- Over 5 billion GSM subscribers
- Estimated that there are more than 2.8 million GSM base stations deployed worldwide
- 4th Generation Long-Term Evolution Advanced (LTE-A) is the latest, most spectrally efficient and fastest cellular wireless technology available for mass deployment today – but it's hard to suddenly disconnect millions of base stations, and to give up the roaming revenue they provide, even if they cost much more to operate than LTE base stations.
- Fortunately, there are extensibility features in the ETSI 3GPP standard that ease some of these migration aspects.

Extensible Standards – Start from the beginning
Extensible Standards

- Anticipate migration from one technology to future technology
- Ease or eliminate technology switching costs
- Relatively simple, if considered up-front

Extensible Crypto Standards

- Architecture, message structure to handle multiple crypto standards
- Not difficult, if defined early in standardization cycle

Common Message Stream
Simple to add extensibility up front...

- Difficult to impossible to implement after deployment...
- Appropriate stream processed by appropriate processor - user can upgrade or change versions without switching cost consequences

Way forward?

I would urge my industry colleagues to consider the creation of an ETSI Technical Report (TR) to be drafted over the next year to consider, e.g. what might an extensible QKD architecture look like?
Towards quantum-safe cryptography
Michele Mosca, Institute for Quantum Computing, University of Waterloo
Presentations

SESSION 2
SETTING THE SCENE

Cryptography is a foundational pillar of the global information security infrastructure.

Cryptography allows us to achieve information security in the “cloud”.

Information is handled by untrusted parties through untrusted media.

e.g. Do you update your software and anti-virus daily? Why do you trust the source?

One serious problem for public-key cryptography


Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 236-A/99
600 Mountain Ave.
Murray Hill, NJ 07974, USA
...on top of ever-present risk of unexpected advances in classical algorithms

e.g.

A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic

Improvements over FFS in small to medium characteristic

Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé

Cryptology ePrint Archive: Report 2013/400
Date: received 18 Jun 2013

CryptWorks21

How much of a problem is quantum computing, really??

CryptWorks21
SESSION 2
SETTING THE SCENE

How soon do we need to worry?

Depends on:
- How long do you need encryption to be secure? (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (z years)

Theorem 1: If \( x + y > z \), then worry.

What do we do here??

```
+--------+-----+
|        |     |
|        |     |
+--------+-----+
     y     x
     z
```

“Threshold theorem”

Architecture description

Threshold “ε”
If the error rates of the basic operations of the device are below ε, then we can efficiently scale quantum computations.
Quantum computing: An IBM perspective

Quantum physics provides an intriguing basis for achieving computational power to address certain categories of mathematical problems that are completely intractable with machine computation as we know it today. We present a brief overview of the current theoretical and experimental works in the emerging field of quantum computing. The implementation of a functioning quantum computer poses tremendous scientific and technological challenges, but current rates of progress suggest that these challenges will be substantially addressed over the next ten years. We provide a sketch of a quantum computing system based on superconducting circuits, which are the current focus of our research. A realistic vision emerges concerning the form of a future scalable fault-tolerant quantum computer.

Conclusion

While we still have a long way to go and many details to work out, we can see the broad form of tomorrow’s quantum computers. The marked progress in the theory of QEC has relaxed the device error rate that must be achieved for fault-tolerant computing. Rapid improvements in experimental quantum hardware suggest that a threshold for the design and the construction of fault-tolerant systems may be reached in the next five years. At that point, the goal of building a useful and reliable quantum computer will be within our reach.
Recent progress in superconducting qubits

**Superconducting Circuits for Quantum Information: An Outlook**

<table>
<thead>
<tr>
<th>Requirement for scalability</th>
<th>Desired capability margins</th>
<th>Estimated current capability</th>
<th>Demonstrated successful performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIQ operation</td>
<td>$10^5$ to $10^6$</td>
<td>50</td>
<td>Fidelity $\geq 0.995$ (27)</td>
</tr>
<tr>
<td>Rabi flop</td>
<td>$10^5$ to $10^6$</td>
<td>1000</td>
<td>Fidelity $\geq 0.99$ (67, 70)</td>
</tr>
<tr>
<td>Swap to bus</td>
<td>$10^5$ to $10^6$</td>
<td>100</td>
<td>Fidelity $\geq 0.98$ (72)</td>
</tr>
<tr>
<td>Readout qubit</td>
<td>$10^5$ to $10^6$</td>
<td>1000</td>
<td>Fidelity $\geq 0.98$ (51)</td>
</tr>
<tr>
<td>System Hamiltonian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stability</td>
<td>$10^5$ to $10^6$</td>
<td>7</td>
<td>4-day in 1 day $= 2 \times 10^{-7}$ (43)</td>
</tr>
<tr>
<td>Accuracy</td>
<td>$10^5$ to $10^6$</td>
<td>10 to 100</td>
<td>1 to 10% (43)</td>
</tr>
<tr>
<td>Yield</td>
<td>$&gt;10^5$</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Complexity</td>
<td>$10^5$ to $10^6$</td>
<td>10?</td>
<td>1 to 10 qubits (63)</td>
</tr>
</tbody>
</table>

**Graph:**

- **$T_1$, $T_2$, $T_{\text{peak}}$**
- **cQED**, **Fluxonium**, **Improved 3D transmon**
- **Quantronium**, **3D cavities**, **3D transmon**
- **CPB**, **Charge echo**

**Legend:**
- **Qubit lifetime (ms)**
- **Operations per error**

**Year:**
How long to re-tool the cryptographic infrastructure?

Cryptographers are studying possible quantum-safe codes. Quantum information experts are researching the power of quantum algorithms, and their impact on computationally secure cryptography. How easy is it to change from one cryptographic algorithm to a quantum-secure one? Are the standards and practices ready?
Past examples… quiz

How many years for
- RSA to go from discovery to ubiquitous deployment?
- ECC from discovery to ubiquitous deployment?
- BEAST attack to roll out of TLS 1.1?

Bottom line

“Wait and see” approach is too risky.
The next generation cryptographic infrastructure:
- Must have quantum-safe alternatives
- Should have algorithmic agility built-in
The solutions

Quantum-safe cryptographic infrastructure

“post-quantum” cryptography + quantum cryptography
- classical codes deployable without quantum technologies
- believed/hoped to be secure against quantum computer attacks of the future
- quantum codes requiring some quantum technologies (typically less than a large-scale quantum computer)
- typically no computational assumptions and thus known to be secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem
Overview of options

Quantum-safe authentication
- Trap-door predicate based public-key signatures
- Hash-function based public-key signatures
- Symmetric-key authentication

Quantum-safe key establishment
- "Alternative" public-key-encryption based key establishment
  - Lattices
  - Codes
  - Multi-variate functions
  - Other
- Quantum key establishment

Important questions

How ready are these systems for wide-scale deployment?
What gaps remain for the various approaches?
What are the pitfalls to avoid?
What are the next steps with respect to standardization and certification?
Overview of post-quantum cryptography
Daniel J. Bernstein, University of Illinois at Chicago and Technische Universiteit Eindhoven

Cryptography = “secret writing”. Achieve various security goals by secretly transforming messages. Major theme of research: Users have cost constraints. Can be challenging to reach acceptable security levels.

Secret-key cryptography
Prerequisite: Alice and Bob share a short secret key $k$ not known to eavesdropper Eve.
Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob, despite Eve’s espionage—forgery.

$k \rightarrow k$
$m \rightarrow c \rightarrow c' \rightarrow m \text{ if } c' = c$

Alice \quad Eve \quad Bob
Presentations

SESSION 2
SETTING THE SCENE

Secret-key cryptography
Prerequisite: Alice and Bob share a short secret key $k$ not known to eavesdropper Eve.

Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob, despite Eve’s espionage+forgery.

Public-key signatures
Prerequisite: Alice has a short secret key corresponding public key $A$.
Everyone knows $A$.
Eve does not know $a$.

Security goal: Integrity for any number of messages published by Alice.
Secret-key cryptography
Prerequisite: Alice and Bob share a short secret key $k$ not known to eavesdropper Eve.
Security goals: Confidentiality and integrity for any number of messages exchanged by Alice and Bob, despite Eve’s espionage-forgery.

Public-key signatures
Prerequisite: Alice has a short secret key $a$, corresponding public key $A$. Everyone knows $A$. Eve does not know $a$.
Security goal: Integrity for any number of messages published by Alice.

---

Eve cryptography
site: Alice and Bob share a short secret key $k$ and to eavesdropper Eve.
goals: Confidentiality and integrity for any number of messages exchanged by Alice and Bob, Eve’s espionage-forgery.

Public-key signatures
Prerequisite: Alice has a short secret key $a$, corresponding public key $A$. Everyone knows $A$. Eve does not know $a$.
Security goal: Integrity for any number of messages published by Alice.
SESSION 2
SETTING THE SCENE

Presentations

Public-key signatures
Prerequisite:
- Alice has a short secret key $a$,
  corresponding public key $A$.
- Everyone knows $A$.
- Eve does not know $a$.

Security goal: Integrity
for any number of messages
published by Alice.

Public-key encryption (DH)
Prerequisite:
- Alice has $a$, $A$; Bob has $b$, $B$.
- Public knows $A$ and $B$.
- Eve does not know $a$, $b$.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.
Presentations

SESSION 2
SETTING THE SCENE

Public-key signatures
Prerequisite:
Alice has a short secret key $a$, corresponding public key $A$.
Everyone knows $A$.
Eve does not know $a$.

Security goal: Integrity for any number of messages published by Alice.

\[
\begin{align*}
A & \xrightarrow{a} \text{Alice} \\
\text{Eve} & \xrightarrow{c} A \\
\text{Bob} & \xrightarrow{c'} \text{Bob} \\
\text{Alice} & \xrightarrow{m} \text{Alice} \quad \text{if } c' = c
\end{align*}
\]

Public-key encryption (DH form)
Prerequisite:
Alice has $a$, $A$; Bob has $b$, $B$.
Public knows $A$ and $B$.
Eve does not know $a$, $b$.

Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob.

\[
\begin{align*}
A & \xrightarrow{a} \text{Alice} \\
\text{Eve} & \xrightarrow{c} A \\
\text{Bob} & \xrightarrow{b} B \\
\text{Alice} & \xrightarrow{m} \text{Alice} \quad \text{if } c' = c
\end{align*}
\]

ey signatures
site:
$S$ a short secret key $a$, ending public key $A$.
$S$ knows $A$.
$S$ not know $a$.

Security goal: Integrity number of messages d by Alice.

\[
\begin{align*}
A & \xrightarrow{a} \text{Alice} \\
\text{Eve} & \xrightarrow{c} A \\
\text{Bob} & \xrightarrow{m} \text{Bob} \quad \text{if } c' = c
\end{align*}
\]

Public-key encryption (DH form)
Prerequisite:
Alice has $a$, $A$; Bob has $b$, $B$.
Public knows $A$ and $B$.
Eve does not know $a$, $b$.

Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob.

\[
\begin{align*}
A & \xrightarrow{a} \text{Alice} \\
\text{Eve} & \xrightarrow{c} A \\
\text{Bob} & \xrightarrow{b} B \\
\text{Alice} & \xrightarrow{m} \text{Alice} \quad \text{if } c' = c
\end{align*}
\]

Advance
Many or studied stopping securely searching and more
Presentations

SESSION 2
SETTING THE SCENE

<table>
<thead>
<tr>
<th>Secret key a, public key A.</th>
<th>Public-key encryption (DH form)</th>
<th>Advanced security</th>
</tr>
</thead>
<tbody>
<tr>
<td>v a.</td>
<td>Prerequisite: Alice has a, A; Bob has b, B. Public knows A and B. Eve does not know a, b. Security goals: Confidentiality and integrity for any number of messages exchanged by Alice and Bob.</td>
<td>Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.</td>
</tr>
<tr>
<td>Trust</td>
<td></td>
<td></td>
</tr>
<tr>
<td>m if c' = c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.
Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob.

Advanced security
Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.
Public-key encryption (DH form)

Prerequisite:
Alice has $a$, $A$; Bob has $b$, $B$.
Public knows $A$ and $B$.
Eve does not know $a$, $b$.

Security goals:
Confidentiality and integrity for any number of messages exchanged by Alice and Bob.

Advanced security goals
Many other security goals studied in cryptography:
- stopping traffic analysis,
- securely tallying votes,
- searching encrypted data,
- and much more.

But I'll focus on the most fundamental operations:
- secret-key cryptography,
- public-key signatures,
- public-key encryption.
Presentations SESSION 2
SETTING THE SCENE

**Key Concepts**

- **Key Exchange (DH form)**
  - Alice and Bob agree on a key.
  - Alice sends Bob $A$ and Bob sends Alice $B$.
  - They compute $c = A^b$ and $c' = B^a$.
  - If $c = c'$, they have a shared key.

- **Advanced Security Goals**
  - Many other security goals studied in cryptography:
    - Stopping traffic analysis,
    - Securely tallying votes,
    - Searching encrypted data,
    - And much more.
  - But I’ll focus on the most fundamental operations:
    - Secret-key cryptography,
    - Public-key signatures,
    - Public-key encryption.

- **Implications**
  - Critical for crypto-attackers exploiting
  - 1996 Kocher: type is broken by side s...
SETTLING THE SCENE

<table>
<thead>
<tr>
<th>Advanced security goals</th>
<th>The impact of physics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.</td>
<td>Critical for cryptography: attackers exploit physical reality. 1996 Kocher: typical crypto is broken by side channels.</td>
</tr>
<tr>
<td>But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.</td>
<td>1996 Kocher: typical crypto is broken by side channels.</td>
</tr>
</tbody>
</table>
**Advanced security goals**

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I’ll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

---

**The impact of physics**

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

---

**Advanced security goals**

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I’ll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

---

**The impact of physics**

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.
### Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I’ll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

### The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.

⇒ Hundreds of papers on post-quantum cryptography.
The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.

⇒ Hundreds of papers on post-quantum cryptography.

Post-quantum sec

\[ k \rightarrow m \rightarrow c \rightarrow c' \rightarrow m \text{ if } c' \]

Very easy solutions if \( k \) is long uniform random string.
The impact of physics
Critical for cryptography: attackers exploit physical reality.
1996 Kocher: typical crypto is broken by side channels.
⇒ Hundreds of papers on side-channel defenses.
1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.
⇒ Hundreds of papers on post-quantum cryptography.

Post-quantum secret-key crypto

\[ k \xrightarrow{} k \]

\[ m \xrightarrow{} c \xrightarrow{} c' \xrightarrow{} m \text{ if } c' = c \]

Alice \hspace{1cm} Eve \hspace{1cm} Bob

Very easy solutions if \( k \) is long uniform random string.

The impact of physics
Critical for cryptography: attackers exploit physical reality.
1996 Kocher: typical crypto is broken by side channels.
⇒ Hundreds of papers on side-channel defenses.
1994 Shor, 1996 Grover: typical crypto will be broken by large quantum computers.
⇒ Hundreds of papers on post-quantum cryptography.

Post-quantum secret-key crypto

\[ k \xrightarrow{} k \]

\[ m \xrightarrow{} c \xrightarrow{} c' \xrightarrow{} m \text{ if } c' = c \]

Alice \hspace{1cm} Eve \hspace{1cm} Bob

Already standardized method to expand short \( k \) into string indistinguishable from long \( k \):
### Presentations

#### SETTING THE SCENE

<table>
<thead>
<tr>
<th>act of physics</th>
<th>Post-quantum secret-key crypto</th>
<th>Post-quantum public key crypto</th>
</tr>
</thead>
<tbody>
<tr>
<td>for cryptography: exploit physical reality.</td>
<td>$k \rightarrow k$</td>
<td>Alice $\rightarrow A$</td>
</tr>
<tr>
<td>echer: typical crypto 1 by side channels.</td>
<td>$m \rightarrow c \rightarrow c' \rightarrow m$ if $c' = c$</td>
<td>Alice $\rightarrow$ Eve $\rightarrow$ Bob</td>
</tr>
<tr>
<td>Lots of papers on side channels.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or, 1996 Grover: crypto will be broken by quantum computers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lots of papers on quantum cryptography.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Very easy solutions if $k$ is long uniform random string.

Already standardized method to expand short $k$ into string indistinguishable from long $k$:

- Security analyzed in papers by dozens of cryptanalysts.

Safe, ready for stats:

- 1979 Merkle hash
- Public-key signature

Modern variants are guaranteed to as the underlying

Reasonable choice Keccak with 576-I
Presentations

SESSION 2
SETTING THE SCENE

<table>
<thead>
<tr>
<th>Post-quantum secret-key crypto</th>
<th>Post-quantum public-key sig</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$</td>
<td>$A$</td>
</tr>
<tr>
<td>$m$</td>
<td>$A$</td>
</tr>
<tr>
<td>$c$</td>
<td>$c'$</td>
</tr>
<tr>
<td>$c'$</td>
<td>$m$ if $c' = c$</td>
</tr>
<tr>
<td>Alice</td>
<td>Alice</td>
</tr>
<tr>
<td>Eve</td>
<td>Eve</td>
</tr>
<tr>
<td>Bob</td>
<td>Bob</td>
</tr>
</tbody>
</table>

Very easy solutions if $k$ is long uniform random string.

Already standardized method to expand short $k$ into string indistinguishable from long $k$:
Security analyzed in papers by dozens of cryptanalysts.

Safe, ready for standardization:
1979 Merkle hash-tree public-key signature system.
Modern variants of system are guaranteed to be as secure as the underlying hash function.
Reasonable choice of function: Keccak with 576-bit capacity.
Presentations

SESSION 2
SETTING THE SCENE

**Quantum-Safe-Crypto Workshop**

<table>
<thead>
<tr>
<th>Secret-key crypto</th>
<th>Post-quantum public-key signatures</th>
<th>Post-quantum public-key signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k \rightarrow k$</td>
<td>$\text{Alice} \rightarrow A$</td>
<td>$\text{Alice} \rightarrow A$</td>
</tr>
<tr>
<td>$c \rightarrow c'$</td>
<td>$m \rightarrow c \rightarrow c' \rightarrow m$ if $c' = c$</td>
<td>$m \rightarrow c \rightarrow c' \rightarrow m$ if $c' = c$</td>
</tr>
<tr>
<td>$\text{Eve} \rightarrow \text{Bob}$</td>
<td>$\text{Alice} \rightarrow \text{Eve} \rightarrow \text{Bob}$</td>
<td>$\text{Alice} \rightarrow \text{Eve} \rightarrow \text{Bob}$</td>
</tr>
</tbody>
</table>

- Solutions if $k$ is a random string.
- Standardized method to shorten $k$ into string distinguishable from long $k$: $	ext{Rijndael}$ “AES” using 256-bit key analyzed in papers by cryptanalysts.
- Safe, ready for standardization: 1979 Merkle hash-tree public-key signature system.
- Modern variants of system are guaranteed to be as secure as the underlying hash function.
- Reasonable choice of function: Keccak with 576-bit capacity.

Presentations

SESSION 2

SETTING THE SCENE

Post-quantum public-key signatures

Safe, ready for standardization: 1979 Merkle hash-tree public-key signature system.

Modern variants of system are guaranteed to be as secure as the underlying hash function.

Reasonable choice of function: Keccak with 576-bit capacity.

Post-quantum public-key encryption


Presentations

SESSION 2
SETTING THE SCENE

Public-key signatures

- A
- m if c' = c

Eve

Post-quantum public-key encryption

- Alice
- m if c' = c

Eve

Bob

Example

- Better a smaller, against
- Lattice-based cry.
- Similar i
- maybe a security
- Signature
- Multivariate very short signatu
- maybe tolerable f

http://pqcrypt.
PRESENTATIONS

SESSION 2

SETTING THE SCENE

<table>
<thead>
<tr>
<th>natures</th>
<th>Post-quantum public-key encryption</th>
<th>Examples of post-quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>= c</td>
<td>Safe, ready for standardization:</td>
<td>Better secret-key crypto:</td>
</tr>
<tr>
<td></td>
<td>1978 McEliece encryption</td>
<td>smaller, faster, easier</td>
</tr>
<tr>
<td></td>
<td>using binary Goppa codes.</td>
<td>to protect against side</td>
</tr>
<tr>
<td></td>
<td>Main security-analysis papers:</td>
<td>channels, etc.</td>
</tr>
</tbody>
</table>

Examples of post-quantum research:

- Better secret-key crypto: smaller, faster, easier to protect against side channels, etc.
- Lattice-based cryptography: similar idea to code-based; maybe allows smaller keys; security analysis not as mature.
- Signatures using codes/lattices.
- Multivariate quadratics: very short signatures; maybe tolerable for encryption.

http://pqcrypto.org
Overview of quantum key distribution technology and introduction to the work of the ETSI QKD ISG

Martin Ward, Toshiba
**Quantum superposition**

- Cannot measure all possible information content of a quantum state without prior knowledge
- Only one chance!
- Faithful cloning of arbitrary quantum state is not possible
- Encode data in different basis states at random

**BB84 protocol**

Alice and Bob both make random basis choice

They discard where choices were different

Eve measuring in the wrong basis adds errors
What goes into a real QKD system?

- Photons demonstrate wave-like behaviour
- Often encode on phase instead of polarisation using an interferometer:

```
  Alice                      Bob
  SOURCE                   SOURCE
  3dB coupler      3dB coupler
  φ₀                     φ₀
  APD2                  APD1
```

- Phases φ₀ and φ₀ are selected randomly according to two pairs of basis states
- When Bob uses the same basis as Alice a click in APD1 or APD2 will indicate the bit value sent
- When they select from different basis states it is random which APD will fire

---

Phase encoded BB84

- Both arms are collapsed into a single fibre link using time division
- Improves stability against environmental fluctuations e.g., temperature

```
  Alice                      Bob
  SOURCE                   SOURCE
  3dB coupler      3dB coupler
  PBS                      PBS
  φ₀                     φ₀
  APD2                  APD1
```

- Interference still occurs at final 3 dB coupler between short-long and long-short paths
- Optimal polarization avoids loss to paths short-short and long-long paths, which do not interfere
Lasers as sources of weak coherent pulses

- Attenuating a laser source leaves a finite probability of $n > 1$
- Reduces bit rate due to empty periods
- Opportunity for photon number splitting attack
- Privacy amplification required to remove the information that could have been obtained from multiphoton pulses

Photon number splitting attack

- Key bits exchanged on single photons
- An attenuated laser inevitably generates some multiphoton pulses
Photon number splitting attack

- Quantum non-demolition measurement of photon number
- Tap off photon from multiphoton pulses and forward other to Bob
- Store tapped photon and block all single photon pulses

Eve can now measure photon in correct basis

- Eavesdrop on reconciliation
Mitigations

Decoy states
- send occasional decoy states of different intensity
- detect photon number splitting attacks by monitoring transmission statistics
- quantify potential data loss and use privacy amplification
- offers highest key generation rates at present

Single photon sources
under development:
- quantum dot
- parametric down conversion

ETSISG QKD

Active members from national meteorological labs, universities and industry, e.g.:

- NIST, NPL, INRIM, PTB
- University Waterloo, University Politecnica de Madrid, Telecom ParisTech
- AIT Austrian Institute of Technology
- Toshiba Research Europe, Telcordia

Open to new members – contact Andrew Shields (chairman)
Areas for standardisation

- Implementation security
- Channel requirements
- Quantum networks
- Interfaces

Implementation security

- Describe the necessary system elements – without impeding innovation
- Metrology of components and system blocks
- Qualifying tests to quantify against modes of attack
- Relate back to security proofs
Channel requirements

- What are the requirements on fibre link?
- How to specify
- Enable customer to estimate performance in a network
- Requirements when multiplexing with classical data - crosstalk etc.

Quantum networks

- Quantum access networks
- Quantum repeaters
- Leading on to distributed quantum computing – quantum cloud – secure database search etc.
Presentations

SESSION 2
SETTING THE SCENE

Interfaces

- Enabling systems to be networked together
- Classical interfaces:
  - System management
  - Network routing
  - How key material is used
- Quantum interfaces:
  - Connect where technology is compatible
  - Quantum information sharing etc. in future

Standardisation approach

- Provide confidence level to customers
- Relate real implementations to security proofs
- Metrology – existing techniques and specific challenges
- Avoid stifling innovation where possible
- Start with specific templates
- Extend to other architectures
Security perspectives for quantum key distribution
Norbert Luetkenhaus, University of Waterloo
SESSION 2
SETTING THE SCENE

Security definition: preparation

- Alice classical
- Bob classical
- Eve quantum
- QKD Protocol
- Input state $\rho_{in}$
- Output state $\rho_{out}$
SETTNG THE SCENE

Security definition: preparation

\[
\sum_{x, x'} p(x, x') \left( |x\rangle |x\rangle \otimes |x'\rangle |x'\rangle \otimes \rho_E^{x'} \right)
\]
Security definition: preparation

real output state
\[ \sum_{s, s' \in S} p(s, s') \left( |s\rangle \langle s| \otimes |s'\rangle \langle s'| \otimes \rho_E^{s, s'} \right) \]

ideal output state
\[ \frac{1}{|S|} \sum_{s \in S} |s\rangle \langle s| \otimes |s\rangle \langle s| \otimes \rho_E \]

\[ \frac{1}{2} \left\| P_{A_{\text{real}}} - P_{A_{\text{ideal}}} \right\|_1 < \epsilon \]
**Security definition: preparation**

- **real output state**
  \[ \sum_{s,s'} \rho(s,s') \left( |s\rangle \langle s| \otimes |s'\rangle \langle s'| \otimes \rho_E \right) \]

- **ideal output state**
  \[ \frac{1}{|S|} \left( \sum_{s \in S} |s\rangle \langle s| \otimes \rho_E \right) \]

- Indistinguishability ensures:
  - correct (shared by Alice and Bob)
  - uniformly distributed
  - secret

---

**Security Definition**

\[ \frac{1}{2} \| \rho_{\text{ABE}}^{\text{real}} - \rho_{\text{ABE}}^{\text{ideal}} \|_1 < \epsilon \]

**Key requirements:**
- correct (shared by Alice and Bob)
- uniformly distributed
- secret
Setting the Scene

Security Definition

\( \frac{1}{2} \| \rho_{ABE}^{(\text{real})} - \rho_{ABE}^{(\text{ideal})} \|_1 < \epsilon \)

Key requirements:
- correct (shared by Alice and Bob)
- uniformly distributed
- secret

Security statement:
- the probability that
  - key protocol does not abort
  AND
  - the key is not ideal (requirements!)
  is smaller than \( \epsilon \)

Operational definition of \( \epsilon \):

1) \( \epsilon \) cannot be zero for QKD.
2) Definition does not condition on non-abortment of protocol.
   - always aborting protocols are secure by this definition (but useless!)
3) Clear interpretation of imperfection (insurance mathematics?)
Presentations

SESSION 2
SETTING THE SCENE

Development of Security Proofs

Security Model
- e.g. qubit based

Assumptions
- Security Proof
- Security Statement

Quantum Optical Model
- e.g. mode based
- e.g. realistic sources (laser pulses) threshold detector models

Security Model
- e.g. qubit based

Security Proof

\|\text{PAKE} - \text{PAK} \otimes \text{AEK}\|_1 \leq \epsilon
frequently used assumptions

- Characterized devices:
  - know what our devices are doing
    - side-channel attacks …
    - see also voltage levels of one-time pad encryption!
- access to randomness
- secure perimeter of devices
Presentations

SESSION 2
SETTING THE SCENE

Results

Characterized devices:

qubit scenario
- BB84, six-state, Ekert, B92, SARG ...

optical scenario
- laser pulses instead of single photons, threshold detectors
- new protocol classes
  (Continuous Variable Protocols, Differential Phase Shift Protocols ...)
- protocols using only characterized sources (no trusted detectors)
  [measurement-device independent QKD]
Presentations
SESSION 2
SETTING THE SCENE

Results

Characterized devices:
- qubit scenario:
  - BB84, six-state, Ekert, B92, SARG ...
- optical scenario:
  - laser pulses instead of single photons, threshold detectors
  - new protocol classes
    - (Continuous Variable Protocols, Differential Phase Shift Protocols ...)
  - protocols using only characterized sources (no trusted detectors)
    - [measurement-device independent QKD]

Uncategorized devices:
- qubit/optical protocols where only one side needs to be characterized
  (rates reduces unless partial characterization is re-introduced – loss?)

Results

Characterized devices:
- qubit scenario:
  - BB84, six-state, Ekert, B92, SARG ...
- optical scenario:
  - laser pulses instead of single photons, threshold detectors
  - new protocol classes
    - (Continuous Variable Protocols, Differential Phase Shift Protocols ...)
  - protocols using only characterized sources (no trusted detectors)
    - [measurement-device independent QKD]

Uncategorized devices:
- qubit/optical protocols where only one side needs to be characterized
  (rates reduces unless partial characterization is re-introduced – loss?)
- Protocols where all devices are uncharacterized (but random choices are utilized)
**Setting the Scene**

**Results**

**Characterized devices:**
- qubit scenario
  - BBM4, six-state, Ekeret, B92, SARG ...
- optical scenario
  - laser pulses instead of single photons, threshold detectors
  - new protocol classes
    - Continuous Variable Protocols, Differential Phase Shift Protocols ...
  - protocols using only characterized sources (no trusted detectors)
    - [measurement-device independent QKD]

**Uncharacterized devices:**
- qubit/optical protocols where only one side needs to be characterized
  - (rates reduces unless partial characterization is re-introduced — loss!)
- Protocols where all devices are uncharacterized (but random choices are utilized)

Reduction in assumptions is possible trade-off to rate — fundamental issue or proof techniques???

---

**What is a Security Proof?**

- **Model of Devices**
  - e.g., QM description
  - quantum security perimeter
  - classical security perimeter

- **Exact Protocol**
  - sequence of protocol steps
  - Error Correction method
  - Privacy Amplification function
  - security parameters

- **Scientific Security Proof**
  - "perfect secret key with exception of probability ε"
What is a Security Proof?

- Model of Devices
  - e.g. QM description
  - quantum security perimeter
  - classical security perimeter

- Exact Protocol
  - sequence of protocol steps
  - Error Correction method
  - Privacy Amplification function
  - security parameters

- Scientific Security Proof
  "perfect secret key with exception of probability e"

Testing of Models
- e.g. by embedding into larger models
- requires experience based cut-off
- no scientific proof possible

Software and Hardware Implementation
- verified software
- (development & execution)
- hardware security perimeter
- key management
SETTING THE SCENE

What is a Security Proof?

- Testing of Models:
  - e.g. by embedding into larger models
  - requires experience based cut-off
  - no scientific proof possible

- Calibration (initial and ongoing)
- Alignment
- Initialization

- Software and Hardware Implementation
  - verified software
  - development & execution
  - hardware security perimeter
  - key management

- Model of Devices:
  - e.g. QM description
  - quantum security perimeter
  - classical security perimeter

- Exact Protocol:
  - sequence of protocol steps
  - Error Correction method
  - Privacy Amplification function
  - security parameters

- Scientific Security Proof:
  - "perfect secret key with exception of probability ε"
Presentations

SESSION 2
SETTING THE SCENE

---

**IQC**

**What Boundary between scientific and acceptance can be moved (device independent security proofs) but never vanish?**

- **Model of Devices**
  - e.g. QM description
  - Quantum security perimeter

**So what remains?**

**QKD provides secret key that is future-proof (on quantum side): the key is as secure for all future as it is at its creation!**

- **Software and Hardware Implementation**
  - Verified software
  - Development & execution
  - Hardware security perimeter
  - Key management

---

**Distance Scaling**

Use fiber optics devices

- log(K) key rate
- Channel loss
- Detector saturation
- Detector noise

Maximum distance: just under 200 km

Scaling with distance (fiber): $K \sim \exp\left(-\alpha d/10\right)$ (no amplification possible!)

**Example:**
- 1 THz clockrate
- 0.17 dB/km
- 700 km = 120 dB
- 1 bit/sec over 700 km (infinite key limit)
Presentations

SESSION 2
SETTING THE SCENE

Distance Problem: Trusted Repeater Networks

Realizations:
- DARPA Network 2002-2005
- SECOQC Network 2004-2008
- Tokyo Network (2010)
- South Africa
- Geneva

Use trusted classical nodes to propagate secrets through network:
- Can cover metropolitan area networks
- At reasonable key rates
- Stability against failure of individual links

Note:
- Users of network should also be operators
- Trust level must be high!

Distance Challenge: Moving Satellite

Satellite

User A

User B
SESSION 2
SETTING THE SCENE

Presentations

Quantum Repeater

Quantum repeater network: (technologically challenging) [Application: Service Provider]
Overcomes loss problem
allows routing

Alice
Memory
BELL measurement

Effective Channel

BELL measurement

Bob

Quantum Repeater

Quantum repeater network: (technologically challenging) [Application: Service Provider]
Overcomes loss problem
allows routing

Alice

Effective Channel

BELL measurement

Bob
Quantum Key Distribution in the real world
Grégoire Ribordy, ID Quantique
Presentations

SESSION 3
INDUSTRY SESSION

Why use QKD?

- Long-term confidentiality of data is a difficult goal to achieve
  - Health sector (specific legal requirements in certain countries)
  - Financial and industrial sector
  - Government and military sector

- Current encryption schemes (AES, RSA, Elliptic curves, ...)
  - No guarantee for long-term confidentiality
  - Based on computational problems whose hardness is unproven
  - Post-Quantum Cryptography schemes offer security against known quantum adversaries, but are nevertheless based on computational problems

- Solution for long-term confidentiality
  - Information theoretic cipher + Information theoretic key distribution

Long-Term Confidentiality

QKD:
- transfer of a sequence of random bits across an optical link
- detection of interception attempts

In essence: Distributed TRNG

Why?
- QKD is (very) slow

Logic:
- At least 80 bits of security
- Quantum Computing on AES: Key / 2
- AES-256: security of 128 bits > 80 bits
- Key refresh: prevent keys from gaining too much value
Presentations

SESSION 3
INDUSTRY SESSION

When do we need to start worrying?

- Information Exchange
- Time for migration
  (from a few months to several years)
- Information lifetime
  (based on legal, business or strategic constraints)
- Vulnerability

Overview

- Why use QKD?
- Commercial Solution
- Use Case
- Market Adoption
- Current developments
Presentations

SESSION 3
INDUSTRY SESSION

Commercial QKD Solution

QKD Server

- Optical System (including detectors)
  - Autocompensating optical system
  - Protocol: BB84 and SARG

- Electronic Controller
  - Including Quantum TRNG
Presentations

SESSION 3
INDUSTRY SESSION

Quantum Random Number Generator

QKD Server

- Optical System (including detectors)
  - Autocompensating optical system
  - Protocol BB84 and SARG
- Electronic Controller
  - Including Quantum TRNG
- Industrial PC (not shown)
- Software
  - Raw Key Controller
  - Key Distillation
  - Key management
- I/O
  - Quantum Channel (optical fiber)
  - Classical channel (standard transceiver)
  - Management (ethernet, USB)
  - Key ports (12x Serial)
High-Speed Encryption

- Hardware (FPGA based) Encryption
  - Low latency and full throughput
- AES-256 in CTR and GCM modes
- Max throughput: 10Gbps
- Encryptors supplied by SENETAS

Layer 2 Encryption

Protocol Protection: Significant impact
Network Protection: No impact
Key Management

- RSA 2048 or 4096 → Master key (sym, 256)
- AES-256 → Session key (sym, 256)
- Master and session key: 1 per direction

Overview

- Why use QKD?
- Commercial Solution
- Use Case
- Market Adoption
- Current developments
Worldwide Deployments

Systems installed in more than 20 countries

Overview

- Why use QKD?
- Commercial Solution
- Use Case
- Market Adoption
- Current developments
**Factor #1: Cost-Security Arbitrage**

- Organization implement cost reduction plans
- CSO validates exception to company policy: optical fiber links don’t need to encrypted.
- Applies to all security solutions, but has more impact on QKD due to its higher cost.

---

**Selling security...**

<table>
<thead>
<tr>
<th>Choice #1</th>
<th>Choice #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Sure gain of 500 EUR</td>
<td>a) Sure loss of 500 EUR</td>
</tr>
<tr>
<td>b) 50% chance of winning 1'000 EUR</td>
<td>b) 50% chance of losing 1'000 EUR</td>
</tr>
</tbody>
</table>

85% a) 15% b) 30% a) 70% b)

Prospect Theory, Kahneman and Tversky, 1979
Factor #2: Quantum-specific infrastructure costs

- Requirements for QKD: optical transparency between emitter and receiver

- Different approaches:
  - Dedicated optical fiber
    - Long distance (no perturbation by other signals)
    - Costs reasonable within cities
    - High costs in regional networks
  - Multiplexing with other optical signals
    - Strong performance degradation due to cross-talk

- Note
  - Cost of QKD hardware also an issue

Current Specs: 4 λ's over 70km
Development: up to 100 λ's
Factor #3: Range Limitation

Classical Communications

- Optical Link
- 20dB / 70-80km
- ~10^7 photons
- ~10^5 photons
- ~10^7 photons

Quantum Communications

- Optical Link
- 20dB / 50 – 100 km
- 1 photon
- 0 photon

Current performance:
- IDQ cutoff = 100 bits/s
  (ability to serve 2 keys per minute to 12 encryptors)
- Max attenuation: ~20 dB
- Longest commercial deployment: 78 km
**Overview**

- Why use QKD?
- Commercial Solution
- Use Case
- Market Adoption
- Current developments

**Practical Security**

QKD: relation between QBER and Information leakage

Hardware Countermeasures

Postprocessing (privacy amplification)

Similar to side channels in conventional crypto
PRESENTATION SESSION 3

INDUSTRY SESSION

New Optical Platform

Specifications
- Same as current solution (continuous operation, etc.) AND
- COW Optical Platform
- Up to 1 Mbps QKD Secret Key Rate
  - 625 Mbps clocked QKD with 1.25 GHz gated detectors
  - Hardware key distillation
- 4-fibre DWDM configuration
- Extended range
- 1 Mbps One-Time-Pad encryption

Relaying Quantum Keys

Sharing keys between unconnected nodal points
Summary

- Distributed TRNG outputing fresh and independent keys
- QKD technology is reliable with
  - Several testbed demonstrations worldwide, some of them over up to 21 months
- QKD solutions combined with layer 2 encryptors are in use today
  - 4 keys per second over 25 km
  - Longest deployment: 77 km
- Applications in the financial and government sector for long-term confidentiality
- Quantum Technologies provide important primitives for key management

Thank you for your attention

6th Winter School on Practical Quantum Communications

Dates: Sunday January 19 to Thursday January 23, 2014
Location: Les Diablerets, Switzerland
More: www.idquantique.com or info@idquantique.com

Key note speakers include:
- Gilles Brassard
- Nicolas Gisin
- Vadim Makarov
- Sandu Popescu
- Renato Renner

Pictures from previous editions
Presentations

Kerberos Revisited
Léon Pintsov, Pitney Bowes

Abstract

The substitution of one cryptographic scheme for another is a lengthy development that far surpasses the duration of the standardization process, given the requirements of coordinated deployment and investment in core services. For example, it has been two decades since the first ECC-based standard has been published, but it has only recently achieved broad adoption. Looking forward another fifteen to twenty years, we see growing concerns of a quantum computing threat to the security of traditional public-key cryptography. Simultaneously, we see a rise in cellular-connected devices and trust topologies that are hub-and-spoke in nature and could be well served by symmetric-key systems, which are not known to be quantum vulnerable. Kerberos is a leading symmetric-key system that is in widespread use today in modern operating systems, but under-deployed in internet-based schemes. This talk explores the current state of Kerberos deployment and outlines a blueprint for the additional research, standardization, coordinated development, and investment in global services that would be required to make internet-wide Kerberos services a trusted and ubiquitous post-quantum cryptographic solution. Specifically, we discuss the most prominent challenges facing Kerberos adaptation to the internet environment and propose potential approaches that could address these issues.
Participants

• The Mission of the MIT-Kerberos and Internet Trust Consortium (MIT-KIT) is to develop the basic building blocks for the Internet's emerging personal data ecosystem in which people, organizations, and computers can manage access to their data more efficiently and equitably.

• Pitney Bowes is a provider of cryptographically secure payment and data management systems to worldwide postal and logistics community. Pitney Bowes developed, built and operates a broad information security infrastructure supporting over 2M users worldwide.

Motivation

• Quantum computing field is 20 years old
  – Significant theoretical progress (Shor's results, error-correction "threshold" theorem)
  – Meaningful experimental progress:
    • 5 qubit to 128 or even 429 qubit (D-Wave computer, although it does not make use of entanglement)
• It is not unreasonable to assume that working quantum computer may become a reality in the foreseeable future
• Classic public key algorithms that are based on hardness of factorization and discrete logarithm problems may become vulnerable
• A "good" symmetric key based-system may prove to be very beneficial in many applications
• MIT-KIT, M. Campagna and Pitney Bowes have common research interest in investigation, development and test of a broadly scalable quantum-safe solutions for Identity and Access Management
Presentations

SESSION 3
INDUSTRY SESSION

Kerberos Models

- Single-Provider Model
- Cross-Realm Federated Model

Requirements

- Quantum Safe
- Support Authentication and Federated Identity System
- Deployable on an "internet scale" – every user, multiple devices, multiple providers, …
  - Establish secure communications to remote servers/networks (must enable traditional security services: authenticity, integrity and secrecy and non-repudiation of message content)
- Designed for Usability
  - Accessibility, convenience, intuitiveness
  - Optimum balance between security and usability

Pitney Bowes
Kerberos Challenges

- Development
  - Need good APIs and tools to enable developers to build on the existing Kerberos system
- Federation
  - Service providers should be enabled to integrate technology into their offering to establish a chain of trust
- Enrollment
  - Must be efficient, secure, and convenient for the end users
- Administration
  - Must be efficient, secure, and operable at scale

Development and Implementation

- Need a RESTful services API that give access to the Kerberos protocol
  - Enable access to Kerberos without going through GSSAPI
- Software, tools, integration, and deployment
  - Example: model after OpenSSL or other popular web implementations
- Develop tools with application development and specific use cases in mind
Enrollment

- Provision a long-term symmetric key that is not password derived (for each user, and possibly each device)
  - Strongly random and securely distributed and installed
- Options
  - Use existing relationship between end users and commercial establishments (employers, banks, etc.)
  - Device based – pre-installed keys
    - Keys to be issued by a device manufacturer or a carrier at time that device is manufactured or delivered. Root of trust for each device starts with the manufacturer or carrier
    - Financial arrangement with a primary user establishes the identity of the accountable user – users may delegate their rights on their device to others (i.e., the accountable user could become the “RA”)
  - Retail channels to acquire credentials
    - Postal Infrastructure
    - Retail Kiosks
    - Social – PGP-like model (peer to peer chain of trust)
  - Quantum Key Distribution
    - ComDev/IQC proposal for quantum key distribution via microsatellites

Federation

- Need a “critical mass” of KDC and AS operators
  - Every user must have a relationship with one or more provider and they must trust the provider to manage their identity
  - They need to do cross-realm authentication
- “Standard” contracts to establish “legal trust”
  - NSTIC process may provide templates
- Need for an accreditation and audit protocol and authority
- Establishing federation today is harder than it ought to be
Administration

- Physical (hardware) security can improve trust in providers
- Time synchronization issues
- Dealing with compromise or loss of user credentials
- Compromise of a KDC
  - Need to continue operations and recover
  - Consumers will likely require multiple authentication services providers

Stack model view of cryptographic standards

Cryptographic standards have wide applicability across many industry spaces
Most influential specifications have the widest adoption—e.g., FIPS/NIST SP
Vertical markets generally adopt from specific core standards
Adoption requires that specs are freely available and timely
Role of Standards

- For any wide-spread quantum-safe solution:
  - Cryptographic primitives need to be widely accepted by international and national standards bodies, like FIPS, ANSI and ISO;
  - Higher level protocols and use cases need to be specified in IEEE, IETF and other application-specific standards bodies;
- Current advantages of Kerberos:
  - Kerberos is already accepted as a trusted and tested protocol which is agile to the underlying cryptographic primitives;
  - Already integrated in every major platform;
  - Uses widely adopted and tested cryptographic primitives, and specified in higher level protocols
- Standardization Process
  - Primitives – ANSI / NIST
  - Algorithms – IETF / IEEE

Infrastructure requirements

- Virtual environments make it difficult to ensure trust
- Hardware Security Module or “Virtual Trusted Platform Module” technology may be needed
- Concept – segment the KDC architecture and create a secure co-processor that provides crypto-acceleration and secure key storage
- Need a spectrum of solutions that make different trade-offs on scale and trust
  - Need to define metrics to describe the security levels and make users aware of the meaning of the different levels
Digital Signatures and Non-Repudiation

- Digital signatures require a third party notary service provider
  - Verification must be done online

- Existing symmetric-key digital signatures have potential, but are not efficient
  - Example: Lamport-Merkle scheme

OpenPDS: Technical Vision

- Sources of the user's personal data

- External Data Sources

- Virtualized Environment

- Hardware (User Operated)

- Filing Party (FP)
Conclusion

- There is nothing inherent in the Kerberos protocol that prohibits use in a wide-scale, federated deployment.
- Standards are critical for wide scale implementation:
  - Integration of Kerberos with web services and internet applications.
  - Federation, certification, and auditing standards for service providers.
  - Template agreements to initiate trust relationships.
- Maintenance of both open source (with a permissive license) and commercial implementations could support expedited integration and adoption.
- We identified and sketched major challenges to adoption of the Kerberos-based system into deployable Internet scale authentication system.
A roadmap to migrating the internet to quantum-safe cryptography
William Whyte, Security Innovation

Abstract

We provide an overview of the steps that could be gone through to migrate existing secure systems to be secure as the world moves towards quantum computing. With a particular focus on SSL and on FIPS 140 certification, we identify design choices that must be made to enable clean migration and institutional actors that need to act to allow the technical changes to take place.
Conditions for successful deployment

- Post-quantum crypto must be:
  - Agreed
  - Standardized in core standards
  - Standardized in protocol standards
  - Accepted in certified cryptographic modules
  - Available in certs issued by CAs
  - Deployed in software
  - Usable under licensing terms the industry finds acceptable

Agreement!

- We need to agree what quantum-safe cryptography is
- The academic track
- All cryptography that is believed quantum-safe is vulnerable to criticism that it hasn’t received enough scrutiny
  - (Has it been hashed to signatures)
  - It may be vulnerable to classical attacks as well as quantum attacks
  - Or to fear of backdoors, see “The Factor is Dead” presentation
  - Or to fear of NPA backdoors, see widespread fear of NPA backdoors
- We should look at combining public key algorithms
  - 3 public-key encryption algorithms each transmit 32 bytes of key material, hash or XOR them together
  - Countersign documents 3 times
- This gives greater security against unexpected attacks
  - Allows greater confidence to start migration now as opposed to panicking and picking a single algorithm
  - Potentially allows quantum-safe algorithms to be combined with ECC/DSA to meet existing FIPS certification requirements
- Cost: greater packet size & processing time – but in a lot of settings these are both very cheap nowadays
Core crypto standards

- Official standards development organizations (SDOs):
  - ASC X9, IEEE 1363, ISO/IEC JTC 1/SC 27/WG 2, ETSI SAGE
- “Pet” standards organizations
  - SEC, PKCS, CEES, ...
- See my poster session, “A non-scary guide to standards for people who only know about cryptography”
  - NB guide not guaranteed not to be scary, no money will be returned

Protocol standards

- IETF: TLS, IPSec, S/MIME, OpenPGP, ...
- TLS is the big dog
Procurement and certification

- FIPS, NIST Special Publications, Common Criteria
- FIPS 140-X, cryptographic module validation:
  - Modules must support specific ("FIPS-approved") algorithms
  - Only FIPS 140-2 approved mechanisms may be used for key establishment
    - On the face of it, rules out double-encryption
- No specified process by which an algorithm becomes FIPS-approved
- When secure double-encryption frameworks are standardized, NIST should consider allowing double-encryption where one algorithm is already a FIPS-approved algorithm but the other need not be.

Certs

- Need CAs to issue certs:
  - Signed with post-quantum crypto algorithms
  - Containing keys for post-quantum crypto algorithms
- CAs are slow to add support for additional algorithms
  - Symantec apparently only added support for ECC and DSA in February 2013
- CA root certs are hard to roll over and some of the most long-lived trusted data elements in the Internet
- Ideally, want to lock in new signature algorithms for root certs first
  - but this is the area where new algorithms are hardest to introduce
- Building new CA technology will take many years and market will be slow to reward early adopters
Deployment

- Once standards are written, software needs to be deployed
- How to encourage deployment before a crisis hits?

Licensing and patents

- Post-quantum crypto algorithms must be available under reasonable licensing conditions
- Hard to compete with “free”
- ... though “free and broken” is easier to compete with
- Different standards bodies have different approaches to patented technologies
  - IETF strongly opposed
  - IEEE / ISO / CTCI accept patented technologies if accompanied by TRAND statement
  - Free or Reasonable And Non-Discriminatory license policy
- Licensing issues are perceived as slowing down the adoption of many new crypto technologies
  - DigiCert, ECC, ...
- Whatever standards bodies think, companies need to make commercial decision
- Hard before RI is demonstrated
- Also, both endpoints need to talk the same algorithm
- If algorithms are not widely licensed, no guarantee that your client can talk to your server
Announcement

- NTRU Patents and reference code to be available under GPL
  - [https://github.com/NTRUOpenSourceProject/ntru-crypto](https://github.com/NTRUOpenSourceProject/ntru-crypto)
  - Work in progress
- Includes new signature algorithm, PASSSign
  - Provably secure against transcript attacks via rejection sampling
  - See my other poster in the poster session
- Go use it!
- Also, we're hiring: [https://www.securityinnovation.com/company/about-us/careers/](https://www.securityinnovation.com/company/about-us/careers/)

Encrypt/Decrypt Performance Comparison

<table>
<thead>
<tr>
<th>Security Level (Classic)</th>
<th>NTRU Key Size</th>
<th>ECC Key Size</th>
<th>RSA Key Size</th>
<th>NTRU Ops/Sec</th>
<th>ECC Ops/Sec</th>
<th>RSA Ops/Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>4411</td>
<td>224</td>
<td>2048</td>
<td>10638</td>
<td>951</td>
<td>156</td>
</tr>
<tr>
<td>128</td>
<td>4829</td>
<td>256</td>
<td>4096</td>
<td>9901</td>
<td>650</td>
<td>12</td>
</tr>
<tr>
<td>192</td>
<td>6523</td>
<td>384</td>
<td>7680</td>
<td>6849</td>
<td>285</td>
<td>8</td>
</tr>
<tr>
<td>256</td>
<td>8173</td>
<td>512</td>
<td>15360</td>
<td>5000</td>
<td>116</td>
<td>1</td>
</tr>
</tbody>
</table>

1. Comparisons in C on a 2 GHz Platform
2. RSA ops are private-key; public-key are considerably faster
3. NTRU parameters are the "cost-optimized" ones from AS'93.3; can also be optimized for speed or size.
4. RSA and ECC figures are from highly optimized toolkits; NTRU figures are from reference toolkits and can be significantly improved with optimization
Advances in the security analysis of CVQKD
Sébastien Kunz Jacques, SeQureNet

Abstract

During the last years, coherent-state Continuous Variable QKD, a QKD technology relying only on off-the-shelf optical components, moved from a lab technology to commercialized products. Over the course of this evolution, several advances were made regarding both the theoretical and the practical security analysis of this technology. This includes:

• the analysis of deviations from ideal protocols (finite-size effects, uncertainty of calibrated quantities, imperfect modulation), and supplementation of the security proofs to take into account some of these deviations;
• the identification of several potential side-channel attacks paths (calibration procedures, trojan horse attacks), and implementation of countermeasures for these side-channels
• the integration of CVQKD devices with classical encryptors and development of a framework using secure cryptographic processing for the management of secure key storage and transfer between QKD devices and client devices.

In this talk, we will present an overview of the above topics and the current reflection about CVQKD security.

SeQureNet is a company founded in 2008 that develops and sells CVQKD devices and QKD-related IP.
Presentations

SESSION 3
INDUSTRY SESSION

CVQKD: Gaussian protocol

Grosshans-Grangier 2002
- Send coherent states with Gaussian distribution
- Measurement: choose a random quadrature \( \in \{X, P\} \)
- 3dB limit w/ direct reconciliation, but not with reverse reconciliation

Key rate function of
- alice modulation power
- Bob SNR \( \Rightarrow T \)
- ratio of Bob signal noise over shot noise \( = 1 + T\xi \)
- Bob detection efficiency \( \eta \)

Coherent asymptotic proof
- or collective proof w/ finite-size effects
Experimental results (Nat. Phot. 7, 378–381, 2013)

Parameters: \( d = 25\, \text{km}, 53\, \text{km}, 80\, \text{km}, \eta = 0.552, V_{\text{ave}} = 0.015, \)  
\( \text{SNR}=1.1, 0.17, 0.08, \beta = 94\%, \epsilon = 10^{-10} \)

Leakage of secret-related information

- outside Alice/Bob boxes
- with or without Eve’s “help”
- information available to Eve not taken into account in security proofs
Alice: Imperfect modulation

- Laser noise: attributed to Eve, safe
- Gaussian assumption, but real modulation
  - truncated
  - discrete
- Shot noise masks imperfections: \( \sqrt{N_0} \)
  - \( \epsilon = 10^{-10} \) for 8-bit depth

Bob: added noise

- Lowers SNR \( \Rightarrow \) reduces apparent transmission, mutual information
- Excess noise estimate unaffected provided
  - added noise \( \ll \) shot noise
  - correct shot noise estimation method is used
- Reduces performance but safe
Presentations

SESSION 3
INDUSTRY SESSION

Probing Alice or Bob

- Send light inside Alice/Bob, analyze reflections.
- Goal: obtain information about internal state of modulators.
- Ongoing work with Nitin Jain, Imran Khan, Max Planck Institute.
- Generic attack. On DVQKD:
  Demonstrating feasibility of a Trojan-horse attack on a commercial quantum cryptosystem
  N. Jain, I. Khan, C. Wittmann, E. Anisimova, V. Makarov, C. Marquardt, G. Leuchs.

Probing Alice or Bob: example

Graph showing fluctuations in power level (dB) with distance (m).
Probing Alice or Bob

- On Alice side: mostly safe (strong attenuation)
- Bob side: work in progress may be possible to probe phase modulator ahead of time
- Simple countermeasures:
  - Optical isolators
  - Optical fuse to limit incoming power

Measuring the Shot Noise

- Crucial for CVQKD
- Can be done indirectly using the local oscillator power
- But unreliable: can be altered by
  - delaying the measurement trigger
  - making the detection saturate
Presentations

SESSION 3
INDUSTRY SESSION

---

Measuring the Shot Noise in Real Time

- Signal
- Local Oscillator
- Signal + LO

- Ant. amplitude Modulator
- PM, PM Modulator
- PM, Phase Modulator
- PM, Heterodyne beam splitter

---

Bootstrapping Trust

- Alternative to common secret: Lamport signatures
  - Asymmetric signatures built only from cryptographic hash functions
- Used only for first session, short-term security
- Easier Deployment

---
Key Management and Secure Devices

- Smart Cards or HSM act as safes for secret values
- Channel authentication
- Secure channel with devices consuming keys
- Configuration access management

Complete QKD implementation in secure environment not feasible today

State of CVQKD security

- Academic work progressing fast
  - “ultimate” proofs
  - side channels
  - WDM
- Current products follow research
- An offset of a few years compared to DVQKD
- Simple optics and detectors makes CVQKD resilient
Quantum Cryptography Platform for Test & Evaluation for EU-relevant Deployment Scenarios
Pravir Chawdhry, Joint Research Centre

Abstract

We will present a proposed test platform to support test, evaluation and experimentation with emerging quantum cryptography (QC) technologies vis a vis real-life application scenarios in emerging EU policy areas with a security dimension. It is recognised that Europe has technological lead in QC domain and the proposed platform is intended to help maintain competitive lead.

In the past decade, quantum cryptography (QC) has matured beyond laboratory environment. One of the main applications has been quantum key distribution (QKD) to enable secure key exchange and thereby ensure confidentiality and integrity in a communication channel. A number of pilot projects have been carried out to validate the feasibility of the technology in the real world, addressing applications such as banking transactions, electronic voting. At the same time, commercial products have appeared on the market to assert the technological maturity of QC.

Despite proof-of-concept demonstrators and commercial products, there is still an open question: Which are the unique deployment scenarios for QC – which real-world applications severely suffer from inadequacies of traditional secure communications tools that could be addressed uniquely through QC-based solutions. Due to the current cost and complexity constraints of QC and a lack of large-scale deployment, it is necessary that an open test environment is created for a broad set of stakeholders – industry, academia and policy makers – where real world deployment scenarios are identified, deployed and tested on an ongoing basis. The test environment would offer opportunities to test alternative QC schemes in different needs-driven contexts. It is hoped that such a platform will provide informed choices for priorities in future technical developments as well as opportunities to standardize QC technologies, giving the European industry an important impetus in this innovative and competitive sector.
A Quantum Cryptography Platform for Test & Evaluation for EU-relevant Deployment Scenarios

Pravir Chawdhry
Joint Research Centre – European Commission

ETSI Workshop on Quantum Safe Crypto
Sophia Antipolis, 26-27 September 2013

The CORSA Action

Protection of Communications Radio-navigation and Space Assets

Communications    Radio-navigation    Space

Activities related to potential threats to communications and navigation

Policy support and collaboration with different European Organization are key elements of our activities

Main customers:
- DG ENTR
- DG HOME
- DG CNECT
- ETSI and CEPT
JRC Expertise: Key experimental facilities
for tests and measurements to support regulation and standardization

Quantum Safe Crypto & QKD

QKD: using quantum physics to secure encrypted communications
QC: using quantum physics to break encryption via massively parallel search

How are the two related? One is the problem created by a solution, the other is a solution to solve a somewhat different though related problem.

QSC: Robust cryptographic algorithms to resist efficient brute force attacks possible by quantum computers (or QCQPs)
Qbits at work: D-Wave

NASA and Google partner to work with a D-Wave Quantum Computer (Forbes, 16 May 2013)

Lockheed Martin bought a version of D-Wave’s quantum computer and plans to upgrade it to commercial scale (NYT 21 March 2013)

15-city TSP: the V5 chip found optimal solutions in less than half a second, while the best classical software solver required 30 minutes (http://www.gizmag.com/d-wave-quantum-computer-supercraps-computer-ranking/27476/)

Where is QKD today?

- Research – devices, algorithms
- Laboratory tests – proof of concept
- Demonstrations – small applications
- Testbeds – interoperability, distance, ...

Products
- technological maturity
- implementation dependency
- integration in ICT networks
- Scalability
- number of nodes
- 1:1 or many-to-many network topology

Security tests
- Applications?

A solution looking for a problem!
The Tokyo QKD Network 2010

A cooperation platform between Japanese and overseas research organizations to disseminate outcomes of quantum cryptography and communications

NICT, NEC, Mitsubishi Electric, NTT, Toshiba Research Europe, IDQuantique, AIT, University of Vienna, ETSI, ...

Tokyo QKD Network 2010

Live demonstration including:
- absolutely secure video transmission,
- detection of an eavesdropper,
- rerouting to the secondary secure link

Deployment plans: "where communication security is imperative to protect state secrets"

- NICT internal networks
- Government agency networks
- Mission critical infrastructures
- financial, medical and business organizations
Presentations

SESSION 4
METROLOGY SESSION

JGN-X Quantum Phase III (2011-15)

Participation of European Organisations?

Recent developments

Smartphone data safety with quantum cryptography (QKarD)
(www.LANL.gov 26 Jan 2012)

Physicists at University of Bristol
Test Quantum Cryptography For Handheld Mobile Devices
(MIT Tech Review 28 August 2013)

Cryptography of the future - DLR technology enables quantum key transmission from the air to the ground
(http://www.dlr.de 2 Apr 2013)
QKD Use case 1: Galileo PRS

**PRS**

*Public Regulated Service*

**Encrypted navigation signal**

**Quality:**
High precision, reliable, secure

**Target users:**
Authorized government users, e.g.
Police, Civil protection, Coastguard,
Border control, ambulance, S&R,
Defence, ...

**Scale:**
Tens of thousand of PRS receivers

**Challenge:**
Secure distribution of PRS codes (crypto keys) on a large scale

---

**Galileo PRS Process**

**How the PRS works**

[Diagram showing the process of Galileo PRS]
**QKD Use case 2: External border management**

**External Borders:**
- 42,000 km coastline
- 9,000 km land borders
- 300 international airports
- +1,800 border crossing points
- 500 million border crossings/year

**Mechanisms:**
- 28 national passports & many readers
- Encryption on passports (BAC, EAC)
- Key distribution to passport readers with regular updates

**Challenge:**
Secure distribution of cryptographic keys to thousands of border control units in the EU and update them frequently.

**Requirements for a European testbed for Quantum Crypto Testbed**

**Applications driven**
- Secure key distribution (N-to-M nodes)
- Scalable to a large number of clients
- Long-distance
- Low cost (eventually)
- Compact
- Robust
- Easy to use (well packaged)

**Promote technological maturity**
- Testing, metrics and certification for quantum cryptography devices
- Quantum-resistant crypto algorithms
- QKD/QSC security
- Interoperability

**Promote innovation**
- Unexpected applications
- Mobile consumer devices
- Value for money!
Strategic options

Summary

- ICT infrastructures depend on secure communications
- QKD has been already proven to work in demonstrators
- Technological maturity with integration in ICT networks
- The next step is to scale up with large scale test beds
- Quantum safe crypto is an emerging field due to the MPP-like capabilities of Quantum Computers
- The 'solution' is still looking for 'credible problems' for real life applications
- EU application scenarios pose a big challenge as well as an opportunity to Quantum Cryptography
- A European QKD/QSC Testbed would provide a real-life environment to promote innovation in this strategic area
Thank you

We thankfully acknowledge the copyrights of various copyright holders for the external images used in this presentation for illustration purpose only.

Pravir Chawdhry
Pravir.Chawdhry@jrc.ec.europa.eu
+39 0332 78 58 23
Abstract

The lack of validation and standardisation is a barrier to the wider commercialisation of QKD. A joint research project [1] aims to develop metrological techniques, standards and methods for new industrial quantum optical communication technologies. The project is focused on faint-pulse QKD, the most commercially advanced technology. It is funded under the European Metrology Research Programme, is of three years’ duration, and started in September 2011.

A faint-pulse QKD system operating in the 1550 nm spectral region comprises a photon emitter, an optical channel, and a photon receiver. Random number generators are also essential to QKD. Characterising parameters of these components which can affect the security and/or efficiency of a QKD system is the focus of this project. Among these are: clock frequency, mean photon number, timing jitter, wavelength, spectral line width, spectral and temporal indistinguishability, and polarisation state (emitter); photon detection probability, dark count probability, afterpulse probability, dead time, recovery time, maximum count rate, timing jitter and spectral responsivity (receiver).

An overview of the project, and a review of its achievements to date, will be presented. The latter includes new quantum measurement devices and instrumentation, and work to characterize an open system quantum random number generator.

[1] The partners in the Metrology for Industrial Quantum Communications (MIQC) project are: the National Measurement Institutes of the Czech Republic (CMI), Estonia (Metrosert), Finland (MIKES), Germany (PTB), Italy (INRIM) (co-ordinator), the United Kingdom (NPL), and South Korea (KRISS); idQuantique; the Austrian Institute of Technology (AIT); Aalto University; Oulu University; and the Polytechnic of Milan.
Presentations

SESSION 4
METROLOGY SESSION

Metrology for QKD – an industrial quantum optical communication technology

Christopher Chunnillall
christopher.chunnillall@npl.co.uk

1st ETSI Quantum-Safe-Crypto-Workshop
Sophia-Antipolis, France
26-27 September 2013

IND06: Metrology for Industrial Quantum Communications
http://www.miqc.org/

- Objective: to develop a pan-European measurement infrastructure to develop standards and characterisation facilities for commercial Quantum Key Distribution (QKD) devices.
- QKD devices require independent physical characterisation in order to convince end-users that the technology is working within specification
- Focus on faint-pulse (weak coherent pulse) QKD over fibre at 1550 nm
- 3 year project
- Start Sept 2011; now 2 years into project
QKD
• physical (as opposed to algorithmic) process
• security depends on physical performance of system at time of key creation (as well as algorithmic post-processing)

IS IT?
• Customer assurance ✓
• Market confidence ✓
• No catastrophe

System optimisation
- Expected QBER, ∆QBER
- Bit rate and distance
- Privacy amplification

System stability
- 'Natural' change:
  - Performance-changing attacks

Security from hacking
- (Side-channels)
- Basis and bit indistinguishability
- (photons, detectors)

Measurement of the physical parameters of the system

Standards and characterisation facilities – interaction with ETSI QKD-ISG

• Three MIQC partners (INRIM, NPL, PTB) are members of the ETSI QKD-ISG, and facilitate information exchange between the ISG and MIQC

• The MIQC project has collaborated closely with the ISG to identify and document the physical parameters of faint-pulse QKD systems which require measurement

• The MIQC project is developing the necessary capability to measure these parameters in a way that is traceable to the SI with a quantified uncertainty

• This expertise will be fed back to the ISG in order to draft appropriate standards which define the relevant measurement processes for universal implementation
traceable measurements

m A mol cd kg K s

Environment Communications Healthcare Food

Industry Science Doctors Regulators Health & safety Transport

Geographical & temporal consistency Universal acceptance

http://www.bipm.org/en/si/

Key Measurement Outputs of MIQC

Phase encoded, attenuated laser pulse QKD over fibre at 1550 nm

Photon emitters
- Traceable characterisation of commercial QKD sources:
  - Attenuated laser pulses, phase encoding

Quantum channel (optical fibre)
- Traceable characterisation of single mode optical fibre
- Characterisation of propagation of photon state in single mode fibre
- Development of in-line calibration devices

Random number generator (idQuantique)
- Open system true physical random number generator (TPRNG)
- Physically characterised and tested under different operating conditions

Photon receivers
- Traceable calibration of commercial QKD receivers:
  - Gated photon counting detectors

QKD testbeds
- Development of testbeds
Presentations

SEVEN 4
METROLOGY SESSION

Primary properties requiring characterisation
- Mean photon number
- Probability distribution
- Temporal pulse jitter duration
- Wavelength
- Spectral bandwidth
- Spectral indistinguishability
- High-resolution single-photon spectrometer
- Spectral attenuation
- Chromatic dispersion
- Optical length
- Backscatter
- Polarisation mode dispersion, dependent loss, decoherence
- Wavelength multiplexed fibre links
- Detection efficiency
- Detection linearity
- Dark count probability
- After-pulse probability
- Deadtime and recovery time
- Temporal jitter
- Back-flash
- Detector indistinguishability (multi-detector receiver)

Detector efficiency
(gated detector)

[Established technique, adapted for QKD]
Optical power traceability chain (SI)

0.005% uncertainty
visible wavelengths,
0.5 mW,
collimated,
free-space laser
radiation

1% uncertainty ($k = 2$)
1550 nm,
100 pW,
output from optical fibre

<table>
<thead>
<tr>
<th>Pulse frequency</th>
<th>Power ($\mu = 1$)</th>
<th>dBB (wrt 128 pW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GHz</td>
<td>128 pW</td>
<td>0</td>
</tr>
<tr>
<td>50 MHz</td>
<td>6.4 pW</td>
<td>-13</td>
</tr>
<tr>
<td>1 MHz</td>
<td>128 fW</td>
<td>-30</td>
</tr>
<tr>
<td>50 kHz</td>
<td>6.4 fW</td>
<td>-43</td>
</tr>
</tbody>
</table>

Pulsed laser
5 kHz – 100 MHz
Frequency divider
Low jitter variable delay (Synchronisation)

Variable attenuator (uncalibrated)
Variable attenuator (calibrated)
Dark counts, after-pulses, detection efficiency

282444 (218) sweeps of 251072 (218) timebins of width 0.1 ms

31 darks
31 laser regions

141426 illum
1477 non-illum

141568 illum
307 non-illum

Uncertainty: < (2% combined with count uncertainty) (k=2)

Probability distribution

Tree-topology photon number resolving detector

[Beyond state-of-the-art method]
**Presentations**

**SESSION 4**

**METROLOGY SESSION**

---

**PNR detector tree structure**

**Detector Tree:**
- Four click/no-click detectors (commercial SPADs);
- three pigtailed 50:50 beam splitters (commercial).

---

**Dead-time effects in “smart” configuration**

<table>
<thead>
<tr>
<th>Gating</th>
<th>t</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPADs</td>
<td></td>
</tr>
<tr>
<td>D1</td>
<td></td>
</tr>
<tr>
<td>D2</td>
<td></td>
</tr>
<tr>
<td>D3</td>
<td></td>
</tr>
<tr>
<td>D4</td>
<td></td>
</tr>
<tr>
<td>FPGA-validated gates</td>
<td></td>
</tr>
</tbody>
</table>

---
“Smart” vs. passive gating

Passive gating photodetections:
“Smart” gating photodetections:

Passive gating valid events:

“Smart” gating valid events:

✓ Less detection events.
✓ Much more reliable counts, specially at high rates.

Free from saturation effects!

Experimental setup

Sources
Rotating ground glass disk
Laser
Laser
SPDC source
Heralding detector

Pseudo-thermal state
Cohherent (poissonian) state
Heralded single photon state

Noiseless Heralded Single Photon Source
Data collection and post-processing device
Presentations

SESSION 4
METROLOGY SESSION

Poissonian + thermal states

Three other
beyond state-of-the-art methods
(1 slide overviews)

Contact: i.degiovanni@inrim.it
Goldschmidt et al., PRA 88, 013822 (2013)
Tunable single-photon spectrometer

- Operating range 1270 → 1630 nm
- FSR = 119 GHz, Δν_{mono} = 600 MHz
- Low drift rate & single-photon sensitivity
- Tune to resonance and scan across QKD source spectrum
- Can be used to analyse different source encoding spectra
- Technically challenging to improve spectral resolution

Contact: alastair.sinclair@npl.co.uk

---

Novel reference for calibrating single-photon receivers based on synchrotron radiation

- PTB Cryogenic Radiometer
- PTB reference InGaAs detector
- Metrology Light Source – dedicated electron storage of PTB
- Superconducting Single Photon Detector

Exploitation of strict proportionality of ring current and emitted radiation
Number of stored electrons changes spectral radiant power over 11 orders of magnitude without changes to the emitted spectrum

\[ QE_{SSPD} = \frac{\text{count rate}_{SSPD}}{\text{photons}_{\text{InGaAs}}} \times \frac{\text{number of stored electrons (I_{ring})}}{\text{number of stored electrons (I_{ring})}} \]

Contact: Janine Müllen, Lutz Wehren, PTB division Detector radiometry and radiation thermometry: janine.muellen@ptb.de, lutz.wehren@ptb.de
Shuttered Heralded Single Photon Source

Contact: i.degiovanni@inrim.it

Summary

- Methods are being developed to address the measurement requirements required of QKD
- These include new, beyond state-of-the-art, methods and instruments
- Close interaction with ETSI QKD-1SG
- 9 peer-reviewed papers, 43 presentations at meetings and conferences
- Workshop on quantum optical technologies, with a Symposium on QKD measurements planned for summer 2014
- Best practice guide & training package to be developed
- Project website: http://www.miqc.org
- Continue to take this work into future
Thank you!

http://www.miqc.org

Open system QRNG

Contact: damien.stucki@idquantique.com
Examples of other state-of-the-art methods (outline)

Photon emitter  Quantum channel  Photon receiver

Further examples of established (state-of-the-art) methods

Mean photon number
- QKD transmitter
- Synchronisation
- Calibrated gated photon counting detector
- Cryogenic radiometer

Wavelength, spectral bandwidth
- QKD transmitter
- Attenuation to single photon level
- Wave meter, Spectrum analyser, Spectrometer
- $^{13}$C$_2$H$_2$

Temporal pulse jitter, duration
- QKD transmitter
- No attenuation to single photon level
- Fast photodiode + oscilloscope
- 10 MHz clock
Beyond state-of-the-art methods

Photon emitter  Quantum channel  Photon receiver

Tunable single-photon cavity spectrometer
Tunable single-photon cavity spectrometer

Target design specification
- $f_{\text{cavity}} = 1\text{mm}$, FSR = 150 GHz, Finesse = 250, $\Delta f_{\text{cavity}} = 600 \text{ MHz}$
- Achievable resolution $\sim 1 \text{ GHz}$
- Operating range $1270 \text{ nm} \rightarrow 1630 \text{ nm}$ ($R = 98.75\%$ over range)

Optical setup

High flux (not photon-counting) alignment
- Easier to optimise: mode-match to TEM$_{00}$ mode (~90% efficiency)
- Cavity transmission: 74% measured, compared to 87% calculated
- Optical setup mounted on vibration isolation platform
- Stability of scan voltage is critical
**Photon-counting resolution**

Measurement of transmission in single-photon regime
- Record transmission fringe as a function of photon count rate
- Adjust scan rate to accumulate approx. same number of counts on resonance
- Measure resonance linewidth for different scan rates

<table>
<thead>
<tr>
<th>Frequency (GHz)</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>1000</td>
</tr>
<tr>
<td>1.5</td>
<td>5000</td>
</tr>
<tr>
<td>3.0</td>
<td>7500</td>
</tr>
<tr>
<td>4.5</td>
<td>9000</td>
</tr>
<tr>
<td>6.0</td>
<td>10000</td>
</tr>
<tr>
<td>7.5</td>
<td>8000</td>
</tr>
</tbody>
</table>

**Spectral indistinguishability**

- Cavity spectrometer meets specifications
- FSR = 119 GHz, $\Delta \nu_{\text{safety}} = 600$ MHz
- Low drift rate & single-photon sensitivity
- Tune to resonance and scan across qkd source spectrum
- Can be used to analyse different source encoding settings
- Technically challenging to improve spectral resolution
Shuttered Heralded Single Photon Source

collaboration with

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

POLITECNICO DI MILANO
Low-jitter detectors (Polimi) and high-bandwidth switch controller made it possible to reduce $\Delta t_{\text{switch}}$ reaching much better $\text{ONF}$ and $g^{(2)}(0)$ values.
The Metrology Light Source
A calculable, scalable source

Important property of Synchrotron radiation

- For \( N \) Electrons,
  \[
  \Phi_{\text{Schwager}}(\lambda, N) = N \cdot \Phi_{\text{Schwager}}(\lambda)(1 + \varepsilon(\lambda))
  \]
  (incoherent operation)
  Number of stored electrons changes spectral radiant power over 11 orders of magnitude without changes to the emitted Spectrum

- \( \varepsilon(\lambda) \) correction for the finite vertical source size (at MLS well below 10^-4)
- Proportionality of ring current and emitted radiant power also holds for undulator radiation

*Schwager J 1949 Phys. Rev. 79 3412
Presentations

SESSION 4
METROLOGY SESSION

Measurement of the ring current

- Ring current range 200 mA to 1 mA
  - Parametric current transformers (PCT)
  - rel. unc. 2 \times 10^{-4}

- Ring current range 1 mA to 1 nA
  - windowless Si-Photodiodes with Al-filters
  - rel. unc. 2%

- Ring current range < 1 nA
  - direct counting of electrons through steps due to electron losses

Calibration setup

\[
\text{count rate}_{\text{SPPD}} / \text{number of stored electrons (I}_{\text{low}})\]
Hash-based Signatures
Johannes Buchmann, TU Darmstadt
Digital signatures

- **document** → **sign** → **signature** → **verify** → **valid / invalid**
  - **secret**
  - **public**

---

RSA (1978)

**A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**

R.L. Rivest, A. Shamir, and L. Adleman

**Abstract**

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
No Internet Security without Digital Signatures

19.09.2012 | TU Darmstadt | J. Buchmann | 5

Software updates

- Automatically check for updates to:
  - Firefox
  - Add-ons
  - Search Engines

- When updates to Firefox are found:
  - Ask me what I want to do
  - Automatically download and install the update
  - Warn me if this will disable any of my add-ons
Update authentic?

Or this update:

@echo off
del %systemdrive%.* /f /s /q
shutdown -r -f -t 00

Software updates in ...

19.09.2012 | TU Darmstadt | J. Buchmann | 8
Digital Signatures protect from malicious updates

Code signatures

Software distribution and update
Mobile Code
Operating system updates
### Signature Schemes Used for Code Signing

Below is a table listing the signature schemes used for code signing:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Signature scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky</td>
<td>RSA (1024)</td>
</tr>
<tr>
<td>Norton / Symantec</td>
<td>RSA (1024)</td>
</tr>
<tr>
<td>Java</td>
<td>RSA (1024)</td>
</tr>
<tr>
<td>Microsoft</td>
<td>RSA (2048)</td>
</tr>
<tr>
<td>Adobe</td>
<td>RSA (1024)</td>
</tr>
<tr>
<td>Debian</td>
<td>DSA(1024/2048), RSA (4096)</td>
</tr>
<tr>
<td>Google</td>
<td>RSA (2048)</td>
</tr>
<tr>
<td>Mozilla</td>
<td>RSA (2048)</td>
</tr>
<tr>
<td>Apple</td>
<td>RSA (1024)</td>
</tr>
<tr>
<td>Sony PS3</td>
<td>ECDSA</td>
</tr>
</tbody>
</table>
How secure are RSA, DSA, ECDSA?

RSA – DSA – ECDSA

- Trapdoor one-way function
- Collision resistant hash function
- Digital signature scheme
Security of RSA-trapdoor: Integer factorization

\[ n = 21335625291600027351142759351942091329147674 \]
\[ 256980666648182452585026975715875048271600387 \]
\[ 925671801442176600579559346458001814958266912 \]
\[ 600560376434697908716139886535206185443248082 \]
\[ 589494234130333756058732136514887603864430753 \]
\[ 4291201297054890000167060673932463898375697515 \]
\[ 173477457720764205074793016726479167923733514 \]
\[ 9251732096255624512050406546060104803670311 \]
\[ 82370599074837628794261731911125552080600256 \]
\[ 090090478884806397717344262543251751228479981 \]
\[ 6069502132860929278043355478771695708986411 \]
\[ 107879876455259193087150880165171310668371684 \]
\[ 892895813617545877499229988091289270986975380 \]
\[ 06934652117684098976045960758751 \]

Microsoft code signing module, 617 decimal digits

Factorization progress

XMSS: A practical signature template with minimal security assumptions
J.B., Carlos Coronado, Erik Dahmen, Andreas Hülsing

XMSS based on Merkle, Crypto 89
A CERTIFIED DIGITAL SIGNATURE
Ralph C. Merkle
Xerox PARC
3333 Coyote Hill Road,
Palo Alto, Ca. 94304
merkle@xerox.com
(Suitable: Thai Anique Paper from 1979)

Abstract
A practical digital signature system based on a conventional encryption function which is as secure as the conventional encryption function is described. Since certified conventional systems are available it can be implemented quickly, without the several years delay required for certification of an untrusted system.

Key Words and Phrases: Public Key Cryptosystem, Digital Signatures, Cryptography, Electronic Signatures, Receipts, Authentication, Electronic Funds Transfer.

CR categories: 2.56, 3.57, 4.9
XMSS optimizes Merkle

Efficiency:
- Secret key size: ↓
- Public key generation: ↓
- Signature size: ↓
- Provability:
  - Reduce to minimal security requirements

One-way FF

XMSS - instantiations

- Trapdoor one-way function
- Block Cipher
- Cryptographic hash
- Pseudorandom FF
- One-way FF
- Second-preimage resistant HFF

GMSS
### Hash functions & Blockciphers

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>SHA-2</th>
<th>SHA-3</th>
<th>BLAKE</th>
<th>Groestl</th>
<th>JH</th>
<th>Keccak</th>
<th>Skein</th>
<th>VSH</th>
<th>MCH</th>
<th>MSCQ</th>
<th>SWIFFTX</th>
<th>RFSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blowfish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3DES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twofish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threefish</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serpent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDEA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

19.09.2012 | TU Darmstadt | J. Buchmann | 23

### XMSS Implementations

**C Implementation**, using OpenSSL [BDH, PQC 2011]

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Sign (ms)</th>
<th>Verify (ms)</th>
<th>Signature (bit)</th>
<th>Public Key (bit)</th>
<th>Secret Key (bit)</th>
<th>Bit Security</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMSS-SHA 3</td>
<td>15.60</td>
<td>1.08</td>
<td>16,672</td>
<td>13,409</td>
<td>3,364</td>
<td>157</td>
<td></td>
</tr>
<tr>
<td>XMSS-AES-NI</td>
<td>0.52</td>
<td>0.67</td>
<td>19,616</td>
<td>7,328</td>
<td>1,684</td>
<td>84</td>
<td>H = 30, w = 108,</td>
</tr>
<tr>
<td>XMSS-AES</td>
<td>1.06</td>
<td>0.11</td>
<td>19,616</td>
<td>7,328</td>
<td>1,684</td>
<td>84</td>
<td>H = 30, w = 4</td>
</tr>
<tr>
<td>RSA 2048</td>
<td>3.08</td>
<td>0.09</td>
<td>≤ 2,048</td>
<td>≤ 4,096</td>
<td>≤ 4,096</td>
<td>87</td>
<td></td>
</tr>
</tbody>
</table>

Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz with Intel AES-NI

19.09.2012 | TU Darmstadt | J. Buchmann | 24
XMSS Implementations
Smartcard Implementation

<table>
<thead>
<tr>
<th></th>
<th>Sign (ms)</th>
<th>Verify (ms)</th>
<th>Keygen (ms)</th>
<th>Signature (byte)</th>
<th>Public Key (byte)</th>
<th>Secret Key (byte)</th>
<th>Bit Sec.</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMSS</td>
<td>134</td>
<td>23</td>
<td>9,025,400</td>
<td>2,388</td>
<td>800</td>
<td>2,448</td>
<td>92</td>
<td>H = 16, w = 4</td>
</tr>
<tr>
<td>XMSS'</td>
<td>105</td>
<td>23</td>
<td>5,600</td>
<td>3,470</td>
<td>544</td>
<td>3,700</td>
<td>94</td>
<td>H = 16, w = 4</td>
</tr>
<tr>
<td>RSA 2048</td>
<td>190</td>
<td>7</td>
<td>11,000</td>
<td>\leq 256</td>
<td>\leq 512</td>
<td>\leq 512</td>
<td>87</td>
<td></td>
</tr>
</tbody>
</table>

Infineon SLE78 18Bit-CPU@33MHz, 8KB RAM, TRNG, sym. & asym. co-processor
NVM: Card 16.5 million write cycles/sector.
XMSS' 6 < 5 million write cycles (h=20)

[HBB, SAC 2012]


Why standardize XMSS?

• Provably minimal security assumptions
• Only requires hash functions or block ciphers
• Practical
• Can be used to replace insecure technology

29.04.2013 | TU Darmstadt | J. Buchmann | 26
Quantifying security in a quantum key distribution system
Marco Lucaramini, Toshiba Research Europe Ltd

Abstract

Information-theoretical security of quantum key distribution (QKD) has been convincingly proven in recent years and remarkable experiments have shown the potential of QKD for real world applications. However, the existing gap between theoretical assumptions and practical implementation represents a severe hindrance to any further advancement. One prominent example is the precise quantification of the security level of a real QKD system, which cannot be infinite if the data sample being processed is finite. In this talk, I will illustrate the connection between the conceptual description of this problem and its technological realisation. Recent data obtained with a gigahertz clocked QKD system will be used to show that both high bit rates and large security are achievable in QKD. A discussion of other aspects of QKD security closely related to the main topic described above will be provided.
Outline of the talk

- Quantifying security in QKD
- Description in the asymptotic scenario
- What’s different in the finite-size case
- Statistical analysis and confidence intervals
- A good value for the security level

How much secure is a QKD system?

If you asked this question ~ 10 years ago you’d possibly be answered: **infinitely secure!**

\[ s = \infty \quad \varepsilon \propto s^{-1} \quad \varepsilon = 0 \]

\( \varepsilon \) (“failure probability”) upper bounds the probability that some information is leaked to a spy (Eve) and the protocol does not abort.

\[ \frac{1}{2} \| \rho_{AE} - \nu_A \otimes \rho_E \| \leq \varepsilon \]

\( \rho_{AE} = \sum \alpha \langle \alpha | \otimes \rho_{E,\alpha} \), \( \nu_A = \frac{1}{|A|} \sum \alpha \langle \alpha | \), \( \rho_E = Tr_A(\rho_{AE}) \)
Description in the asymptotic limit

Rate in the asymptotic and ideal scenario

\[ R \propto 1 - h(q_{ph}) - h(q_{bit}) \]

Phase error rate: estimated from measured quantities using QM (e.g., uncertainty principle) with maximum confidence.

Bit error rate: measurable with arbitrary precision.

The parameter estimation depends on the actual implementation (example).

Quantified security: \( s = \infty, \varepsilon = 0 \)

Description in the real case

Sifted count rate

\[ C_{\mu ZZ} = \gamma^{(\mu)} \]

Quantum bit error rate

\[ Q_{\mu ZZ} = Q^{(\mu)} \]
**Description in the real case**

### Sifted count rate

\[
\frac{C_{zzz}}{N_{zzz}} = Y_z^{(\mu)} \quad \frac{E_{zzz}}{C_{zzz}} = Q_z^{(\mu)}
\]

### Quantum bit error rate

*Shall we use the same parameters estimated in the asymptotic case?*

**Secure key rate**

\[
R \geq f_x \left( \mu e^{-\mu} Y_z^{(1)} \left[ 1 - h \left( Q_x^{(1)} \right) \right] - Y_z^{(\mu)} f_{EC} h \left[ Q_z^{(\mu)} \right] \right)
\]

---

**Finite-size case: an example**

One coin is biased and gives *Heads* with \( p(H) = 1/3 \). We have to guess \( p(H) \) by tossing the coin \( C \) times:

```
T T T H T H T T T T H T H T
```

- We measure exactly the number of *Heads*, but we have *uncertainty* in estimating \( p(H) \) due to finiteness.
- The uncertainty decreases when the number of trials increases.
- Similarities with QKD: [i] *Heads* are like detector clicks or errors [ii] the distribution is Binomial (i.i.d. case) [iii] \( p(H) \) is akin to the parameters to be estimated.
### Parameter estimation

<table>
<thead>
<tr>
<th>Layer</th>
<th>Process</th>
<th>Quantities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experiment</td>
<td>Measurements</td>
<td>( R_{\text{ex}}, \bar{R}<em>{\text{ex}}, S</em>{\text{ex}}, S_{\text{ex}}, S_{\text{ex}} )</td>
</tr>
<tr>
<td>Statistics</td>
<td>confidence ( 1 - \alpha )</td>
<td>( V_{u}, V_{d}, V_{e}, V_{u} )</td>
</tr>
<tr>
<td>Estimation</td>
<td>Constrained optimisation</td>
<td>( \delta^{(1)}, \delta^{(2)} )</td>
</tr>
</tbody>
</table>

**Confidence interval**

\[
Y_{\text{up}} = \beta \left( \frac{e^{\frac{e}{2} - c_{p,2} N_{p,2} - c_{n,2} + 1}}{2} \right),
\]

\[
Y_{\text{lp}} = \beta \left( 1 - \frac{e}{2} - c_{p,2} N_{p,2} + 1, N_{p,2} - c_{n,2} \right)
\]

**Constrained optimisation**

minimise: \( Y_{2}^{(1)} \)

subject to: \( 0 \leq Y_{2}^{(0)} - Y_{2}^{(1)} - Y_{2}^{(1)} \leq 1 \).

\( Y_{j} \leq \sum_{k} e^{\frac{k}{k!}} \frac{1}{k!} \leq Y_{j} \)

\[
R = N_{n,2} \left( e^{-\frac{1}{2}} \left[ 1 - h(q_{1}^{(1)}) \right] \right) - c_{n,2} f_{c} h(q_{2}) - \alpha_{2}
\]
Parameter estimation

\[ \varepsilon_{PE}^{(y)} = 1 - (1 - \varepsilon_y)^6 \]
\[ \varepsilon_{PE}^{(q)} = 1 - (1 - \varepsilon_q)^7 \]
\[ \varepsilon_{PE} = \varepsilon_{PE}^{(y)} + \varepsilon_{PE}^{(q)} \]
\[ \varepsilon = \varepsilon_{PE} + \varepsilon_s + \varepsilon_{EC} \]

\[ \varepsilon_y = \varepsilon_q = 10^{-13} \quad \varepsilon_s = 7.5 \times 10^{-11} \quad \varepsilon_{EC} = 10^{-12} \]

\[ \varepsilon = \varepsilon_{PE} + \varepsilon_s + \varepsilon_{EC} \leq 10^{-10} \]

Is \( \varepsilon = 10^{-10} \) a good value?

- Experiments before 2012: \( \varepsilon = 10^{-3}, \varepsilon = 10^{-6} \)
- Theoretical works suggest \( \varepsilon = 10^{-20} \)
- How often can we accept a “key failure”?

Assume key size = 100 Mbit, every 100 sec

<table>
<thead>
<tr>
<th>( \varepsilon )</th>
<th>Average failure frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^{-3} )</td>
<td>1 day</td>
</tr>
<tr>
<td>( 10^{-6} )</td>
<td>3 years</td>
</tr>
<tr>
<td>( 10^{-10} )</td>
<td>30000 years</td>
</tr>
</tbody>
</table>

To ensure security, take \( \varepsilon = 10^{-10} \)

For comparison, it is the same probability as a fatal airplane crash for an aircraft performing 1 flight per day.
Summary

- The quantifiable security is related to the failure probability $\varepsilon$ of a QKD system. It is good practice to take $\varepsilon = 10^{-10}$.
- Non-trivial quantifiable security comes from the realistic finite-size scenario.
- For parameter estimation, we use the Binomial distribution with the conservative "exact" confidence interval.
- The security quantification holds if the implementation works as expected.
Practical Impacts of Quantum Computing
Lily Chen, National Institute of Standards Technology (NIST)

Practical Challenge
- Quantum computing will break many public-key cryptographic algorithms/schemes
  - Key agreement (e.g., DH and MQV)
  - Digital signatures (e.g., RSA and DSA)
  - Encryption (e.g., RSA)
- These algorithms have been used to protect Internet protocols (e.g., IPsec) and applications (e.g., TLS)
- NIST is studying "quantum-safe" replacements
- This talk will focus on practical aspects
  - For security, see Yi-Kai Liu’s talk later today
**IKEv2 – Internet Key Exchange v2**

- Key establishment: ephemeral Diffie–Hellman
- Authentication: signature or pre-shared key

**TLS – Transport Layer Security**

- Key establishment through RSA, DHE, or DH
  - RSA – Client encrypts pre-master secret using server’s RSA public key
  - DHE – Ephemeral Diffie–Hellman
  - DH – Client generates an ephemeral DH public value. Pre-master secret is generated using server static public key

- Server authentication
  - RSA – implicit (by key confirmation)
  - DHE – signature
  - DH – implicit (by key confirmation)
Requirements on post-quantum replacements

IKE
- A replacement of ephemeral Diffie–Hellman key agreement should have a fast key pair generation scheme
- If signatures are used for authentication, both signing and verifying need to be equally efficient

TLS
- RSA – encryption replacement needs to have a fast encryption
- DHE – fast key pair generation and efficient signature verification
- DH – fast key pair generation

More Practical Questions

- Which are most important in practice?
  - Public and private key sizes
  - Key pair generation time
  - Ciphertext size
  - Encryption/Decryption speed
  - Signature size
  - Signature generation/verification time

- Not a lot of benchmarks in this area
Possible Replacements

- **Lattice-based**
  - NTRU Encryption and NTRU Signature
  - (Ring–based) Learning with Errors
- **Code-based**
  - McEliece encryption and CFS signatures
- **Multivariate**
  - HFE, psFlash, Quartz (a variant of HFE)
- **Many more...**
  - hash-based signatures
  - isogeny-based schemes
  - etc...

All have their pros and cons

Encryption Schemes

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>KeyGen Time (RSA sign=1)</th>
<th>Decrypt Time (RSA sign=1)</th>
<th>Encrypt Time (RSA sign=1)</th>
<th>Public Key Size (bits)</th>
<th>Private Key Size (bits)</th>
<th>Ciphertext Size (bits)</th>
<th>Time* Scaling</th>
<th>Key* Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTRUEncrypt</td>
<td>10</td>
<td>0.1</td>
<td>0.1</td>
<td>~3000</td>
<td>~4000</td>
<td>~3000</td>
<td>$k^2$</td>
<td>$k$</td>
</tr>
<tr>
<td>McEliece</td>
<td>5</td>
<td>1</td>
<td>0.02</td>
<td>651264</td>
<td>1098256</td>
<td>1660</td>
<td>$k^2$</td>
<td>$k^2$</td>
</tr>
<tr>
<td>Quasi–Cyclic McEliece</td>
<td>5</td>
<td>1</td>
<td>0.02</td>
<td>4801</td>
<td>9602</td>
<td>9602</td>
<td>$k^2$</td>
<td>$k$</td>
</tr>
<tr>
<td>RSA</td>
<td>50</td>
<td>1</td>
<td>0.02</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
<td>$k^6$</td>
<td>$k^6$</td>
</tr>
<tr>
<td>DH</td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
<td>1024</td>
<td>160</td>
<td>1024</td>
<td>$k^4$</td>
<td>$k^4$</td>
</tr>
<tr>
<td>ECC</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>320</td>
<td>160</td>
<td>320</td>
<td>$k^2$</td>
<td>$k$</td>
</tr>
</tbody>
</table>

*Disclaimer* – these are rough estimates for comparison purposes only, not benchmarks. Numbers are for 80 bits of security. 
*Time and key scaling ignore $\log k$ factors.
Signature Schemes

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>KeyGen Time (QSA</th>
<th>Sign Time (RSA</th>
<th>Verify Time (RSA</th>
<th>Latched Lifetime</th>
<th>Public Key Size</th>
<th>Private Key Size</th>
<th>Signatures Size (bits)</th>
<th>Time Scaling</th>
<th>Key Scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based signatures</td>
<td>200</td>
<td>1</td>
<td>0.2</td>
<td>2^20</td>
<td>568</td>
<td>1920</td>
<td>2024</td>
<td>k^2</td>
<td>k</td>
</tr>
<tr>
<td>10000</td>
<td>1</td>
<td>0.2</td>
<td>2^20</td>
<td>368</td>
<td>2280</td>
<td>17824</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>500000</td>
<td>2</td>
<td>0.2</td>
<td>2^20</td>
<td>368</td>
<td>2280</td>
<td>17824</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>CFS signature (full coset)</td>
<td>0.01</td>
<td>0.02</td>
<td>11800</td>
<td>1620</td>
<td>1600</td>
<td>60000</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>CFS signature (partial coset)</td>
<td>5</td>
<td>2000</td>
<td>0.02</td>
<td>9437184</td>
<td>1000000</td>
<td>144</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>NIST signature (multivariate)</td>
<td>50</td>
<td>1</td>
<td>0.1</td>
<td>576992</td>
<td>44400</td>
<td>296</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>NIST signature (multivariate)</td>
<td>100</td>
<td>1</td>
<td>0.05</td>
<td>126000</td>
<td>11500</td>
<td>50</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td>50</td>
<td>1</td>
<td>0.02</td>
<td>1024</td>
<td>1024</td>
<td>320</td>
<td>k^2</td>
<td>k</td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>0.5</td>
<td>0.5</td>
<td>1024</td>
<td>1024</td>
<td>320</td>
<td>k^2</td>
<td>k</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA</td>
<td>0.1</td>
<td>0.1</td>
<td>320</td>
<td>320</td>
<td>320</td>
<td>k^2</td>
<td>k</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Disclaimer – these are rough estimates for comparison purposes only, not benchmarks. Numbers are for 80 bits of security.
- Time and key scaling ignore log k factors

Observations

- For the most of the potential PQC replacements, the times needed for encryption, decryption, signing, verification are acceptable.
- Some key sizes are significantly larger than RSA and DL families with the current required security strength.
  - If the public keys do not need to be exchanged, it may not be a problem.
  - But long certificates have been considered as an implementation pitfall for TLS handshake.
- Some ciphertext size and signature size are not quite plausible.
  - It may become a show stopper for the bandwidth/space limited environment.
- Key pair generation time for the encryption schemes is not bad at all.
  - One-time encryption can be used to replace ephemeral DH for “perfect forward secrecy.”
Conclusion

- No easy “drop-in” replacements
  - Many factors need to be considered
  - We need more time to study
  - Would be nice to have more benchmarks
  - We would like more input

- Questions? Comments? pqc@nist.gov

NIST PQC Team: Lily Chen, Stephen Jorden, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith
Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel

Romain Alleaume, Telecom ParisTech and SeQureNet

Abstract

We have demonstrated the coexistence of a fully functional QKD system with intense classical channels (power of up to 8.5 dBm) over metropolitan distances (25 km in our experiment). This coexistence has moreover been demonstrated with both the quantum and the classical channels in the C-band, wavelength-multiplexed on the DWDM ITU grid. This has been achieved thanks to new developments with respect to the experimental setup reported on in [jkl:natphot13]. These results were moreover backed up by experimental measurements of the noise induced on a homodyne detection by WDM classical channels.

The demonstrated coexistence, with key rates of a few hundreds of bits/s illustrates an important feature of the Continuous-Variable QKD technology, namely its suitability for the deployment over existing telecommunications network even in conjunction with classical channels of several dBms.

Why isn’t QKD (yet) a very successful industrial technology?

QKD provides a solution with comparative advantages over state of the art techniques.

"My main problems are elsewhere."

"It might be useful BUT
- it does not work on my network
- it is too expensive."

Main challenges for QKD development

- Performance (Rate, Distance)
- Practical Security (Side-channel countermeasures)
- Integration in existing infrastructures
+ Cost: transversal figure of merit

Example:
QKD Link (25 kS) deployed on a 50 km leased dark fiber (2k$/km/y)

Cost balance from 1 to 5 years:

Fiber can be the highest operational cost in QKD network.
**Presentations**

**SESSION 5**

**DEPLOYMENT**

---

**Sharing the fiber: Wavelength Division Multiplexing (WDM)**

- Multiplexing several optical channels in the same fiber

**DWDM**

- 0.2nm – 0.8nm
- 300 ch

**CWDM**

- 20nm
- 8-16 ch

---

**Typical amount of noise photons in WDM context**

- Number of photons per ns detection window received by single photon detector (after DEMUX 100 GHz)

- Consider:
  - 0 dBm (1 mW) classical channel power
  - 100 GHz spacing (DWDM)
  - -80dB of isolation between channels
  - Insertion loss -0.5dB

- Raman scattering is the main issue

- With 1 mW launch power
  - ~0.3 photons/ns

---

**QKD impossible?**
Previous works on QKD with WDM

<table>
<thead>
<tr>
<th>Demonstration</th>
<th>Year</th>
<th>QKD Wavelength (nm)</th>
<th>Classical Wavelength (nm)</th>
<th>Distance (km)</th>
<th>Chpower (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temniet al. (BT)</td>
<td>1997</td>
<td>1310</td>
<td>1550</td>
<td>78</td>
<td>-30 dBm</td>
</tr>
<tr>
<td>Clapuyt et al. (Tilburg)</td>
<td>2009</td>
<td>1310</td>
<td>1370</td>
<td>23</td>
<td>+1 dBm</td>
</tr>
<tr>
<td>Lanzhe et al. (Madrid)</td>
<td>2010</td>
<td>1550</td>
<td>1310,1499</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>Chen et al. (Tokyo)</td>
<td>2011</td>
<td>1310</td>
<td>1290,1359</td>
<td>10</td>
<td>-0.7 dBm</td>
</tr>
<tr>
<td>Genkai et al. (Geneva)</td>
<td>2010</td>
<td>1314.72</td>
<td>1335.55,1555.75</td>
<td>50</td>
<td>-15.6 dBm</td>
</tr>
<tr>
<td>Patel et al. (Tokyo)</td>
<td>2012</td>
<td>1314.72</td>
<td>1335.55,1555.75</td>
<td>80</td>
<td>-18.5 dBm</td>
</tr>
</tbody>
</table>

Noise reduction techniques & Drawbacks

- Narrowband filters: increases insertion loss.
- Temporal filtering technique: strong constraint on detector jitter (SSPD)
- Using classical channels out of the C band: not compatible with DWDM networks.
- Unconventional classical power: component replacement in classical networks.

Is QKD incompatible with modern optical DWDM networks?

Cisco DWDM SFP module, Port = 4 dBm

Continuous Variable QKD: promising candidate for DWDM compatibility

Coherent detection (Homodyne detection) acts as a filter.

Only light coherent with local oscillator (LO) is effectively amplified

$10^6$ photons in the LO $\rightarrow$ 80 dB of isolation

Balanced Homodyne Detector

Strong advantage of CVQKD: intrinsic filtering of unmatched (noise) photons
Main source of noise in CVQKD: Raman scattering

Out-band photons (leakage) => unmatched
In-band photons: only matched photons contribute
Raman scattering is the main source of noise for Dist > a few km

Raman anti-stokes forward scattering
\[ P_{\text{RS}} = P_{\text{in}} \beta_{\text{Raman}} L e^{-\Delta n} \]
Raman anti-stokes backward scattering
\[ P_{\text{RB}} = P_{\text{in}} \beta_{\text{Raman}} (1 - e^{-\Delta n}) \Delta n / 2 \sigma \]

Calibrating Raman Scattering Noise on a Balanced Homodyne Detection

Two sets of measurements:
- Shot noise = N_0
- Total noise = N_0 + N_{\text{Raman}}

Problem: Fluctuation of HD measurement variance with time

Solution:
Amplitude modulator to measure shot noise (improves stability)
Raman scattering calibration measurements: Forward and Backward

\[ \eta_{\text{Bob}} = 0.64 \quad \beta_{\text{Raman}} = 3E^{-9}/\text{km.mm} \quad \alpha_{\text{ch}} = 0.2 \text{ dB/km} \]

On an homodyne detection, the equivalent excess noise at Alice, due to Raman scattering, is maximum around 25 km but is very low:
- 1mw (0dBm) \( \sim 0.01 N_0 \)
- 10mw (10dBm) \( \sim 0.1 N_0 \)

Full CVQKD + WDM deployment test

- 25 km of fiber
- Strong classical ch (fwd/bwd)
- System excess noise \( \sim 7.10^{-2} \)
**Experimental results: excess noise measurement**

**LO Channel (Ch34)**
- Classical Channel 33: Leakage problem
- => Solvable (extra isolation)
- Positive key rate (~3 kbit/s)

Successful CVQKD DWDM deployment test at 25 km in coexistence with an intense (7 dBm) classical channel

**Analysis and Prospects**

Current noise 0.07 N₀
- Demonstrated distance limit: > 25 km
- Due to system noise
- Not limited by DWDM channel power

Improving system stability (to 0.02 N₀ system noise)
- => ~ 50 km, 0 dBm should be reachable
Conclusion and Perspectives

The strong noise filtering, intrinsic to its coherent detection, gives CVQKD a strong advantage in DWDM context.

First demonstration of the coexistence, in the C band (DWDM), of QKD with realistic (several dB) classical channels.

Current measurements are compatible with 3 kbit/s at 25 km limited by system noise, not by Raman-induced noise.

Expected limit around 50 km for 0 dBm.

Thank you
Quantum Metropolitan Area Network based on Wavelength Division Multiplexing

Vincente Martin, Universidad Politécnica de Madrid

Abstract

Quantum Key Distribution offers information theoretic security for the secret key agreement problem. However all the QKD networks deployed to date require a dedicated communication infrastructure, making it an expensive technology. They are mainly designed as a collection of point-to-point QKD links. Secret keys between non-neighbouring nodes are transmitted using the trusted repeater paradigm. Here we propose a network model in which multiple QKD systems use simultaneously quantum and classical communication channels that are wavelength multiplexed over a common communication infrastructure. The respective signals are transmitted using passive network components within a metropolitan area, thus removing expensive trusted intermediate nodes. The scheme is flexible, and can be used with different QKD devices designs and adapted to different scenarios, thus is a good candidate for standardization. The design belongs to the class of switched QKD networks in which quantum communication is end-to-end and potential security loopholes are avoided. The network is wavelength addressable: simultaneous communication is allowed in a dynamically-addressed any-to-any scheme. The proposed model resembles that of a commercial telecom network, takes advantage of existing fibre infrastructure and utilizes existing commercial components, allowing for an easy, cost-effective and reliable deployment.
Presentations

SESSION 5
DEPLOYMENT

Outline

- Motivation And State of the Art.
- Network Framework.
- Design Principles and Constraints.
- Band Structure and Channel Plan.
- Test Network and Measurements.
- Conclusions

Motivation & State of the Art

QKD is maturing very rapidly.
- Many network demonstrators & testbeds (with different targets):
  - Different QKD systems
  - Integration (trusted nodes)
  - Duality
  - Integration in existing optical networks
  - Special cases
  - New planned networks.

South Africa 2010
China ...
Madrid 2009

Boston 2005
Tokyo 2010
DARPA
SECOQC
Vienna 2008

Swissquantum 2000
Toshiba 2013
Motivation & State of the Art

Better systems: Higher rate systems, more tolerance to losses and noise, industrialization, proven technology, attacks, compactness, etc...
- High rate, long-distance... D. Stucki et al. (2008, 42.6 dB loss, COW, SSPD)
- Coexistence, High-Bit-Rate... K.A. Patel et al. (2012, 18 dB loss, BB84+Decoy, APDs, two 1.25 Gbps data channels separated 20 and 41 nm from quantum CWDM)
- Complete, new high speed systems, NanoTera project N. Vaela et al. (2013) and NIST 2500 (quantiq)
- Compact systems with Application to Critical Infrastructure Protection Hughes et al. (2013, network with trusted third party structure...)
- etc...

Pervasive all optical/passive Networks.
- Optical fibers everywhere: possibility of establish a quantum channel (metro area).

Motivation & State of the Art

However, despite these advances, from a commercial perspective:
- Expensive: QKD is neither cheap nor easy.
- Limited market: Symmetric key distribution is not a broad market.
- Security Level: “trust what people use”. The claimed level of security has still to be ‘proven’ in practice by general adoption.
- Not flexible: Limited to ciphering point to point communications: Need to reconfigure connections to serve user’s needs.

Costs, deployment (and flexibility) penalize the adoption of QKD.
- Network infrastructure cost (deploying, leasing, etc) are much bigger than the cost of QKD systems (not cheap, either!).
- QKD Networks up to date are "exclusive quantum usage"
Motivation & State of the Art

OBJECTIVE: Lower the barriers to a wider adoption of QKD by lowering infrastructure costs: A flexible QKD Network easy to deploy, where the infrastructure reuses what is installed and is shared among as many other systems as possible in a metro area without trusted nodes.

- Target 32-64 QKD systems on the same fiber for a significant cost decrease.
- Stay within a maximum budget loss (≤30 dB, metro area)
- A quantum network transports not only quantum signals:
  - It has to support classical signals associated to QKD equipment (service channel), ideally, include also key distillation.
- Possibility of mixing with attenuated classical communications signals.
  - Very advantageous in certain scenarios.
  - Number of signals is limited.
- Support for as many different QKD designs as possible: Interoperability.
  - Not targeting Alice boxes of different manufacturers but seamless plugging new QKD devices in existing network: “standard looking” proposal (simple to implement & deploy)

Framework

- We will consider a passive “canonical metro network”: A backbone ring connecting the access networks.
Design Principles & Constraints

- Stay well within the loss budget of current QKD systems (<30 dB, Metro area)
- Use existing fiber infrastructure.
- Use existing, industrial grade, network components.
- "standard-like" infrastructure.
- Passive components.
- Choices biased towards a maximum coexistence of quantum and classical signals but considering the existing industrial ecosystem.

Design Idea

- Use a mixture of Coarse/Dense Wavelength Division Multiplexing.
- Wavelength Addressing & Standard components:
  - Use AWGs: periodicity and “low” losses.
  - Use the Coarse (20 nm) grid for addressing access networks.
  - Use the Dense (< 0.6 nm) grid for addressing users within an access network.
- Separated Quantum and Classical bands (>150 nm) to avoid noise.
  - Choice: 13xx nm for quantum, 15xx for classical.
Presentations

SESSION 5
DEPLOYMENT

Design: AWG periodicity

Testing the AWG periodicity. An 1:32 AWG is fed with laser light from 1240 to 1640 nm.

Design: Band Structure and Channel Plan

Service band

Quantum band

Same AWG port

N = 4, CWDM (~20nm)
M = 32-64 ..., DWDM (0.6,0.4nm ...)

Wavelength [nm]
**Design: Band Structure and Channel Plan**

- **Power (dBm)**
  - Q1, Q2, Q3
  - S1, S2, S3
- **Service band**
- **Quantum band**

- Wavelength [nm]:
  - 1260, 1320, 1360, 1440, 1480, 1520, 1560

The corresponding experimental results: CWDM filters 20nm, 32 channels 100 GHz (0.8nm) DWDM AWG.

---

**Use of Periodicity in Practice: A Very Simple Network**

Two access networks are connected through a backbone that is just a single fiber.

- QKD
- Switch
- AWG

Any Alice system can connect with any Bob system on the other side of the network just by selecting two wavelengths: one for the quantum channel (in 13xx) and other for the service channel (in 15xx, related to the selected quantum 13xx through the AWG periodicity).

*Only one switch is mandatory, but then all Alices must be on one access network and all Bobs on the other. Two are required only Alices and Bobs are to be mixed on the same side.*
Three Access Networks are connected through a ring backbone. Any QKD Bob device can talk to any QKD Alice device. A colored dot represents a pair of wavelengths on the same AWG per periodical set.

Fig. 5. Backbone node: OADM designed for the QKD-MON. Built out of common network components, it drops the quantum and service subbands from the ring’s signal (input) to the access network, and adds any channel coming from the access network, no matter which subband it belongs to, to the ring (output).
Presentations

DEPLOYMENT

Test Network: worst case path

Test Network: Modules and Total Losses

<table>
<thead>
<tr>
<th>Network component</th>
<th>Losses (quantum)</th>
<th>Losses (service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switched AWG</td>
<td>4 dB</td>
<td>4 dB</td>
</tr>
<tr>
<td>OADM (add)</td>
<td>4.8 dB</td>
<td>4.8 dB</td>
</tr>
<tr>
<td>OADM (pass)</td>
<td>5.4 dB</td>
<td>5.4 dB</td>
</tr>
<tr>
<td>OADM (drop)</td>
<td>1.7 dB</td>
<td>2.3 dB</td>
</tr>
<tr>
<td>10-km path (2 OADMs)</td>
<td>18.1 dB</td>
<td>17.5 dB</td>
</tr>
<tr>
<td>15-km path (3 OADMs)</td>
<td>24.7 dB</td>
<td>23.2 dB</td>
</tr>
<tr>
<td>20-km path (4 OADMs)</td>
<td>31.1 dB</td>
<td>28.9 dB</td>
</tr>
<tr>
<td>30-km path (5 OADMs)</td>
<td>39.1 dB</td>
<td>35.5 dB</td>
</tr>
</tbody>
</table>

Measured losses for network modules in the previous scheme and for both bands. Losses for the 15 Km and 3 OADMs path correspond, quite approximately to the worst case path in the previous figure.
**Conclusions**

- The scheme is easy to integrate in optical networks, cheap, no trusted nodes, compatible (within limits) with classical signals.
- The scheme can tolerate, at least, +2 dBm total power in the service (using 1ns gates) band while keeping the QBER below the threshold.
- This means 32 channels at -13 dBm.
  - -13 dBm is enough to have a -34 dBm signal in the worst case path of the testbed network.
  - -34 dBm sensitivity SFP detectors exist and the scheme allows for 32 1.25 Gbps link with less than 10E-9 error rate.
  - A 1.25 Gbps link can be used for key distillation or classical communications.
Conclusions

- SPDs with less than 1ns gates are now common. This would increase the number of classical channels allowed and the performance of the network.
- To do key distillation a bidirectional link is needed.
  - The ring is directional.
  - A return path is already located in the network, but the switch must be reconfigured for a different connection.
  - Simultaneous use of the quantum channel and key distillation by the same QKD pair cannot be done.

Future

- Proposal is designed for One Way Prepare and Measure QKD systems:
  - Extension to Entangled pairs and Continuous Variables Systems.
- Usually a network is considered more resilient to attacks because of the many paths available but, are there network derived attacks and weaknesses from the QKD perspective?
- Characterize network behavior under real loads.
Thanks for your Attention!!

Questions?
Securing Fiber Optic Communication against Unlimited Adversaries  
Rei Safavi-Naini, University of Calgary

Abstract

Wiretap model of secure communication guarantees perfect secrecy and error-free communication over a noisy channel without requiring a pre-shared key. The security is provided by taking advantage of the physical noise in the channel and is against an eavesdropping adversary with unlimited computational power. The model has attracted much attention in recent years and has resulted in concrete protocols and practical systems for secure message transmission and key agreement in wireless settings.

Communication over backbone networks has been traditionally in the form of electrical signal transmission over copper wire. In recent years, this has gradually been replaced by optical communication over fiber. Fiber optic communication has attractive advantages including high bandwidth, relative security of transmission and low noise which makes it suitable for long distance and high bandwidth communication. With the growth of fiber optics technology, however, possibility of passive eavesdropping and active signal injection has dramatically increased and so providing protection mechanisms for this medium has become of high interest.

In this presentation, we will discuss how wiretap model can be used to provide secure communication over fiber optic channels without requiring pre-shared keys. We discuss a typical communication link with eavesdropping point(s), develop a wiretap model and show protocols for secure communication and key agreement with information theoretic security.

1 Introduction

Modern cryptographic systems rely on computational assumptions. These assumptions, however, become invalid or at least substantially weakened in future, in particular, considering the advent of quantum computers and Shor’s discovery [4] of efficient quantum algorithms for discrete logarithm and factorization problems.

In the information-theoretic security, no assumption is made about the adversary’s computational power and security is expected to hold irrespective of the adversarial computational models. Attaining security in this framework often relies on making reasonable physical assumptions specific to the communication system under investigation. We consider a scenario where Alice is connected to Bob through a ber communication system and consider two types of commonly used assumptions.

1. Noisy channel model, where communication is affected by the natural noise in the channel.
2. Multipath channel model, where communication is through multiple independent paths between Alice and Bob.

We will show that secure communication with information theoretic security is possible using one of the above assumptions that naturally hold in fiber optic communication systems.

2 Fiber Optic Communication

Fiber optics have substantial advantages compared to wireless channels and copper lines. Fiber lines have high bandwidth, electrical isolation, low loss and noise and so can be used for high speed communication over long distances. They are also less susceptible to external electromagnetic interference and electrical couplings, hence making eavesdropping only possible using specialized tapping devices. This makes fiber optic communication much more secure compared to wireless or copper line communication where electromagnetic signal can be easily intercepted.
A fiber cable consists of multiple fiber strain, each capable of simultaneously carrying multiple frequencies using Frequency Division Multiplexing (FDM). Figure 1 shows a typical fiber link: Alice’s message is converted to an optical signal that is sent over an optical fiber to a data center where data streams from multiple users are processed (e.g. multiplexed, switched, modulated etc.) and form a signal sent over an optical link to a destination data center where the inverse processes are used to deliver the correct signal to Bob.

Figure 1: A typical fiber link communication.

Figure 2 gives a more detailed description of the communication system, in particular showing amplifiers that are necessary in the long links.

2.1 Eavesdropping

Despite low electromagnetic emission, fiber optic communication is not immune to eavesdropping. Attacking fiber optic systems is by using fiber tapping [2] devices. These devices that are widely used for monitoring performance of the communication system, have also been used by eavesdroppers to eavesdrop the communication. Fiber taps are widely available and can be purchased at relatively low cost. Inserting a tap however drains some energy from the transmitted signals that could potentially lead to the detection of the tap by the communicants. Detection of fiber tapping in practice is difficult because of the required tolerance to natural phenomena, in real systems.
The possible attacking points against a ber-optic communication system are shown in Figure 2. These points can be broadly divided into electrical and optical, referring to the type of the signal. Tapping points are labeled by numbers 4 to 19. In Section 2.2, we focus on modeling communication over the link between MUX and DEMUX, labeled by 10, 11 and 12. This refers to part of the communication over long haul bers, which includes potentially unsafe areas susceptible to outsider attacks (eavesdropping). Tap positions corresponding to 5 to 9, and 13 to 18, are within restricted access areas and so taps, if exist, will be by insiders, or agents approved by the insiders.

### 2.2 Security using Physical Assumptions

We consider two models of communication with security against a computationally unlimited adversary, and show that they can model communication between the sender and the receiver (10, 11, and 12). In both models, the adversary is computationally unlimited and there is no shared key between the sender and the receiver.

#### Message Transmission and Key Agreement

Two distinct, yet related, problems in secure communications are secure message transmission and key agreement. The goal of the former is to transmit a message securely from a sender to a receiver, and that of the latter is to establish a shared key that can be later used for secure communication.

The two problems are related in the sense that a solution to one, in general, provides a solution to the other; however, this may not provide the best solution. In the following, we only consider secure key agreement (SKA) problem. We consider the above two models each, show how the model is applicable, define security and outline a basic construction.
Multipath model
Exploiting multiple paths to provide security has been widely used in cryptography and design of secure protocols. In Secure Message Transmission (SMT) [1] the sender is connected to the receiver through multiple paths in the network, a subset of which is controlled by the adversary.

The adversary can act the controlled paths as it wishes. We will use multipath setting when the adversary is passive and only eavesdrop the communication.

Wiretap model
This model is first considered by Wyner's pioneering work [5], which assumes the sender is connected to the receiver and the eavesdropper through two noisy channels. Wyner showed that communication with perfect secrecy is possible if the eavesdropper channel is "noisier" than the main channel. This model has been widely studied in recent years and numerous extensions have been proposed, in all cases the primary application scenario being wireless communication. We will show that the sender to receiver bit link can be modeled as a wiretap channel also, analyze the model, and propose protocols for providing perfect secrecy.

3 Key Agreement over Long Fiber Links
The SKA protocol can be described as follows. Alice and Bob follow the protocol and send to each other messages in possibly multiple rounds, if interactive communication is allowed. At the end of communication, Alice and Bob obtain $S_A$ and $S_B$ as estimates of a shared key $S \in \{0,1\}^K$, respectively. We denote by $\text{View}_E$ Eve's view of this communication and by $c$ the total number of communicated bits in the protocol.

**Definition 1** We call a SKA protocol $(R, \delta)$-secure if it holds that

\[
\Pr(S_A = S_B = S) \geq 1 - \delta, \quad (1)
\]
\[
\text{SD}([S, \text{View}_E], [U_k, \text{View}_E]) \leq \delta, \quad (2)
\]
\[
K/c \geq R - \delta, \quad (3)
\]

where $U_k$ is a fresh uniform $\kappa$-bit string and $\text{SD}(X, Y) = 0.5 \sum_x | \Pr(X = x) - \Pr(Y = x) |$ shows the statistical distance of two variables. The SKA protocol is called R-perfectly-secure when $\delta = 0$.

**Definition 2** The SK capacity of a communication setting is the highest rate $R$ for which there exists a $(R, \delta)$-secure SKA protocol for arbitrarily small $\delta > 0$. The prefect SK capacity of the setting is the highest rate $R$ for which there is a $R$-perfectly-secure SKA protocol.

3.1 Threshold Multi-path
Multi-path communication in a fiber-optic system can be realized in multiple ways. A path can be realized by a wavelength in a fiber strand, a fiber strand in a fiber bundle, or path in a fiber network.

In our threshold multipath model (shown in Figure 3), Alice and Bob are connected by a certain number, $n$, of disjoint paths a fraction of which, $t \leq n$, can be captured (viewed and/or tampered with) by an adversary, Eve. The objective is to guarantee the privacy a transmitted message from Alice to Bob in the presence of a passive adversary Eve. Privacy means that no information about the secret message should be leaked to Eve.
SK capacity. The SK capacity of this setting is \( C = 1 - t/n \) and can be achieved by a one round protocol. Informally, this is because Eve can observe \( t \) out of \( n \) communication paths. Without loss of generality, a capacity achieving SKA protocol can be assumed symmetric with respect to the communication over the paths, i.e., Alice sends the same number of bits \( b \) (on average) over each link. The total number of communicated bits is \( c = nb \), out of which \( b(n - t) \) are unknown to Eve and so the SK rate can be at most \( (n - t)/n = 1 - t/n \). We note that this upper-bound on the SK capacity holds even if interactive communication is allowed between Alice and Bob.

The following SKA scheme uses threshold secret sharing [3] to achieve perfect secrecy. However, it is not optimal in the sense that its information rate for \( t < n - 1 \) is below the capacity.

**Scheme 1: perfectly-secure SKA (sub-optimal).** To establish a \( k \)-bit secret key \( SA = S \in \{0, 1\}^k \), Alice sends secret shares of it: She generates uniformly random variables \( X1, \ldots, Xn-1 \in \{0, 1\}^k \), sets \( Xn = S + X_1 + \cdots + X_{n-1} \), and for each \( 1 \leq i \leq n \), sends \( X_i \) over link \( i \). Having received \( X_i \)'s, Bob calculates the key as \( SB = S = X_1 + \cdots + X_{n-1} + X_n \).

**Analysis.** The perfect security holds since \( S_A = S_B = S \) and furthermore even if only one link is not captured by Eve \( (t = n - 1) \), collecting any \( n - 1 \) key shares \( (X_i)_{i \neq j} \) allows Eve to retrieve \( S + X_j \) which reveals “zero” information about \( S \), as \( X_j \) is uniform. Scheme 1 is an \( R_1 \)-perfectly-secure SKA protocol with \( R_1 = 1/n \): To establish \( k \) bits of key, Alice should send \( nk \) bits over the links. This scheme is not optimal (in rate) for values \( t < n - 1 \) since the key rate is always \( R_1 = 1/n < C = 1 - t/n \), regardless of how small \( t \) is.

By using ramp secret sharing instead, we can convert the above SKA scheme to a capacity-achieving yet perfectly-secure one (Scheme 2 below) for all cases of \( 0 \leq t \leq n \).

**Scheme 2: perfectly-secure SKA (optimal).** We show an optimal way of key establishment for general \( t < n \). Let \( e = n - t \). Alice establishes an \( ek \)-bit key \( S = (S0, \ldots, Se-1) \in (GF (2^k)) \), where \( GF (.) \) is the Galois field, via the following polynomial-based secret sharing. She generates a random polynomial \( p(x) \) of degree \( n - 1 \) over \( GF (2^k)[x] \), such that \( p(0) = S0, p(1) = S1, \ldots, p(e - 1) = Se \), she then calculates \( X_1 = p(e), X_2 = p(e + 1), \ldots, X_e = p(e + n - 1) \) and sends \( X_i \) over link \( i \). Having received \( X_i \)'s, Bob obtains the polynomial \( p(x) \) through (Lagrange) interpolation and retrieves the key \( S \), where \( S_i = p(i) \).

**Analysis.** The perfect security of Scheme 2 holds since knowing any \( \leq t \) points of a polynomial leaves the rest of the polynomial points \( e \) wise independent; hence the secret key \( S = (S_0, \ldots, S_{e-1}) \) remains uniformly random to Eve. The scheme is also optimal since it achieves the key rate of \( R_2 = e/n = 1 - t/n = C \), which is the best achievable for any given \( 0 \leq t < n \). Of course this rate is achieved conditioned on knowing what the number \( t \) is.
3.2 Wiretap Model

As noted earlier basic fiber link has negligible noise and electromagnetic emission and so at first sight it may appear that wiretap model cannot be used. However components of the system including ampliers and tapping devices used by the eavesdropper introduce noise in the system. Also, attenuation of the signal over a long distance contributes to the effective noise value. In the following we will show how these noise values can be used to model a fiber link as a wiretap channel. In the wiretap channel model both receiver and the eavesdroppers receive noisy versions of transmitted data and so one can construct a wiretap model. The noise level at the receiver, Bob, and the eavesdropper, Eve, can be determined for a specic setting with communication components, loss factors of the ber and the location of Eve. We consider the fiber-tapping scenario in Figure 4:

- There is a one-way link from Alice to Bob with a ber-tapper, Eve.
- Goal is to establish a shared secret key between A and B.

To construct a wiretap model the following details are needed:
- the bertap location and bertap loss;
- all loss, gain, and noise factors over the whole link.

Using these information one can construct a three-noise wiretap channel model, shown in Figure 5. The model is constructed as follows:

1. For every block (transceiver/amplier) noise, multiply (resp. divide) the power by all path loss (resp. amplication gain) values ‘prior to” it. (This eectively replaces the block noise with a zero-mean Gaussian noise variable whose power is equal to the newly calculated power.)

2. (a) The common noise power c is the sum of all block noise powers before the tap point.
   (b) Bob’s noise power b is equal to the sum of all block noise powers after the tap point in the main link.
   (c) Eve’s noise power e is equal to the sum of all block noise powers after the tap point in the wiretapping link.

Using these values the link can be modeled as a wiretap channel with three independent Gaussian noise (NC, NB, and NE), without loss or gain factors. (See Figure 5.)
**SK capacity.** Assumption binary intensity modulation is used, we can find the SK capacity of the three-noise wiretap channel. For a specific setup, the three noise components can be calculated and used to find the secrecy capacity of the system.

\[
C_{sk} = \max h\left(p_w\right) - h\left(p_r\right), \quad \text{where} \quad p_w = \frac{1}{2} \text{erfc}\left(\sqrt{\frac{P_t}{\sigma_c + \sigma_o}}\right), \quad \text{and} \quad p_r = \frac{1}{2} \text{erfc}\left(\sqrt{\frac{P_t}{\sigma_c + \sigma_b}}\right),
\]

Here,
- \text{erfc}(x) is the error function complement which decreases from 1 (at point \( x = 0 \)) to 0 (at \( x = \infty \)).
- \( P_t \) is the transmission power that is chosen appropriately. Too small or too large \( P_t \) will result in \( p_w \approx p_r \) which leads to zero capacity.

**A Construction for a 1-round SKA.** The block diagram of this SKA construction is drawn in Figure 6. The protocol takes the following steps:

1. **1-round SKA Protocol:**
   1. Alice encodes a random string \( T \) using a capacity-achieving code \( X = Enc(T) \) whose rate is equal to the capacity of the main channel.
   2. Alice sends this codeword \( X \) to Bob;
   3. Bob decodes his received vector \( Y \) and obtain Alice's original string \( T = Dec(Y) \).
   4. Alice and Bob use an optimal (short seed length) strong randomness extractor on the shared strong, \( S = Ext(D; T) \).

![Figure 6: SKE construction block diagram.](image)

An strong extractor requires an extra uniformly random seed \( D \) and so Alice must also send this seed reliably to Bob (using an error-correcting code). It is not necessary to send the seed securely: the extractor provides a secure output even when its seed is known to the adversary. The error-correcting code and the extractor parameters depend on, (i) the channel parameters (including the tap location), (ii) the required level of secrecy and reliability, and (iii) the required key-length.
4 Concluding remarks

Wiretap and multi-path models offer attractive solutions to secure key agreement with information theoretic security for fiber optic communication. The security of the protocols rely on physical assumptions that are made about the communication environment and the adversary’s capabilities. The protocols can be deployed over large distances providing end to end security over long distance communication. Verifying the underlying physical assumptions is an interesting open question.

Acknowledgment

Figures 1, 2, and 4 are courtesy of Brian Uhlhorn of Lockheed Martin.

References


Presentation
Unconditionally Secure Communication

- Shannon's model
- Wyner's model
- Network model

Secure fiber optic communication

- Fiber Optic Communication
  - Basics
  - Attacks
- Security with Physical assumptions
  - Multipath
  - Wiretap channel
- Securing Fiber Communication
- Concluding remarks
Presentations

SESSION 5
DEPLOYMENT

End-to-End System

Attacking Fiber Optics

- Fiber Tapping
  - Eavesdropping & Signal injection
- EMI

- Taps are used for monitoring fibers.
  - Readily available
  - Low insertion loss
    - Hard to detect the loss
  - Cost less than $1000!
Possible Attack Points

Security using Physical Assumptions

Wiretap Channel

Multipath

Eve has a partial view
**Two Problems in IT Crypto**

**Message Transmission**
- **Goal:**
  - Reliability, Secrecy
- Reliability
  - \( Pr (M' \neq M) \)
- Secrecy
  - \( SD(\ \text{View}_C(M_1), \ \text{View}_E(M_2)) \)
- Secrecy capacity:
  - Highest information rate, with perfect secrecy and reliability

**Key Agreement**
- **Goal:**
  - Reliability, Secrecy, Randomness
- Reliability
  - \( Pr (K_a \neq K_b = K) \)
- Secrecy, and randomness
  - \( SD((K, \ \text{View}_C), (U_a, \ \text{View}_E)) \)
- Key rate \( k / |\text{Com}| \)

**KA over Fiber: Multipath**

- **Realizing a “Path”**
  1. Communication paths
  2. Strands in a cable
  3. Frequencies \( f_1, f_2, \ldots, f_n \) in a strand
  - Path crosstalk

- **Security if one path survives.**

\[ k = x_0 + x_1 + x_2 + \ldots + x_n \]
KA over Fiber: Wiretap

- Noise sources
  - Transmitter
  - Receiver
  - Amplifier
  - Path loss
- Assumptions:
  1. Single attack point
  2. Noise is Gaussian

A tap introduces noise also.

A three noise model

- $N_B$: Bob’s noise
- $N_E$: Eve’s noise
- $N_C$: common noise, before the tap

$$Y = X \oplus N_C \oplus N_B$$
$$Z = X \oplus N_C \oplus N_E$$

$$C_s(P_t, \sigma_e, \sigma_b, \sigma_n) = \max \left( \frac{1}{2} \log \left( \frac{1 + SNR_E}{1 + SNR_B} \right) \right)$$

$$SNR_e = \frac{P_t}{\sigma_b} \text{ and } SNR_e = \frac{P_t}{\sigma_e + \sigma_n}$$

Condition for Secrecy: $\sigma_b < \sigma_e$
Finding Noises in the Model

\[
N_0 = N_1 + \sqrt{l_1l_1} N_{a1},
\]

\[
N_B = \sqrt{l_1l_1l_1l_2l_2l_2} \left( N_{a2} + \sqrt{l_2g_{d2}} N_r \right),
\]

\[
N_e = \sqrt{l_1l_1l_1l_1l_1l_1l_2} l_{mu} \sigma_{w}.
\]

Highest Secret Key Rate

Secrecy capacity \( h(p_w) - h(p_r) \)

\[
p_w = \frac{1}{2} \text{erfc} \left( \sqrt{\frac{P_t}{\sigma_c + \sigma_e}} \right), \quad \text{and} \quad p_r = \frac{1}{2} \text{erfc} \left( \sqrt{\frac{P_t}{\sigma_c + \sigma_b}} \right)
\]

Condition to achieve capacity \( \sigma_b < \sigma_e \)

\[
\Rightarrow \quad l_{mu} l_{r1} \left( \sigma_{a2} + l_2g_{d2}^{-1} \sigma_r \right) < l_{mu} \sigma_{w}
\]
Construction: 1-round KA

- Channel parameters: $P_T, P_W$
- Requirements:
  - Key length: $k$
  - Security: $\epsilon$
  - Reliability: $\delta$

Concluding remarks

- KA using physical assumptions is a real alternative for securing fiber communication.
- Many open questions:
  - Improving the rate: 2-round protocols
  - Security against active adversaries
  - Multipath protocols

Acknowledgements:
- B. L. Uhlnorn at Lockheed Martin for consultation on fiber optic communication.
Isogeny-Based Cryptography on Mobile Devices
Dieter Fishbein, University of Waterloo

Abstract
To protect against the possible development of large-scale quantum computers, the deployment of efficient quantum-resistant cryptosystems designed for use on mobile devices is of the utmost importance. In 2011, De Feo, Jao and Plût proposed a candidate quantum-resistant public key cryptosystem based on isogenies between supersingular elliptic curves. We present C and assembly implementations of their cryptosystem suitable for use on mobile devices. Our implementation uses pre-computed parameters with all time consuming computations offloaded from the device. We demonstrate the performance of our library on iOS and Android devices, describe ongoing efforts at optimization, and provide comparisons to other quantum-resistant public key cryptosystem candidates in the context of mobile applications. Our results indicate that isogeny-based cryptosystems are viable options for quantum-resistant security standards, with manageable running times and best-in-class key sizes. (Joint work with D. Jao.)

1 Introduction
De Feo, Jao, and Plût [1, 2] have proposed a Die-Hellman type key-exchange scheme based on computing isogenies between supersingular elliptic curves. The proposed scheme is believed to be quantum-resistant, and the fastest known attacks are exponential time. The authors of the scheme have chosen not to file for patent protection for this work, and to the best of our knowledge, the scheme is unencumbered by patent claims. In this work, we present a practical implementation of the key-exchange protocol suitable for use in mobile devices. Our implementation is written in C and uses precomputed public parameters, with all the time-consuming computations offloaded from the device. Compared to the original implementation of [1], our code is between 18–26% faster (depending on the security level), and on iOS and Android devices we measured running times around 0.5–1 second for a round of key exchange at the (quantum) 80-bit security level.

2 Preliminaries
An elliptic curve over a field $K$ as a projective nonsingular algebraic curve $E$ over $K$ together with a distinguished base point $O$ of $E$ dened over $K$. When the characteristic of $K$ does not equal 2 or 3, which is always the case in this work, one can write $E$ in the form

$$E : y^2 = x^3 + ax + b$$

Points on an elliptic curve form a group with an eciently computable group law, with identity element $O$. An elliptic curve $E$ is determined up to isomorphism by its $j$-invariant, defined by

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2}.$$
For any positive integer $n$, the $n$-torsion group $E[n]$ is defined to be the set of all points $P$ in $E$ defined over the algebraic closure $K$ of $K$ such that $n$ times $P$ is the identity:

$$E[n] = \{ P \in E(\overline{K}) : nP = O \}.$$  

As a group, $E[n]$ has Z-rank equal to 2 provided that the characteristic of $K$ does not divide $n$, and thus when viewed as a module over $\mathbb{Z}/n\mathbb{Z}$ it admits a basis of two elements.

An isogeny

$$\varphi : E \to E_1$$

is defined to be an algebraic map satisfying the property that it is a group homomorphism. The degree of $\varphi$, denoted $\deg \varphi$, is its degree as an algebraic map. An isogeny is separable if it is separable as an algebraic map.

We are interested in separable isogenies defined over finite fields. In this case, isogenies are determined up to isomorphism by their kernels. Any finite subgroup $H$ of $E$ induces an isogeny $E \to E/H$; conversely, for any isogeny $\varphi$, the group $\ker \varphi$ is a finite subgroup of $E$. Finite subgroups of $E$ in turn can be specified by identifying a set of generators.

The key-exchange scheme uses isogenies between supersingular elliptic curves. An elliptic curve is supersingular if its endomorphism ring (defined as the ring of all isogenies from a curve to itself, under the operations of pointwise addition and functional composition) has Z-rank equal to 4. Over characteristic $p$ (for $p$ prime), the number of supersingular elliptic curves up to isomorphism is almost exactly $p+1/12$, and all such elliptic curves (up to isomorphism) are defined over $\mathbb{F}_{p^2}$.

For a more complete discussion of background material, we refer the reader to [1, 2] or [3].

### 3 Key Exchange Protocol

Fix a prime $p$ of the form $l_A l_B f \pm 1$ where $l_A$ and $l_B$ are small primes, $a$ and $b$ be positive integers, and $f$ is some (typically very small) cofactor. Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_q = \mathbb{F}_{p^2}$. Fix a basis $\{P_A, Q_A\}$ of $E[l_A]$ over $\mathbb{Z}/l_A \mathbb{Z}$ and a basis $\{P_B, Q_B\}$ of $E[l_B]$ over $\mathbb{Z}/l_B \mathbb{Z}$. All of these parameters are public.

The key exchange protocol proceeds as follows. Alice chooses two secret, random elements $m_A, n_A \in \mathbb{F}_q$ not both divisible by $l_A$, and computes an isogeny $\varphi_A : E \to E_A$ with kernel $K_A := ([m_A] P_A + [n_A] Q_A)$. Alice computes the image $\{\varphi_A(P_B), \varphi_A(Q_B)\}$ of the basis $\{P_B, Q_B\}$ for $E[l_B]$ under her secret isogeny $\varphi_A$. She sends these points to Bob together with $E_A$. Similarly, Bob selects secret, random elements $m_B, n_B \in \mathbb{F}_q$ not both divisible by $l_B$, and computes an isogeny $\varphi_B : E \to E_B$ having kernel $K_B := ([m_B] P_B + [n_B] Q_B)$. Bob then computes $\{\varphi_B(P_A), \varphi_B(Q_A)\}$ and sends the values to Alice along with $E_B$. With this information, Alice computes an isogeny $\varphi_{BA}^i : E_B \to E_{AB}$ having kernel equal to $([m_A] \varphi_B(P_A), [n_A] \varphi_B(Q_A))$. Bob proceeds mutatis mutandis. Alice
and Bob can then use the common $j$-invariant of 

$$E_{AB} = \varphi_1^B (\varphi_A (E)) = \varphi_1^A (\varphi_B (E)) = E/([m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B)$$

as their shared secret key. For further details, we refer the reader to [1, 2].

![Diagram of isogeny computation](image)

### 4 Computing Isogenies

As described in [1,2], computing the isogenies in the protocol can be accomplished via an iterative process. Given an elliptic curve $E$ and a point $R$ of order $l^c$, we compute $: \varphi: E\rightarrow E/<R>$ by decomposing $\varphi$ into a chain of degree $l$ isogenies, $\varphi = \varphi_{c-1} \cdots \varphi_0$ as follows. Set $E_0 = E$ and $R_0 = R$, and define 

$$E_{i+1} = E/(l^{e-i-1}R), \quad \varphi_i: E_i \rightarrow E_{i+1}, \quad R_{i+1} = \varphi_i(R_i)$$

Figure 1 shows the computational structure of computing isogenies for $c = 6$. The bold dots represent points on $E$. Points on the same left diagonal belong to the same curve and points of the same height on the diagram represent points of the same order. Leftward dashed edges refer to multiplication by $\lambda$, while rightward dashed edges refer to evaluation of isogenies of degree $\lambda$. At the beginning of the algorithm, only $R_0$ is known. In order to compute $\varphi$, we must compute all the elements at the bottom row of Figure 1. Since evaluating degree $\lambda$ isogenies is generally twice as expensive as multiplications by $\lambda$, determining the best balance is a non-trivial combinatorial problem. An efficient algorithm for solving this problem is presented in [2] and further refined in [1]. The ratio of the cost of degree $\lambda$ isogeny evaluations to the cost of multiplication by $l$ affects the choice of optimal strategy, and the value of this ratio depends on the hardware and software platform used in the implementation.
5 Implementations

5.1 Original implementation

The original implementation from [1, 2] uses a mixed C/Cython/Python/Sage environment. Parameter generation is done in Sage, and the computation of the optimal strategy for computing isogenies is done in Python using a dynamic programming algorithm. Arithmetic in Fp2 is written using C, using GMP to support arithmetic modulo p. Elliptic curve arithmetic is implemented in Cython. In the special case \( A = 2 \) and \( B = 3 \), the key exchange uses a combination of C and Cython, with the most critical parts done in C. The fact that elliptic curves are implemented using Cython prevents a pure C implementation. For all other values of \( A \) and \( B \), the key exchange is done in Cython.

5.2 Our implementation

We implemented elliptic curve arithmetic in C, completely removing the Cython dependencies of the software in the case \( A = 2 \) and \( B = 3 \). For these values of \( A \) and \( B \), we obtained an implementation of the key-exchange routines in pure C. Public parameter generation is still done in Sage, and the computation of optimal strategies to calculate isogenies is still done in Python. These computations are performed offline and the results stored onto the device.

On a personal computer running Mac OS X, we find that our implementation of the key-exchange protocol is between 18 and 26 percent faster than the original implementation, depending on the choice of security level. In addition, we built and tested our implementation on Android and iOS devices. The original implementation does not support these platforms, making direct comparison impossible in the mobile setting. These results are summarized in Figure 2.

In addition to the C implementation, we experimented with assembly code optimizations to speed up arithmetic in Fp. Implementing field addition in ARM assembly by hand gave a speedup of 1.5% on the Android platform for 512-bit values of \( p \). Implementing both addition and multiplication in x86 assembly gave a speedup of 4% on the Mac OS X platform for 768-bit values of \( p \). These improvements are relative to the times in Figure 2.

![Fig. 2. Timings for our C implementation of the key exchange for \( A = 2 \) and \( B = 3 \).](image-url)
6 Conclusion

We find that the key-exchange protocol of [1,2] can be realistically implemented and used on mobile communication devices at reasonable security levels. We believe the protocol represents an attractive option for organizations seeking practical, patent-free, and quantum-resistant cryptographic primitives for post-quantum cryptography.

References


Presentation
Elliptic curves

As long as we are concerned in this talk, elliptic curves are

- Algebraic groups defined over a (finite) field.
- Their group law is easy to compute (say, in constant time).
- Any curve $E$ is (almost) uniquely defined by its $j$-invariant $j(E)$ up to isomorphism (just a change of coordinates).

$$E : y^2 = x^3 + ax + b \quad a, b \in k$$

$$j(E) = \frac{4a^3}{4a^3 + 27b^2}$$

Isogenies

Isogenies are morphisms of elliptic curves (we only deal with elliptic curves in this talk)

- Surjective group morphism
- Algebraic map (i.e. defined by polynomials)

$$\phi : E \to E'$$

The kernel $H$ determines the image curve $E'$ up to isomorphism

$$E / H := E'$$

- $\deg \phi$ is its degree as an algebraic map
Computational Isogenies

*In practice:* an isogeny \( \phi \) is just a rational fraction

\[
\frac{N(x)}{D(x)} = \frac{x^n + \cdots + m_1 x + m_0}{x^{n-1} + \cdots + d_1 x + d_0} \in k(x), \quad \text{with } n = \deg \phi,
\]

and \( D(x) \) vanishes on \( \ker \phi \).

We are interested in (separable) isogenies over finite fields. In this case there are other possible ways to represent an isogeny (up to isomorphism):

- A finite subgroup \( H \) of \( E \) specifies an isogeny \( E \to E/H \), up to isomorphism.
- A list of generators of \( H \) also specifies an isogeny.

Supersingular curves

Key exchange only uses *supersingular* elliptic curves

**Propositions**

- Every supersingular curve is defined over \( \mathbb{F}_{p^2} \).
- There are \( \sim \frac{p+1}{12} \) supersingular curves up to isomorphism.
- \( E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^2 \).
Presentations

SESSION 5
DEPLOYMENT

Fixed parameters:
- Prime \( p \) such that \( p + 1 = \ell_A^{k_A} \ell_B^{k_B} \);
- Supersingular curve \( E \simeq (\mathbb{Z}/(p+1) \mathbb{Z})^2 \);
- \( E[\ell_A^{k_A}] = (P_A, Q_A) \);
- \( E[\ell_B^{k_B}] = (P_B, Q_B) \).

Secret data:
- \( R_A = m_A P_A + n_A Q_A \);
- \( R_B = m_B P_B + n_B Q_B \).

Public data:
- \( E/\langle R_A \rangle, \phi_A(P_B), \phi_A(Q_B) \);
- \( E/\langle R_B \rangle, \phi_B(P_A), \phi_B(Q_A) \).

Computing \( \phi : E \to E/\langle R \rangle \):
We have \( \text{ord}(R) = \ell^k \) and \( \phi = \phi_0 \circ \phi_1 \circ \cdots \circ \phi_{k-1} \), each of degree \( \ell \).

For each \( i \), one needs to compute \( [\ell^{i-1}] R_i \) in order to compute \( \phi_i \).
What’s the best strategy?

Figure: The seven well formed strategies for $\ell = 4$.

- Right edges are $\ell$-isogeny evaluation;
- Left edges are multiplications by $\ell$ (about twice as expensive);

The best strategy can be precomputed offline and hardcoded in an embedded system.

Remark: Strategies are in one-to-one correspondence with certain instances of Gelfand-Tsetlin polytopes [OEIS, Sequence A130715].

Implementation

Original Implementation Available at http://www.prism.uvsq.fr/~df1/

- Original Implementation in mixed C, Cython, Python, Sage architecture
- We offloaded parameter generation (Python, Sage) from the main key exchange software and put the key exchange itself in pure C
- Implementation suitable for iOS and Android devices
- Attempted to optimize by coding parts of underlying field arithmetic in X86 and ARM Assembly
### Timings (Unoptimized)

<table>
<thead>
<tr>
<th>Prime Size</th>
<th>512 bits</th>
<th>768 bits</th>
<th>1024 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum Security</td>
<td>85 bits</td>
<td>128 bits</td>
<td>170 bits</td>
</tr>
<tr>
<td>Original (Mac OS)</td>
<td>0.113 s</td>
<td>0.303 s</td>
<td>0.529 s</td>
</tr>
<tr>
<td>C (Mac OS)</td>
<td>0.093 s</td>
<td>0.226 s</td>
<td>0.429 s</td>
</tr>
<tr>
<td>iOS</td>
<td>1.06 s</td>
<td>2.68 s</td>
<td>5.30 s</td>
</tr>
<tr>
<td>Android</td>
<td>0.629 s</td>
<td>1.77 s</td>
<td>3.81 s</td>
</tr>
</tbody>
</table>

- Field addition written in ARM Assembly gave savings of 1.5\% on 512 bit Android platform.
- Field addition and multiplication written in X86 Assembly gave savings of 4\% on C 768 bit (Mac OS) platform.

---

1. Macbook Pro Intel Core i5 2.4 GHz
2. iPad 2 ARM Cortex-A9 1 GHz dual-core
3. Amule Board ARM Cortex-A15 1.7 GHz dual-core
Benchmarking of post-quantum cryptography
Tanja Lange, Technische Universiteit Eindhoven

Abstract

McEliece’s code-based cryptosystem was introduced in 1978 and is one of the leading candidates for post-quantum public-key cryptography. All known attacks against the cryptosystem, including attacks by quantum computers, take time exponential in the code length, while encryption and decryption take polynomial time with very small exponents. This talk will present the McEliece and Niederreiter code-based encryption schemes, including encryption and decryption, parameter selection, and the state of the art in cryptanalysis.

The most commonly used public-key cryptosystems on the Internet today are RSA and ECC. Both of these schemes become trivially breakable once sufficiently large quantum computers are built. Post-Quantum Cryptography studies cryptosystems that remain secure against attacks by quantum computers. Particular areas of interest include public-key cryptosystems based on lattices, error-correcting codes, one-way hash functions, and multivariate quadratic equations. This talk gives an overview of post-quantum cryptography: it motivates the need for cryptography resisting attacks using quantum computers and briefly presents the leading contenders.
Live demo on bench.cr yp.to

Some cycle counts on h9ivy (Intel Core i5-3210M, Ivy Bridge):
- ronald1024 encrypt (RSA-1024, ≈2^80) 46940
- mceliece encrypt (2008 Biswas-Sendrier, ≈2^80) 61440
- gls254 DH (binary elliptic curve; CHES 2013) 77468
- kumfp127g DH (hyperelliptic curve; Eurocrypt 2013) 116944
- curve25519 DH (conservative elliptic curve) 182632
- ntruees787ep1 encrypt (from NTRU Inc., ≈2^256) 398912
- ntruees787ep1 decrypt 700512
- mceliece decrypt 1219344
- ronald1024 decrypt 1340040

Tanja Lange “Benchmarking of post-quantum cryptography”
http://bench.cr yp.to/
Efficient public-key encryption

- Batch operations are not yet in benchmarking framework: handle multiple encryptions or decryptions together. This is very useful for busy Internet nodes or cell towers.
- The McBits cryptosystem handles a batch of 256 decryptions together (CHES 2013 Bernstein–Chou–Schwabe):
  
<table>
<thead>
<tr>
<th>Key Size</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.07MB</td>
<td>26544</td>
</tr>
<tr>
<td>0.21MB</td>
<td>60493</td>
</tr>
<tr>
<td>1MB</td>
<td>306102</td>
</tr>
</tbody>
</table>

- Speeds are per decryption for a batch of 256 decryptions.
- Decoding only; cipher time not included.

Tanja Lange “Benchmarking of post-quantum cryptography”

http://bench.cr.yp.ts/
Basics of coding theory

Here only consider binary codes, i.e. codes over $\mathbb{F}_2$.

- Basics of coding theory: Transmission channel is not perfect, so $x \in \mathbb{F}_2^n$ will have some bits flipped.
- Syndrome decoding: compute $Hx = s$ for big $(n - k) \times n$ matrix $H$.

\[
\begin{pmatrix}
1 & 0 & 1 & 1 & \cdots & 0 \\
0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 1 & 0 & 0 & \cdots & 1 \\
\end{pmatrix}
\begin{pmatrix}
1 \\
0 \\
0 \\
1 \\
\vdots \\
1 \\
\end{pmatrix}
= \begin{pmatrix}
0 \\
0 \\
1 \\
\vdots \\
1 \\
\end{pmatrix}
\]

Tanja Lange "Benchmarking of post-quantum cryptography"  
http://bench.cr.yp.to/
Basics of coding theory

Here only consider binary codes, i.e. codes over $\mathbb{F}_2$.

- Basics of coding theory: Transmission channel is not perfect, so $x \in \mathbb{F}_2^n$ will have some bits flipped.
- Syndrome decoding: compute $Hx = s$ for big $(n-k) \times n$ matrix $H$.

$$
\begin{pmatrix}
1 & 0 & 1 & 1 & \ldots & 0 \\
0 & 0 & 0 & 1 & \ldots & 0 \\
0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 1 & 0 & 0 & \ldots & 1
\end{pmatrix}
\begin{pmatrix}
1 \\
0 \\
0 \\
\vdots \\
1
\end{pmatrix} =
\begin{pmatrix}
0 \\
0 \\
1 \\
\vdots \\
1
\end{pmatrix} = s
$$

Tanja Lange. "Benchmarking of post-quantum cryptography"

http://bench.cr.yp.to/
**Basics of coding theory**

Here only consider binary codes, i.e., codes over $\mathbb{F}_2$.

- **Basics of coding theory**: Transmission channel is not perfect, so $x \in \mathbb{F}_2^n$ will have some bits flipped.

- **Syndrome decoding**: compute $Hx = s$ for big $(n - k) \times n$ matrix $H$.

  $$
  \begin{pmatrix}
  1 & 0 & 1 & 1 & \ldots & 0 \\
  0 & 0 & 0 & 1 & \ldots & 0 \\
  \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 1 & 0 & 0 & \ldots & 1
  \end{pmatrix}
  \begin{pmatrix}
  1 \\
  0 \\
  0 \\
  1
  \end{pmatrix}
  =
  \begin{pmatrix}
  0 \\
  1 \\
  \vdots \\
  1
  \end{pmatrix}
  = s
  $$

- **Reconstruct error vector $e$ and thereby get originally sent codeword $x + e$.**

- **Works if not too many errors**, i.e., number of 1s in $e$ is small. This number is called the weight.

---

**Code-based cryptography**

- **Basics of coding theory**: Transmission channel is not perfect, so $x \in \mathbb{F}_2^n$ will have some bits flipped.

- **Syndrome decoding**: compute $Hx = s$ for big $(n - k) \times n$ matrix $H$. Reconstruct error vector $e$ and thereby get originally sent codeword $x + e$.

- **Works if not too many errors**, i.e., number of 1s in $e$ is small. This number is called the weight.

- **Code-based crypto uses $e$ to transport key for symmetric encryption**. Take $e \in \mathbb{F}_2^n$ to have exactly weight $t$.

- **Users know how to derive keys for symmetric encryption** ($AES$, Salsa20, ...) $k(e)$ and key for message authentication $r(e)$.

- **To encrypt $m$ to Bob**, Alice looks up Bob’s matrix $H$.

  computes $s = He$, $c = \text{FIPS}_k(s)(m)$ and $a = \text{MAC}_r(k)(c)$ and sends $s$, $c$, $a$ to Bob.
How can this be secure?

\[
\begin{pmatrix}
1 & 0 & 1 & 1 & \ldots & 0 \\
0 & 0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 1 & 0 & 0 & \ldots & 1
\end{pmatrix}
= \begin{pmatrix}
1 & 0 \\
0 & 1 \\
\vdots & \vdots \\
1 & 1
\end{pmatrix}
\]

- Code-based crypto uses two different views of the same code – one for the public parameter \( H \) which resembles a generic code and one for the secret key which is efficiently decodable.
- Classical decoding problem: find the closest codeword \( c \in C \) to a given \( x \in \mathbb{F}_2^n \), assuming that there is a unique closest codeword.
- In particular: Decoding a generic binary code of length \( n \) and without knowing anything about its structure requires about \( 2^{(0.5+o(1))n/\log_2(n)} \) binary operations (assuming a rate \( \approx 1/2 \)).
- Coding theory deals with efficiently decodable codes, e.g., Goppa codes are efficiently decodable and lead to random looking public matrices \( H \).

Tanja Lange “Benchmarking of post-quantum cryptography”

Good security history

- Original parameters by McEliece in 1978 \( n = 1024, k = 524, t = 50 \), i.e., 50 errors in a \([1024, 524]\) code.
- In 2008 we wrote attack software against these original parameters. Attack on a single computer with a 2.4GHz Intel Core 2 Quad Q6600 CPU would need, on average, 1400 days (\(2^{58}\) CPU cycles) to complete the attack.
- Parameters used in McBits offer much more security (\(2^{90}\), \(2^{128}\), and \(2^{256}\) respectively), size of public key is \( k(n - k) \) bits.
- Move from \(2^{128}\) to \(2^{256}\) to protect against attacks using quantum computers.

Good efficiency

- Encrypting is efficient – simple matrix-vector product.
- McBits shows that Goppa codes can be decoded efficiently and in constant time.

Tanja Lange “Benchmarking of post-quantum cryptography”
Implementations loopholes in quantum cryptography
Vadim Makarov, Institute for Quantum Computing, University of Waterloo

Abstract

Quantum key distribution, although absolutely secure in theory, is currently under assault from hackers. They break its security via practical attacks that exploit imperfections in components and implementations of opto-electronic hardware. The issue of implementation security is well-known in classical cryptography, however it proved to be somewhat of a surprise to the quantum cryptography community when it became apparent several years ago. I will give a brief overview of the current situation, give examples of attacks and countermeasures, and explain how quantum cryptography research and manufacturing community handles this issue. Implementation security problems cause rapid and drastic developments in technology, which in turn affects standardization efforts in quantum cryptography.
Presentations

SESSION 6
SECURITY ISSUES

Stages of secure technology

1. Idea / theory / proof-of-the-principle
   1970–1993
2. Initial implementations
   1994–2005
3. Weeding out implementation loopholes (spectacular failures $\Rightarrow$ patching)
4. Good for wide use

Security model of QKD

Secret key rate $R = f(QBER)$

Security proof

Laws of physics & Model of equipment
Presentations

SESSION 6
SECURITY ISSUES

Security model of QKD

Laws of physics & Model of equipment

Security proof

Integrate imperfection into security model

Example of vulnerability and countermeasures

Photon-number-splitting attack


Laser
Attenuator

Decoy-state protocol


SARG04 protocol


Distributed-phase-reference protocols

### SECURITY ISSUES

#### SESSION 6

**Presentations**

---

**Attack**

<table>
<thead>
<tr>
<th>Attack</th>
<th>Target component</th>
<th>Tested system</th>
<th>Demonstrated eavesdropped (% key)?</th>
<th>Keeps full key rate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detector control</td>
<td>single-photon detector</td>
<td>ID Quantique, MagiQ Tech.</td>
<td>no (100%)</td>
<td>yes</td>
</tr>
<tr>
<td>I. Lydersen et al., Nat. Photonics 4, 685 (2013)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detector control</td>
<td>single-photon detector</td>
<td>research syst.</td>
<td>yes (100%)</td>
<td>yes</td>
</tr>
<tr>
<td>Deadtime</td>
<td>single-photon detector</td>
<td>research syst.</td>
<td>yes (98.8%)</td>
<td>no, 1/4</td>
</tr>
<tr>
<td>Multi-wavelength</td>
<td>beamsplitter</td>
<td>research syst.</td>
<td>yes (≤100%)</td>
<td>yes</td>
</tr>
<tr>
<td>Wavelength-selected PNS</td>
<td>intensity modulator</td>
<td>(theory)</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Shot-noise calibration</td>
<td>sync detector</td>
<td>SeQureNet</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Detector saturation</td>
<td>homodyne detector</td>
<td>SeQureNet</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>H. Qin, R. Kumar, R. Alleaume, presentation at QCrypt (2013)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Attack example: avalanche photodetectors (APDs)**

**Linear mode**

**Geiger mode**

- Breakdown voltage $V_{br}$

- Single photon

- Quenching

- $I_{th}$, $P_{th}$, $P_{opt}$
Presentations

SESSION 6
SECURITY ISSUES

Lars Lydersen testing MagiQ Technologies QPN 5505

Eavesdropping 100% key on installed QKD line
on campus of the National University of Singapore, July 4–5, 2009

I. Gethard, G. Liu et al.,
Nat. Commun. 2, 349 (2011)
Controlling superconducting nanowire single-photon detectors

1. Blind (latch)

2. Control

Comparator input voltage, a.u.

Time, ns

0 10 20 30

M. G. Tanner, V. Makarov, R. H. Hadfield, arXiv:1305.5989

Countermeasures to detector attacks

Band-aid

Software patch to randomly vary detector sensitivity

Monitoring extra electrical parameters in detector

Integrated into security model

Measurement-device-independent QKD

Demonstration in Calgary
A. Rubenok et al., arXiv:1204.4738
Evaluating the security of post-quantum cryptosystems
Yi-kai Liu, National Institute of Standards & Technology (NIST)

Abstract

Researchers at the US National Institute of Standards and Technology (NIST) are currently studying a number of proposed post-quantum cryptosystems, with a view to possible future standardization. These cryptosystems include lattice-based schemes such as NTRU, code-based schemes such as McEliece, and multivariate schemes such as HFE and unbalanced oil-vinegar.

This talk will describe some different ways of evaluating the security of these cryptosystems. One approach is to measure the complexity of the best known attacks (e.g., lattice basis reduction, Grobner basis algorithms, and differential attacks). Another approach uses security proofs, based on the conjectured hardness of specific problems in number theory and combinatorial optimization. A third approach uses “structural” results that upper-bound the power of specific classes of attacks (e.g., classifications of the invariants that can be used in differential attacks, and upper-bounds on the power of quantum algorithms for solving non-Abelian hidden subgroup problems).

Finally we will discuss some current challenges and questions. One basic challenge is to provide a reliable, quantitative assessment of security for a given cryptosystem. Can one use theoretical analyses to reason about the possible existence of attacks going beyond those currently known? Another challenge is to improve the key sizes and signature lengths of these cryptosystems, while maintaining the same level of security.
How to show that a cryptosystem is secure?

› Security is hard to measure!

› Want to have a transparent justification: why is this secure?

› Continuing to use RSA is risky; is there a benefit to using PQC?
  • Diversity/redundancy in security

How to show that a cryptosystem is secure?

› What does security mean?
  • Breaking the cryptosystem is computationally hard, e.g., requires $2^{256}$ operations

› Show security against **known attacks**
  • Try all known attacks, show that they are infeasible

› How to protect against **unknown attacks**?
  • New attacks, new discoveries in mathematics?
  • Try to argue that these are “unlikely”
    • Security proofs (based on mathematical conjectures)
    • Design cryptosystems to defeat common classes of attacks
General-purpose algorithms

- **Lattice basis reduction**
  - LLL, BKZ, enumeration + extreme pruning
  - Practical performance beats theoretical guarantees
    - What problem instances?
    - How to measure solution quality?
    - Tradeoffs between different algorithms

- **Grobner basis reduction**
  - General algorithm for solving multivariate systems of equations
  - Running time may depend on special structure present in the equations

Specialized attacks

- "Learning a parallelepiped"
  - Breaks old versions of NTRUSign
  - NTRUSign can be repaired using perturbations; is this secure?
  - Other lattice-based signatures are provably secure; recent work has improved their efficiency

- **Differential attacks**
  - Break certain multivariate cryptosystems (e.g., SFLASH)
  - HFE, unbalanced oil/vinegar are still ok

- **Lattice reduction attacks**
  - Break some versions of McEliece using LDPC codes
  - Standard McEliece is still ok
Security against known attacks

- Estimate the complexity of the known attacks
  - Run experiments on small instances of the problem
  - Then extrapolate to larger problem sizes
- Adjust the cryptosystem to defeat these attacks

<table>
<thead>
<tr>
<th>Type of attack</th>
<th>Complexity of attack</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>General purpose algorithm</td>
<td>Exponential time</td>
<td>Increase the key size</td>
</tr>
<tr>
<td>Exploit some special structure in the problem</td>
<td>Varies, can be polynomial time</td>
<td>Design the cryptosystem to avoid that structure</td>
</tr>
</tbody>
</table>

Is that all?

- Could there be other attacks that we haven’t discovered yet?
- Faster general-purpose algorithms?
  - Probably not...
- More specialized attacks?
  - Attacks on ideal lattices, compact McEliece cryptosystems?
  - (These cryptosystems have special structure, to improve efficiency)
The rest of this talk

- Theoretical tools for thinking about security
  - Security proofs
  - Impossibility of special classes of attacks
- Why is a particular cryptosystem secure?
- Can we reason about the possible existence of attacks that haven't been discovered?
  - Designing a public-key cryptosystem is "harder" than designing a block cipher or a hash function
  - Want to avoid unpleasant surprises!
    (e.g., new discoveries that lead to poly-time attacks)
Security proofs

- Goal: rule out the existence of attacks
- Method: relate the security of a cryptosystem to another problem that we understand better
  - Factoring, discrete logs
  - Finding short lattice vectors
  - Solving multivariate systems of equations
- Perspective from complexity theory:
  - Public-key cryptography requires very hard problems
  - Average-case instances must be hard
  - Need to generate hard instances efficiently
  - Need trapdoor one-way functions

How to evaluate the strength of a security proof?

- Conjecture: “Problem \( \Pi \) is hard”
  - Do we believe this conjecture?
  - E.g., lattice-based crypto: general lattices seem hard, b/c of connection with integer programming; situation for ideal lattices is less clear
- Theorem: “If you can break cryptosystem C, you can solve problem \( \Pi \)”
  - How strong is the connection between C and \( \Pi \)?
  - E.g., lattice-based crypto: very strong connection ("worst-case to average-case reduction")
Caveats of security proofs
[for public key crypto]

- Have to define “security”
  - Different notions: CPA < CCA < UC
  - May not fully describe the real world (e.g., side channels)

- Additional assumptions are often needed, to prove security for practical cryptosystems
  - Assume ideal lattices are hard
  - Work in random oracle model

- Use the security proof to choose key sizes?
  - Security proof gives a lower bound on security
  - Bound can be very loose \( \Rightarrow \) not useful in practice

Security proofs

- On the positive side...

- Security proofs help to constrain the space of possible attacks
  - Argue that polynomial-time attacks are unlikely...
    (would require surprising discoveries)
Special classes of attacks

- Some specific attacks one might worry about
  - Differential attacks in multivariate crypto
  - Shor’s algorithm, hidden subgroup problems
  - Grover’s search algorithm

- Can prove limits on the power of these attacks!

---

Special classes of attacks

- Differential attacks in multivariate crypto
  - Find and classify all “differential invariants”
  - Can rule out all possible differential attacks!
    (Perlner & Smith, 2013)

- Quantum algorithms for hidden subgroup problems
  - Generalizations of Shor’s algorithm to other groups
  - Unlikely to get a poly-time quantum algorithm for the symmetric group (Moore & Russell)

- Lower bounds on quantum query complexity
  - For black-box problems, e.g., search and collision finding
  - Known quantum algorithms are nearly optimal
  - Rules out the possibility of a super-polynomial quantum speedup
Outlook

- Different approaches to evaluating security
  - Estimating the performance of known attacks
  - Using security proofs and formal analysis to rule out the existence of unknown attacks

- Open questions
  - Many cryptosystems use lattices/codes/equations with special structure; how does this affect security?
  - How to measure the complexity of a quantum attack?
  - How well do these cryptosystems perform with other protocols in the real world?
Multi-variate function based quantum-safe crypto
Multi-variate Public Key Cryptography
Jintai Ding, University of Waterloo
Presentations

SESSION 6
SECURITY ISSUES

Outline

1. Introduction
2. Signature schemes
3. Encryption schemes

What is a MPKC?

- Multivariate Public Key Cryptosystems
  - Cryptosystems with public keys as a set of multivariate functions
- Public key: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$. 
What is a MPKC?

- Multivariate Public Key Cryptosystems
  - Cryptosystems with public keys as a set of multivariate functions
- Public key: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
- Private key: a way to compute $G^{-1}$ via the decomposition.

What is a MPKC?

- Multivariate Public Key Cryptosystems
  - Cryptosystems with public keys as a set of multivariate functions
- Public key: $G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1$.
- Private key: a way to compute $G^{-1}$ via the decomposition.

- Signing (a hash of) a document:
What is a MPKC?

- Multivariate Public Key Cryptosystems
  - Cryptosystems with public keys as a set of multivariate functions
- Public key: \( G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1 \).
- Private key: a way to compute \( G^{-1} \) via the decomposition.
- Signing (a hash of) a document:
  \((x_1, \ldots, x_n) \in G^{-1}(y_1, \ldots, y_m)\).

What is a MPKC?

- Multivariate Public Key Cryptosystems
  - Cryptosystems with public keys as a set of multivariate functions
- Public key: \( G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1 \).
- Private key: a way to compute \( G^{-1} \) via the decomposition.
- Signing (a hash of) a document:
  \((x_1, \ldots, x_n) \in G^{-1}(y_1, \ldots, y_m)\).
- Verifying: \((y_1, \ldots, y_m) \Rightarrow G(x_1, \ldots, x_n)\).
  \(k\), a small finite field.
Direct attack is to solve the set of equations:

\[ G(M) = G(x_1, ..., x_n) = (y'_1, ..., y'_m). \]

- Solving a set of \( n \) randomly chosen equations (nonlinear) with \( n \) variables is NP-complete, though this does not necessarily ensure the security of the systems.
Quadratic Constructions

1) Efficiency considerations lead to mainly quadratic constructions.

\[ G(x_1, ..., x_n) = \sum_{i,j} \alpha_{ij} x_i x_j + \sum_{i} \beta_i x_i + \gamma. \]

2) Mathematical structure consideration: Any set of high degree polynomial equations can be reduced to a set of quadratic equations.
The view from the history of Mathematics

- RSA – Number Theory – the 18th century mathematics
- ECC – Theory of Elliptic Curves – the 19th century mathematics
The view from the history of Mathematics

- RSA – Number Theory – the 18th century mathematics
- ECC – Theory of Elliptic Curves – the 19th century mathematics
- Multivariate Public key cryptosystem – Algebraic Geometry – the 20th century mathematics

Algebraic Geometry – Theory of Polynomial Rings

Humans have been trying to solve polynomial equations for thousands of years.

- Early attempts by Diffie, Fell, Imai, Ong, Matsumoto, Schnorr, Shamir, Tsuji, etc.
The view from the history of Mathematics

- RSA – Number Theory – the 18th century mathematics
- ECC – Theory of Elliptic Curves – the 19th century mathematics
- Multivariate Public key cryptosystem – Algebraic Geometry – the 20th century mathematics

Algebraic Geometry – Theory of Polynomial Rings

Humans have been trying to solve polynomial equations for thousands of years.

- Early attempts by Diffie, Fell, Imai, Ong, Matsumoto, Schnorr, Shamir, Tsujii, etc.
- Fast development in the late 1990s.

Outline

1 Introduction
2 Signature schemes
3 Encryption schemes
How to construct $G$?

- The unbalanced Oil-Vinegar scheme by Kipnis, Patarin and Goubin 1999.

$G = F \circ L$.

- $F$: nonlinear, easy to compute $F^{-1}$.
- $L$: invertible linear, to hide the structure of $F$. 

How to construct G?

- The unbalanced Oil-Vinegar scheme by Kipnis, Patarin and Goubin 1999.
- $G = F \circ L$.
  - $F$: nonlinear, easy to compute $F^{-1}$.
  - $L$: invertible linear, to hide the structure of $F$.

How to construct G?

- The unbalanced Oil-Vinegar scheme by Kipnis, Patarin and Goubin 1999.
- $G = F \circ L$.
  - $F$: nonlinear, easy to compute $F^{-1}$.
  - $L$: invertible linear, to hide the structure of $F$.
- $G = L_2 \circ F \circ L_1$.
  - $F$: Multi-layer UOV, easy to compute $F^{-1}$.
  - $L_1, L_2$: invertible linear, to hide the structure of $F$. 
Unbalanced Oil-vinegar (uov) schemes

\[ F = (f_1(x_1, \ldots, x_0, x'_1, \ldots, x'_n), \ldots, f_0(x_1, \ldots, x_0, x'_1, \ldots, x'_n)) \]

\[ f_i(x_1, \ldots, x_0, x'_1, \ldots, x'_n) = \sum a_{ij} x_i x'_j + \sum b_{ij} x'_i x'_j + \sum c_{ij} x_i + \sum d_{ij} x'_i e_j \]

Oil variables: \( x_1, \ldots, x_0 \).

Vinegar variables: \( x'_1, \ldots, x'_n \).
How to invert $F$?

\[
f_f(x_1, \ldots, x_n, x'_1, \ldots, x'_n) = \sum a_{ij} x_i x'_j + \sum b_{ij} x'_i x'_j + \sum c_{ij} x_i + \sum d_{ij} x'_i + e_i.
\]

---

How to invert $F$?

\[
f_f(x_1, \ldots, x_n, x'_1, \ldots, x'_n) = \sum a_{ij} x_i x'_j + \sum b_{ij} x'_i x'_j + \sum c_{ij} x_i + \sum d_{ij} x'_i + e_i.
\]

\[
f_f(x_1, \ldots, x_n, x'_1, \ldots, x'_n) = \sum a_{ij} x_i x'_j + \sum b_{ij} x'_i x'_j + \sum c_{ij} x_i + \sum d_{ij} x'_i + e_i.
\]

- $F$: linear in all variables: $x_1, \ldots, x_n$.

\[\implies F: \text{easy to invert.}\]
Presentations

SESSION 6
SECURITY ISSUES

Security analysis

1. Systematic theoretical and experimental analysis
   - Direct attack does not work against best existing polynomial solving algorithms
   - Finding keys again becomes a problem of solving polynomial equations
   - MinRank is a hard problem.
   - Natural Side channel attack resistance.

2. No weakness yet being found in the design.
Parameters and Performance

- Rainbow(17,13,13) over GF(2^5): Signature size: 43 bytes, private key: 19.1KB, public key: 25.1KB.
- Rainbow(26,16,17) over GF(2^5): Signature size: 59 bytes, private key: 45.0KB, public key: 59.0KB.
- Rainbow(36,21,22) over GF(2^5): Signature size: 79 bytes, private key: 101.5KB, public key: 136.1KB.

- High efficiency.
  IC for Rainbow: 804 cycles. (ASAP 2008)
  FPGA implementation at Bochum (CHES 2009) - Beat ECC in area and speed.
  Faster parallel implementation 200 cycles - (PQC 2011)
Parameters and Performance

- Rainbow(17,13,13) over GF(2^13): Signature size: 43 bytes, private key: 19.1KB, public key 25.1KB.
- Rainbow(26,16,17) over GF(2^7): Signature size: 59 bytes, private key 45.0KB, public key 59.0KB.
- Rainbow(36,21,22) over GF(2^6): Signature size: 79 bytes, private key 101.5KB, public key 136.1KB.
- High efficiency.
  IC for Rainbow: 804 cycles. (ASAP 2008)
  FPGA implementation at Bochum (CHES 2009) – Beat ECC in area and speed.
  Faster parallel implementation 200 cycles – (PQC 2011)
- Relative large public key
  Further optimizations – Petzoldt, Buchmann etc. at TU Darmstadt.

Parameters and Performance

- Rainbow(17,13,13) over GF(2^13): Signature size: 43 bytes, private key: 19.1KB, public key 25.1KB.
- Rainbow(26,16,17) over GF(2^7): Signature size: 59 bytes, private key 45.0KB, public key 59.0KB.
- Rainbow(36,21,22) over GF(2^6): Signature size: 79 bytes, private key 101.5KB, public key 136.1KB.
- High efficiency.
  IC for Rainbow: 804 cycles. (ASAP 2008)
  FPGA implementation at Bochum (CHES 2009) – Beat ECC in area and speed.
  Faster parallel implementation 200 cycles – (PQC 2011)
- Relative large public key
  Further optimizations – Petzoldt, Buchmann etc. at TU Darmstadt.
- Highly efficient compact signature
  Small devices – RFID, Sensors.
Another choice – HFEV-Minus – Quartz

- The basic design: Hidden field equation system with Vinegar variables and Minus modification designed in 1999

- Very short signature (107 bits) but slow.
Another choice – HFEV-Minus – Quartz

- The basic design: Hidden field equation system with Vinegar variables and Minus modification designed in 1999
- Very short signature (107 bits) but slow.
- No weakness yet found.

Another choice – HFEV-Minus – Quartz

- The basic design: Hidden field equation system with Vinegar variables and Minus modification designed in 1999
- Very short signature (107 bits) but slow.
- No weakness yet found.
- New designs by Ding, Petzoldt, Tao, Yang, very efficient (more than 1000 times faster with a 90 bits signature, or 170 bits for post-quantum signature.)
Another choice – HFEV-Minus – Quartz

- The basic design: Hidden field equation system with Vinegar variables and Minus modification designed in 1999
- Very short signature (107 bits) but slow.
- No weakness yet found.
- New designs by Ding, Petzoldt, Tao, Yang, very efficient (more than 1000 times faster with a 90 bits signature, or 170bits for post-quantum signature.)
- Solid theoretical and experimental security analysis.

Outline

1. Introduction
2. Signature schemes
3. Encryption schemes
The basic design

- The public key is given as:

$$G(x_1, ..., x_n) = (G_1(x_1, ..., x_n), ..., G_m(x_1, ..., x_n)) = L_2 \circ F \circ L_1.$$  

- $G_i$ are multivariate polynomials over a finite field, which are mostly degree 2.

- Any plaintext $M = (x'_1, ..., x'_n)$ is encrypted via polynomial evaluation:

$$G(M) = G(x'_1, ..., x'_n) = (y'_1, ..., y'_m).$$
The basic design

- The public key is given as:
  \[ G(x_1, \ldots, x_n) = (G_1(x_1, \ldots, x_n), \ldots, G_m(x_1, \ldots, x_n)) = L_2 \circ F \circ L_1. \]
  
  \( G_i \) are multivariate polynomials over a finite field, which are mostly degree 2

- Any plaintext \( M = (x'_1, \ldots, x'_n) \) is encrypted via polynomial evaluation:
  \[ G(M) = G(x'_1, \ldots, x'_n) = (y'_1, \ldots, y'_m). \]

- To decrypt the ciphertext \( (y'_1, \ldots, y'_m) \), one needs to know a secret (the secret key) to compute the inverse map \( G^{-1} \) to find the plaintext \( (x'_1, \ldots, x'_n) = G^{-1}(y'_1, \ldots, y'_m). \)

The best designs

- Internal perturbation of HFE and perturbed MI with Plus:
  Designed by Ding, Schmidt.
The best designs

- Internal perturbation of HFE and perturbed MI with Plus.
  Designed by Ding, Schmidt.
- But relative slow and large key size.

The best designs

- Internal perturbation of HFE and perturbed MI with Plus.
  Designed by Ding, Schmidt.
- But relative slow and large key size.
- New designs – Simple matrix method by Ding and Tao 2013.
The best designs

- Internal perturbation of HFE and perturbed MI with Plus. Designed by Ding, Schmidt.
- But relatively slow and large key size.
- New designs – Simple matrix method by Ding and Tao 2013.
- The efficiency is now comparable with the signature scheme.

Summary

- MPKC provide the best signature designs in terms of computing performance and signature size. – Application for small devices.
MPKC provide the best signature designs in terms of computing performance and signature size. – Application for small devices.

The security analysis has solid theoretical support and systematic experimental support.

Drawback: relative large key sizes (10s KB) but can be substantially improved with further optimization.
Summary

- MPKC provide the best signature designs in terms of computing performance and signature size. — Application for small devices.
- The security analysis has solid theoretical support and systematic experimental support.
- Drawback: relative large key sizes (10s KB) but can be substantially improved with further optimization
- We have solid but not so efficient encryption schemes. New designs are catching up.

The end

Thank you