SAFEcrypto: Secure Architectures of Future Emerging cryptography

Máire O’Neill
Queen’s University Belfast
SAFEcrypto will provide a new generation of practical, robust and physically secure post-quantum cryptographic solutions that ensure long-term security for future ICT systems, services and applications.

Focus is on **lattice-based cryptography** and solutions demonstrated for:

1. Satellite communications
2. Public-safety communications systems
3. Municipal Data Analytics
Summary of Objectives

1. Investigate practicality of LBC primitives (digital signatures, authentication, IBE and ABE) to determine their fit-for-purpose in real-world applications

2. Design and implement hardware & software architectures of LBC primitives that will fulfill the needs of a wide range of applications

3. Investigate the physical security of the LBC implementations to protect against leakage of sensitive information via side channel and fault attacks

4. Evaluate LBC in current secure comms protocols, such as TLS, IPSec

5. Deliver *proof-of-concept demonstrators* of LBC primitives applied to 3 case-studies:
   - Satellite Communications
   - Public Safety Communication
   - Municipal Data Analytics
Lattice Based Cryptographic Building Blocks

- **Matrix vector multiplication** for standard lattices
- **Polynomial multiplication** for ideal lattices
- **Discrete Gaussian Sampling**
  - Bernoulli sampling
  - Cumulative Distribution Table (CDT) sampling
  - Knuth-Yao sampling
  - Ziggurat sampling
  - Micciancio-Walter Gaussian Sampler
Challenges for Practical LBC Implementations

• Need to be as efficient and versatile as classical Public Key systems, such as RSA and ECC

• Embedded devices are constrained
  - No large memories
  - Limited computational power

• Choice of parameters is crucial - long-term/QC-security
  - Parameters tend to be larger than classic PK schemes
  - Directly affects performance
  - Scalability

• Choice of Gaussian Sampler
  - Different choice for signatures Vs encryption
  - Different choice for high speed Vs compact design

www.safecrypto.eu | @safecrypto
### Hardware Designs of Lattice-based Cryptography

#### LWE Vs Ring-LWE Encryption
- Standard LBC shown to be practical – 1272 Ops/sec on Spartan 6 FPGA

<table>
<thead>
<tr>
<th>Operation and Algorithm</th>
<th>Device</th>
<th>LUT/FF/SLICE</th>
<th>BRAM/DSP</th>
<th>MHz</th>
<th>Cycles</th>
<th>Ops/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWE Encrypt ($\lambda = 128$)</td>
<td>S6LX45</td>
<td>6152/4804/1866</td>
<td>73/1</td>
<td>125</td>
<td>98304</td>
<td>1272</td>
</tr>
<tr>
<td>LWE Encrypt ($\lambda = 64$)</td>
<td>S6LX45</td>
<td>6078/4676/1811</td>
<td>73/1</td>
<td>125</td>
<td>98304</td>
<td>1272</td>
</tr>
<tr>
<td>LWE Decrypt</td>
<td>S6LX45</td>
<td>63/58/32</td>
<td>13/1</td>
<td>144</td>
<td>32768</td>
<td>4395</td>
</tr>
<tr>
<td>RLWE Encrypt (Pöppelmann &amp; Güneysu (PG), 2014)*</td>
<td>S6LX16</td>
<td>4121/3513/-</td>
<td>14/1</td>
<td>160</td>
<td>6861</td>
<td>23321</td>
</tr>
<tr>
<td>RLWE Decrypt (PG 2014)*</td>
<td>S6LX16</td>
<td>4121/3513/-</td>
<td>14/1</td>
<td>160</td>
<td>4404</td>
<td>36331</td>
</tr>
<tr>
<td>RLWE Encrypt (PG 2014)*</td>
<td>V6LX75T</td>
<td>4549/3624/1506</td>
<td>12/1</td>
<td>262</td>
<td>6861</td>
<td>38187</td>
</tr>
<tr>
<td>RLWE Decrypt (PG 2014)*</td>
<td>V6LX75T</td>
<td>4549/3624/1506</td>
<td>12/1</td>
<td>262</td>
<td>4404</td>
<td>59492</td>
</tr>
<tr>
<td>RLWE Encrypt (PG 2014)</td>
<td>S6LX9</td>
<td>282/238/95</td>
<td>2/1</td>
<td>144</td>
<td>136212</td>
<td>1057</td>
</tr>
<tr>
<td>RLWE Decrypt (PG 2014)</td>
<td>S6LX9</td>
<td>94/87/32</td>
<td>1/1</td>
<td>189</td>
<td>66338</td>
<td>2849</td>
</tr>
<tr>
<td>RLWE Encrypt (Roy et al, 2014)*</td>
<td>V6LX75T</td>
<td>1349/860/-</td>
<td>2/1</td>
<td>313</td>
<td>6300</td>
<td>49751</td>
</tr>
<tr>
<td>RLWE Decrypt (Roy et al, 2014)*</td>
<td>V6LX75T</td>
<td>1349/860/-</td>
<td>2/1</td>
<td>313</td>
<td>2800</td>
<td>109890</td>
</tr>
</tbody>
</table>
Discrete Gaussian Sampling is a key component in LBC, but can be a major bottleneck in practice

- Comprehensive evaluation offers recommendations on most appropriate sampler to use for encryption, authentication, high-speed applications etc..
- Proposed independent-time hardware designs of a range of samplers offering security against side-channel timing attacks
Open source software library enabling the development of quantum-safe crypto solutions for commercial applications. Currently supports:

- **Signatures**: BLISS-B, Dilithium, Dilithium-G, Ring-TESLA, DLP, ENS
- **Encryption**: RLWE, Kyber
- **KEM**: ENS, Kyber

**Digital Signatures: Classical vs LBC Signatures** (Intel Core i7 6700 3.4 GHz)
Practical Identity-Based Encryption over NTRU Lattices

➢ First ANSI C Implementation of DLP-IBE Scheme

Accelerating the DLP-IBE scheme (192-bit security) [Intel Core i7 6700 3.4 GHz]

<table>
<thead>
<tr>
<th>Operation</th>
<th>Cortex-M0</th>
<th>Cortex-M4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>3,297,380</td>
<td>972,744</td>
</tr>
<tr>
<td>Decryption</td>
<td>1,155,000</td>
<td>318,539</td>
</tr>
</tbody>
</table>

ARM Cortex-M0/M4

6ms per enc operation @ 80 bit security
Satellite Communications

Security and key management vital within satellite systems

• Currently:  - systems owned and operated by one organisation
  - symmetric key crypto exclusively used

• In future:  - Repurposing of satellites and sharing of infrastructure
  - Number of space-based entities, missions & number/variety of end users will increase
  - Public key cryptography will be used

• Given the longevity of satellite systems, public key solutions needs to withstand attacks for 10-40 years

=> ideal case study for post-quantum cryptography
Satellite Communications Use-case

**First Demo:** Simulates the activities required to establish, use and maintain a quantum-safe channel between an *Operational Control Centre* and *Satellite* for exchanging Telecommand & Housekeeping Telemetry data.

- Models the Key Establishment, Operational Use and Key Update phases of the key management lifecycle
- Integrates SAFEcrypto open-source quantum-safe implementations of BLISS and Ring-LWE into StrongSwan

www.safecrypto.eu | @safecrypto
Conclusions & Future Work

Conclusions

• Lattice-based cryptosystems are a promising Post-Quantum cryptography solution for long-term security applications
  - LBC offers versatility in the range of cryptosystems it can support
• LBC Encryption & signatures now more practical than RSA-based schemes
• SAFEcrypto outputs demonstrating that LBC can meet the requirements of real world scenarios.

Future Plans

• Design and implementation of physically secure HW/SW LBC schemes
• Proof of concept demonstrators for the 3 case studies will generate quantum-safe solutions for: IKEv2, TLS, DTLS, KMIP
• Assist with current global initiatives:
  – ETSI QSC Industry Specification Group
  – US NIST process for Quantum-safe public-key candidates