NOKIA Bell Labs

PRINCE algorithm for Industrial IoT

A high-throughput, low-area implementation

- Johanna Kruse (Wireless Implementation and Trial Systems, Stuttgart, Germany)
- Dr. Dimitrios Schinianakis (Networks, Analytics, Algorithms, Control and Security, Munich, Germany)

- 15-06-2017

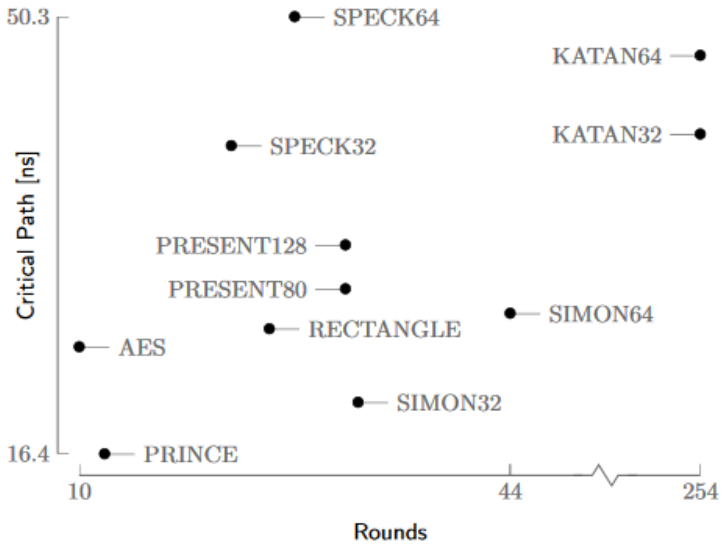
Agenda

- Motivation
- Use Case for Industrial IoT
- PRINCE algorithm
- Discussion of results
- Further research

State of the Art
Lightweight Cryptography

- Emerging field of Lightweight Cryptography
- Target: **constrained devices**
- **Single-cycle** implementation to decrease latency

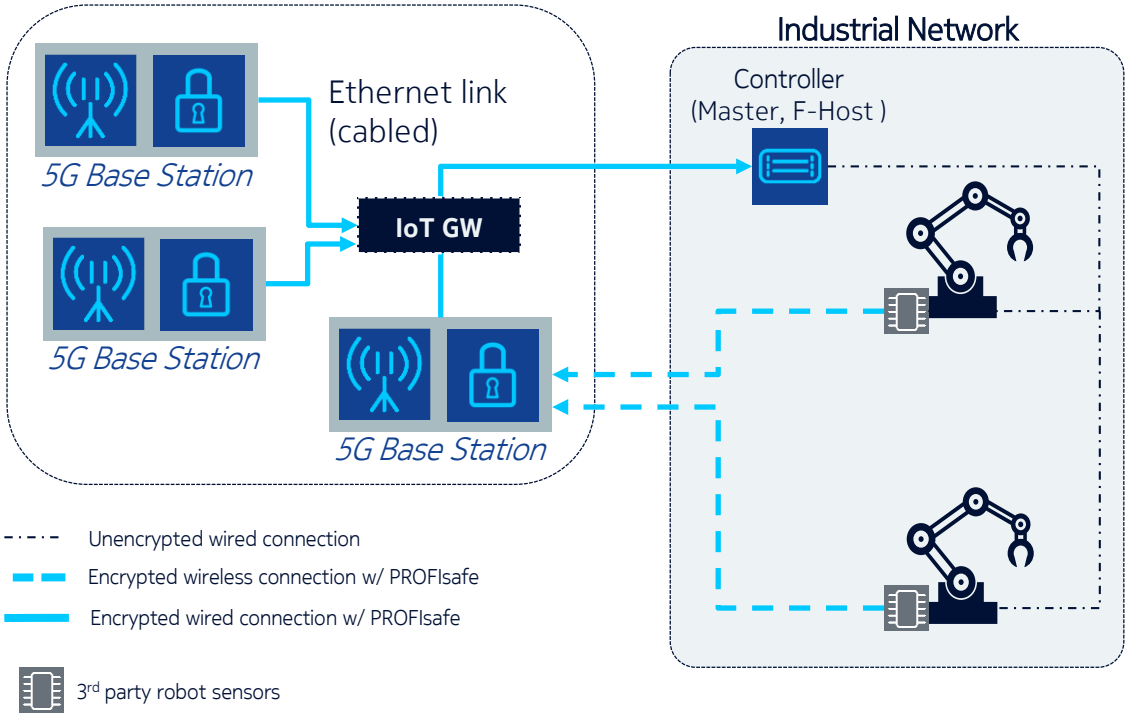
- **Problem**: low throughput



Maene P., Verbauwhede I. (2016) Single-Cycle Implementations of Block Ciphers. In: Güneysu T., Leander G., Moradi A. (eds) Lightweight Cryptography for Security and Privacy. Lecture Notes in Computer Science, vol 9542. Springer, Cham

Use Case for Industrial IoT

Secure wireless robot sensor over industrial protocol (Profinet)

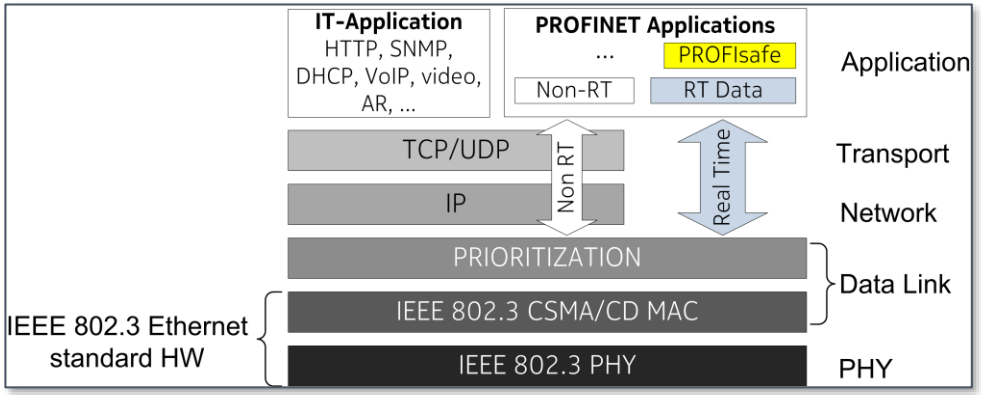


5G air interface optimized for industrial applications

- Ultra **low-latency** (4-8ms)
- Large # of devices
- High reliability
- **MAC Layer Encryption** required (e.g. Profinet/Profisafe)

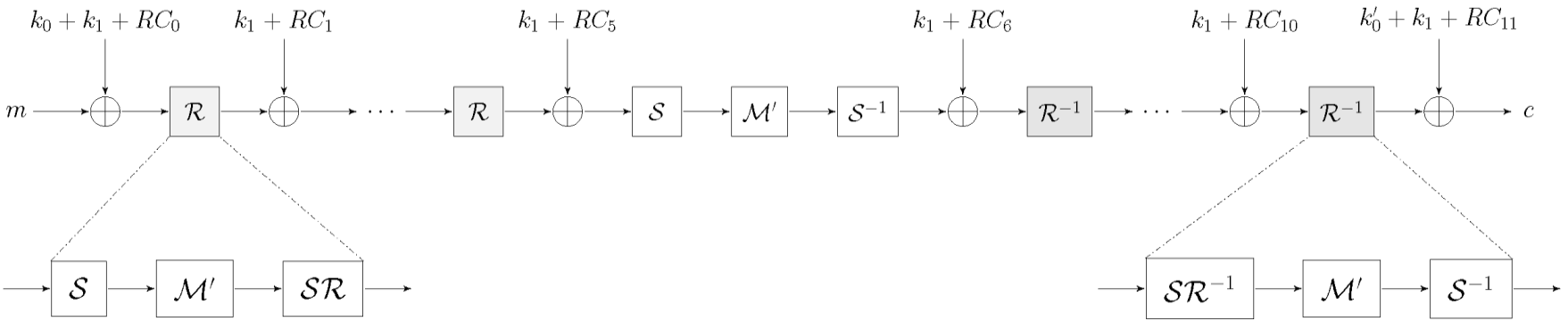
Use Case for Industrial IoT
Security perspective

- Adhere to **strict budget** for security operations
- Ultra **high-throughput** (multiple device connectivity on the same interface)
- Authentication & integrity protection per message
- **Infrequent short-packet** transmission – low protocol overhead



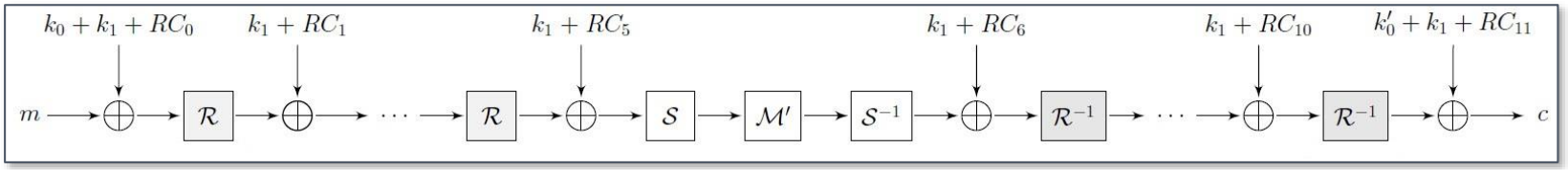
PI North America, “PROFINET, industrial ethernet for advanced manufacturing”, http://us.profinet.com/technology/profinet/, accessed: 2016-09-26.

PRINCE algorithm
Design

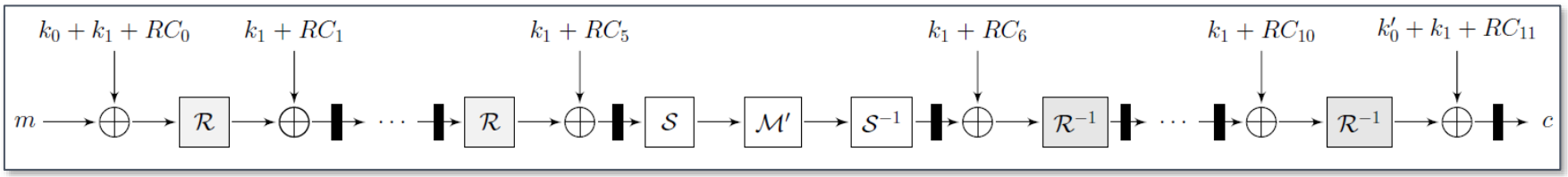


- 64-bit plaintext/ciphertext
- 128-bit key
- originally **single-cycle** approach
- focus on **low latency**
- **Hardware-oriented**

PRINCE algorithm
Pipelined Implementation



Use of **pipelining** to increase throughput



Discussion of Results
PRINCE results

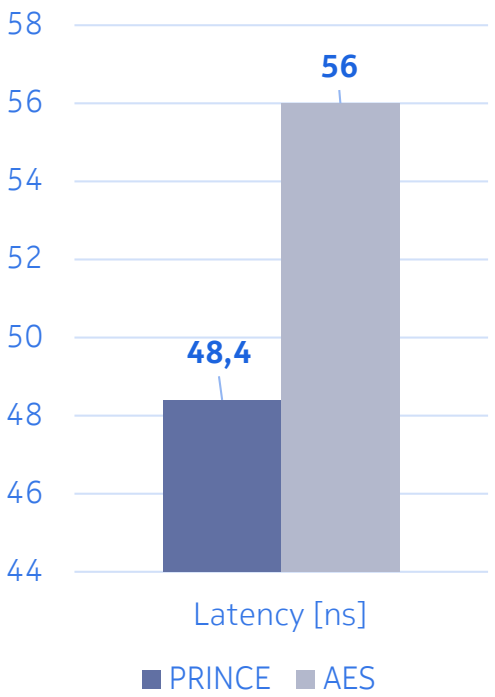
	Pipeline stages	Max. frequency [MHz]	Period [ns]	Latency [ns]	Throughput [Gbit/s]	Area [#LUT]	Area [#FF]	Area [#slices]	Mbps/Slice
PRINCE	0	35.7	28	28	2.284	844	128	252	9.06
	11	227.273	4.4	48.4	14.545	828	832	267	54.477

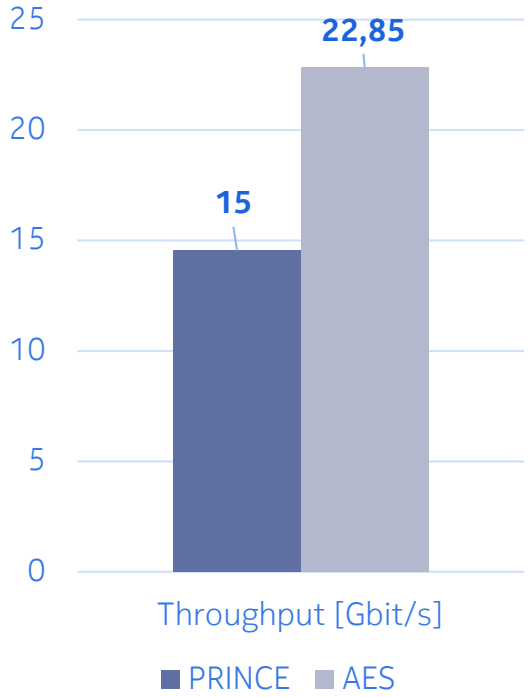
- **FPGA Implementation**: Zynq-7000 (Artix-7, ARM Cortex A9)

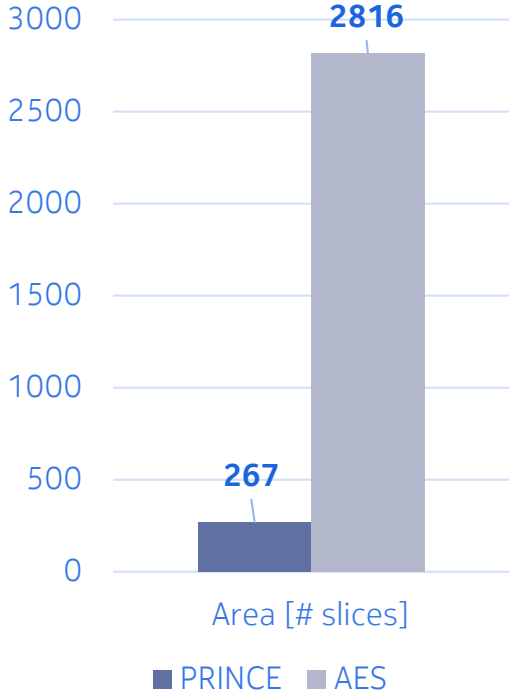
Discussion of Results
PRINCE vs AES

	Pipeline stages	Max. frequency [MHz]	Period [ns]	Latency [ns]	Throughput [Gbit/s]	Area [#LUT]	Area [#FF]	Area [#slices]	Mbps/Slice
PRINCE	0	35.7	28	28	2.284	844	128	252	9.06
	11	227.273	4.4	48.4	14.545	828	832	**267**	54.477
AES	0	25	40	40	3.2	7563	256	2020	1.58
	10	178.571	5.6	56	22.85	9511	2242	**2816**	8.11

Discussion of Results
Comparison PRINCE - AES



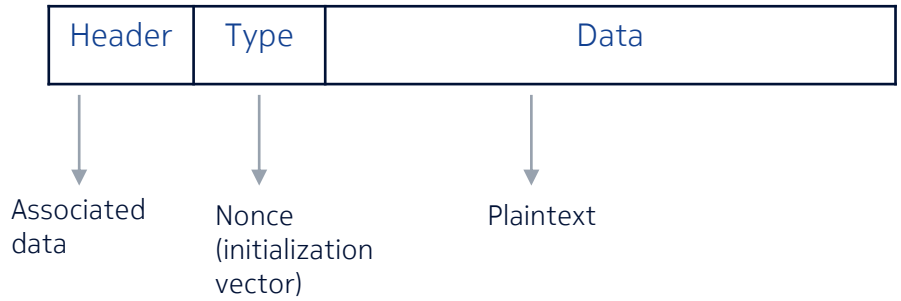




Further research
Authenticated Encryption with Associated Data (AEAD)

- **Nonce-based AEAD**: never repeating initialization vector across all instances of encryption and all devices in the network under a given key
- Possibility of **authentication only** without encryption
- Nonce N, plaintext P and associated data A → Ciphertext C and authenticated tag T

Typical Ethernet Frame



Summary and Outlook

- PRINCE as an efficient ciphering algorithm targeting **area-constrained devices**
- Capability to support **massive machine type communication**
- Further research: **Authenticated encryption** in combination with PRINCE

Sources

(1) Borghoff J. et al. (2012) PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications. In: Wang X., Sako K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg

(2) PI North America, “PROFINET, industrial ethernet for advanced manufacturing”, http://us.profinet.com/technology/profinet/, accessed: 2016-09-26.

(3) FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

(4) Maene P., Verbauwhede I. (2016) Single-Cycle Implementations of Block Ciphers. In: Güneysu T., Leander G., Moradi A. (eds) Lightweight Cryptography for Security and Privacy. Lecture Notes in Computer Science, vol 9542. Springer, Cham

(5) Bassham L., Calik C., McKay K., Mouha N. und Turan M. S. , „Profiles for the Lightweight Cryptograohy Standardization Process,“ NIST - National Institute of Standards and Technology, 2017.

(6) Rogaway P., “Evaluation of Some Blockcipher Modes of Operation”, Evaluation carried out for the Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, University of California, 2011

NOKIA


NOKIA

Backup

Copyright and confidentiality

Revision history and metadata

Please delete this slide if document is uncontrolled

Document ID: DXXXXXXXXX
Document Location:
Organization:

Version	Description of charges	Date	Author	Owner	Status	Reviewed by	Reviewed date	Approver	Approval date
		DD-MM-YYYY					DD-MM-YYYY		DD-MM-YYYY