POLITECHNIKA POZNAŃSKA
POZNAN UNIVERSITY OF TECHNOLOGY

NAWA
NARODOWA AGENCJA WYMIANY AKADEMICKIEJ

SDSU San Diego State University

Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework

Poznan Workshop, October 2024

Lightweight Cryptography

Poznan University of Technology

PhD DSc. Eng. Paweł Śniatała, prof. PP
PhD Eng. Anna Grocholewska-Czuryło
MSc. Marek Fechner
MSc. Eng. Konrad Śniatała
Eng. Szymon Baliński

Poznan Workshop, October 2024

Agenda

1. Lightweight Cryptography
2. Criteria when choosing an algorithm
3. NIST LWC Competition
4. List of lightweight cryptographic algorithms
5. Future works

Lightweight Cryptography

- What is the difference between cryptography and lightweight cryptography?
- Role of the lightweight cryptography in IoT
- Lightweight cryptography in UVAs

https://www.adsgroup.org.uk/knowledge/countering-the-malicious-usage-of-drones/

Criteria when choosing an algorithm (I)

1. Security:
- Cryptographic Resistance
- Key and block length
- Analysis and verification

2. Performance:
- Capacity
- Delay

3. Resource Consumption:
- Memory
- Energy

4. Implementation complexity:
- Ease of implementation
- Potential Errors

5. Resistance to side-channel attacks:
- Physical attacks
- Protection measures

6. Licensing and Intellectual Property:
- Licensing
- Open Source

Criteria when choosing an algorithm (II)

7. Compliance with standards:

- International standards
- Interoperability

8. Scalability and Flexibility:

- Adaptability
- Support for different platforms

9. Implementation experience:

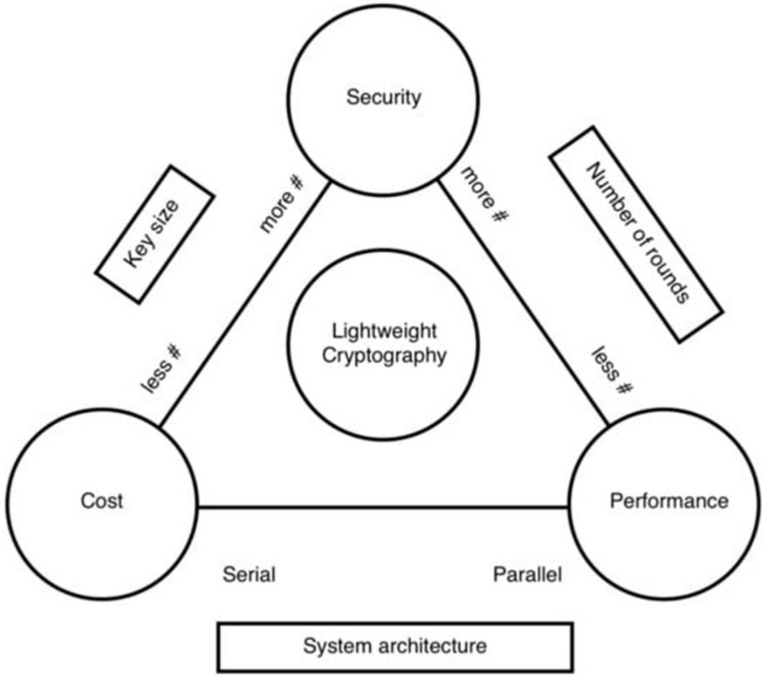
- Case studies
- Community and support

https://www.nokia.com/sites/default/files/2022-01/cybersecurity4_0.jpg

POLITECHNIKA POZNAŃSKA

NIST LWC Competition

- National Institute of Standards and Technology
- Genesis of the Contest
- Contest Goals
- Contest Phases



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

https://csrc.nist.gov/projects/lightweight-cryptography

ASCON

	Ascon-128	Ascon-128a
State(Bits)	320	320
Key(Bits)	128	128
Rate/Block (Bits)	64	128
Security (Bits)	128	128

- **Type**: Sponge
- **Mode of operation**: Duplex

- Winner of the NIST competition
- Uses only bitwise operations
- Resistant to side-channel attacks

A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses, Hasindu Madushan, DOI: 10.3390/electronics11244199

PHOTON-Beetle

	PHOTON-Beetle-AEAD[128]	PHOTON-Beetle-AEAD[32]
State(Bits)	256	256
Key(Bits)	128	128
Rate/Block (Bits)	128	32
Security (Bits)	121	128

- **Type**: Sponge
- **Mode of operation**: Beetle

- Finalist of the NIST competition
- Uses Beetle Sponge
- Resistant to multi-block manipulation attack

A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses, Hasindu Madushan, DOI: 10.3390/electronics11244199

POLITECHNIKA POZNAŃSKA

TinyJAMBU

	TinyJambu
State(Bits)	128
Key(Bits)	128
Rate/Block (Bits)	32
Security (Bits)	120

- **Type**: Sponge
- **Mode of operation**: TinyJambu

- Finalist of the NIST competition
- Uses Nonlinear-feedback shift register
- Resistant to abuses nonce
- Prepared to perform parallel

A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses, Hasindu Madushan, DOI: 10.3390/electronics11244199

ISAP

	ISAP-K-128	ISAP-A-128
State(Bits)	400	320
Key(Bits)	128	128
Rate/Block (Bits)	144	64
Security (Bits)	128	128

- **Type**: Sponge
- **Mode of operation**: ISAP

- Finalist of the NIST competition
- Different permutations in variants
- Re-keying function
- Uniqueness of the nonce

A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses, Hasindu Madushan, DOI: 10.3390/electronics11244199

Grain

	Grain-128AEAD
State(Bits)	256
Key(Bits)	128
Rate/Block (Bits)	1
Security (Bits)	128

- **Type**: Stream
- **Mode of operation**: N/A

- Finalist of the NIST competition
- Only stream cipher in final
- Two main components
- Fault attacks

A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses, Hasindu Madushan, DOI: 10.3390/electronics11244199

Fault Analysis of GRAIN-128, Alexandre Berzati, DOI: 10.1109/HST.2009.5225030

ACORN

	ACORN-128
State(Bits)	293
Key(Bits)	128
Rate/Block (Bits)	1
Security (Bits)	128

- **Type**: Stream
- **Mode of operation**: N/A

- Finalist of the CAESAR competition
- Prepared to perform parallel
- Linear-feedback shift register

Shi, Tairong, i Jie Guan. „Cryptanalysis of the Authentication in ACORN". KSII Transactions on Internet and Information Systems 13, nr 8 (2019): 4060–4075. https://doi.org/10.3837/tiis.2019.08.013.

PRESENT

	PRESENT
State(Bits)	64
Key(Bits)	80 or 128
Rate/Block (Bits)	64
Security (Bits)	80 or 128

- **Type**: Block
- **Mode of operation**: N/A

- PRESENT is included in the following standards:
  - ISO/IEC 29167-11:2014
  - ISO/IEC 29192-2:2019

· Ultra Low-Power Encryption/Decryption Core for Lightweight IoT Applications.”, Zaky, Ahmed, https://doi.org/10.1109/ICENCO48310.2019.9027471

Future work

- Classification of algorithms according to the presented criteria
- Choice of encryption key management method
- Selecting algorithms and testing
- Implementing selected algorithm

References (I)

- Madushan, Hasindu, Iftekhar Salam, i Janaka Alawatugoda. „A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses”. Electronics 11, nr 24 (2022): 4199. https://doi.org/10.3390/electronics11244199.
- Dobraunig, Christoph, Maria Eichlseder, Florian Mendel, i Martin Schläffer. „Ascon v1.2: Lightweight Authenticated Encryption and Hashing”. Journal of Cryptology 34, nr 3 (2021): 33. https://doi.org/10.1007/s00145-021-09398-9.
- Berzati, Alexandre, Cecile Canovas, Guilhem Castagnos, Blandine Debraize, Louis Goubin, Aline Gouget, Pascal Paillier, and Stephanie Salgado. „Fault Analysis of GRAIN-128.” In 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, 7+. San Francisco, CA, July 27, 2009. https://doi.org/10.1109/HST.2009.5225030.
- Zaky, Ahmed, Eslam Elmitwalli, Mostafa Hemeda, Yehea Ismail, and Khaled Salah. „Ultra Low-Power Encryption/Decryption Core for Lightweight IoT Applications.” In 2019 15th International Computer Engineering Conference (ICENCO), 39–43. Cairo, Egypt, December 2019. https://doi.org/10.1109/ICENCO48310.2019.9027471.
- Shi, Tairong, i Jie Guan. „Cryptanalysis of the Authentication in ACORN”. KSII Transactions on Internet and Information Systems 13, nr 8 (2019): 4060–4075. https://doi.org/10.3837/tiis.2019.08.013.

POLITECHNIKA POZNAŃSKA

Thank you very much.