Recent Advances & Trends in Lightweight Cryptography for IoT Security

Nilupulee A. Gunathilake, Ahmed Al-Dubai and William J. Buchanan
School of Computing, Edinburgh Napier University

Abstract

Lightweight cryptography is a novel diversion from conventional cryptography to minimise its high level of resource requirements, thus it would impeccably fit in the IoT environment. The IoT platform is constrained in terms of physical size, internal capacity, other storage allocations like RAM/ROM and data rates. However, provision of sufficient security is challenging because the existing cryptographic methods are too heavy to adopt in the IoT. Consequently, an interest arose in the recent past to construct new cryptographic algorithms in a lightweight scale.

This effort bridges **all areas in lightweight cryptography** (history, development & cryptanalysis)

Introduction

Lightweight cryptography is categorised as symmetric, asymmetric and hash. Many symmetric and hash implementations are available to try in practical systems, *i.e., PRESENT, KLEIN, PHOTON, etc.*, whereas a few asymmetric algorithms are accessible, *i.e., ELLI derived from ECC*.

- ❑ **Ultra-lightweight:** Tailored in specific areas of the algorithm, *i.e., selected µCs/cipher sections/operations – PRESENT, Grain (low gate count in hardware), Quarma (low latency in hardware) and Chaskey (high speed on µCs)*
- ❑ **Ubiquitous lightweight:** Compatible with wide variety of platforms, i.e., 8b to 32b µCs – Ascon, GIMLI and AES

Inventions, observations and adaption of lightweight cryptography are still emerging. This complete survey summarises the history, development of all available algorithm types followed by standardisation process, benchmarking and finally, security analysis.

Development of Lightweight Cryptography

Symmetric Lightweight Cryptography

- **Block ciphers**: The highest contribution. KLEIN, Lilliput, PRESENT, Rectangle and Skinnyare known as ultra-light-weight because their key sizes, block sizes and computational rounds are in the least range. XTEA is contemplated to be super-fast.
- **Stream ciphers**: Enocoro-80, Grain and Trivium are known to be well suited in terms of light-weight primitives.
- **Dedicated AE**: A greater interest is seen in ARCON, Ascon and Hummingbird-2. Hummingbiard-2 is still vulnerable to differential attacks in a related key setting. Nonce misuses could be identified in Helix and FIDES.
- **MAC**: Chaskey is widely accepted which has 128b of IS, key and block sizes. The other ones are is SipHash, TuLP and LightMAC.

Asymmetric Lightweight Cryptography

ECC, ELLI and HECC are based on the elliptic curve. Alternative efforts are seen in post-quantum (ALIKE, CryptoGPS , etc.) and lattice (NTRU, etc.) cryptographic techniques.

Lightweight Hash: Keccak, Quark and SPONGENT are enhancing their versions. Some other methods are Armadillo, QUARK, Lesamnta-LW,GLUON and SPN-Hash.

Security Analysis

Cryptological Approaches

- A survey [1] mentions that it is possible to gain a 12%reduction in area and a 20% increase in speed via AES optimisation
- Researches [2] proposes trustworthy neighbourhood mechanism depending on the connection history
- Some studies propose improved key management methodologies that encourage each node on the network to have a different key. Then once a key is leaked, only that particular node would be at risk without compromising the entire network

Refer our paper for more…

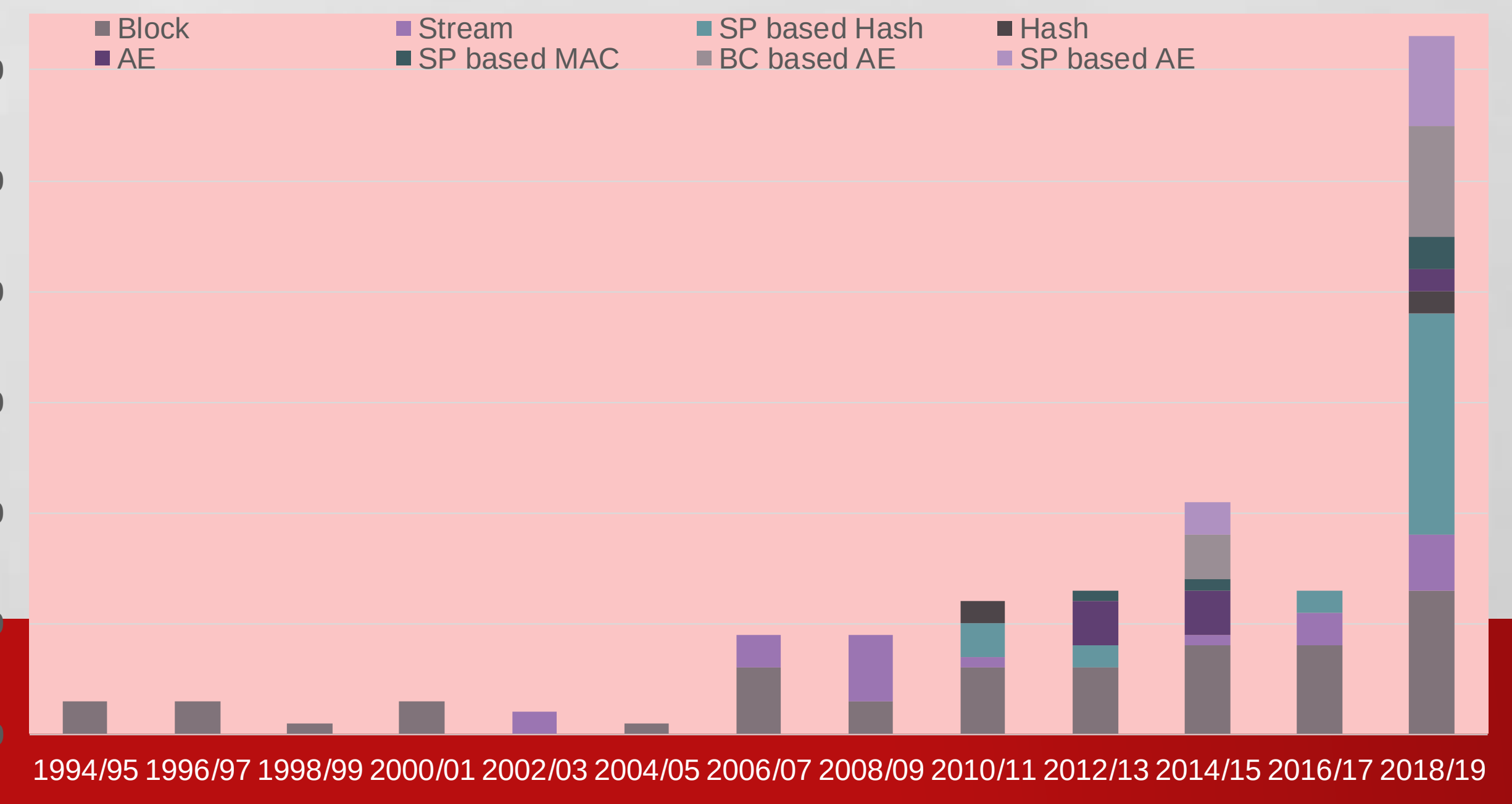
Cryptanalysis Approaches

- Study [3] presents the first third-party cryptanalysis of BORON against differential and linear criteria.
- Research [4] demonstrates optimal leakage models for CFA for SIMON, PRINCE and AES.
- A CPA on PRESENT [5] was able to derive the first 8B of the encryption key.
- Research [6] is about DEMA of PRESENT. It verifies the tamper resistance using several selection functions.
- Other vital impactors like optical, clock, cache and so on, based work are yet unavailable in side-channel robustness.

Table 1: Lightweight ciphers based on trending method.

Trend	Type	Examples
LUT	Non-linear	Piccolo, PRESENT, Prince
Bit-sliced based	Non-linear	3-Way, Ascon, iScream
ARX based	Non-linear	Chaskey, Hight, Speck, XTEA
MDS matrices	Linear	CLEFIA, LED, PHOTON
Bit permutations	Linear	FLY, RECTANGLE, Piccolo
XOR & rotations	Linear	Blake2s/b, GIMLI, Noekeon

Fig.1: Published lightweight algorithms from 1994-2019



Standardisation

The professional bodies involved are **government agencies, regional organizations and international associations.**

- FIPS 185 and 197 by the USA
- NESSIE and eSTREAM portfolio by the EU
- CRYPTREC by the government of Japan
- TTA by South Korea
- GOST R 34.12-2015 by the government of Russia
- ISO/IEC international standards in issues of 29167, 29192-2, 29192-3, 29192-5, 18033-3 and 18033-4
- NIST) standards in issues of NISTIR 8268 and NISTIR 8114

Benchmarking

General benchmarking measures are;

- 80b is the minimum security strength (112b is for long time requirements)
- 25% - 30% of minimum security margin adaption
- Hardware implementation to be up to standardised levels, *i.e., chip area, etc.*
- Software execution to be verified through standardised benchmarking tools, *i.e., FELICS*
- Clear licensing and liability where necessary
- Maturity of the cryptographic mechanism, *i.e., entropy*

FELICS is the utmost benchmarking tool for software implementations. Other contributors are XBX, BLOC project and CRYPTREC.

The ATHENa project and CRYPTREC are the main partners in hardware benchmarking.

Conclusions

- ❑ Lightweight cryptography is for IoT security
- ❑ Physical security is to be improved drastically
- ❑ Government agencies, regional organisations and international associations are involved in standardisation process
- ❑ FELICS is the predominating benchmarking tool
- ❑ Lightweight scripting languages to be improved

Contact Information

Nilupulee Gunathilake
Blockpass ID Lab, Edinburgh Napier University
Email: **nilupulee.gunathilake@napier.ac.uk**
Website: https://www.linkedin.com/in/nilupulee89/

References

1. I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptographyfor Internet of Insecure Things: A Survey," in 2019 IEEE 9th AnnualComputing and Communication Workshop and Conference (CCWC).IEEE, 01 2019, pp. 0475–0481, doi: 10.1109/CCWC.2019.8666557
2. S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Trusted Third Party BasedKey Management for Enhancing LoRaWAN Security," inIEEE/ACS14th International Conference on Computer Systems and Applications(AICCSA), 10 2017, pp. 1306–1313, doi: 10.1109/AICCSA.2017.73
3. H. Liang and M. Wang, "Cryptanalysis of the Lightweight Block CipherBORON,"Security and Communication Networks, vol. 2019, pp. 1–12,12 2019, doi: 10.1155/2019/7862738
4. A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De,and S. Mukhopadhyay, "Enhanced Power and Electromagnetic SCAResistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO,"IEEE Journal of Solid-State Circuits, 2019
5. O. Lo, W. J. Buchanan, and D. Carson, "Correlation Power Analysis onthe PRESENT Block Cipher on an Embedded Device," inProceedingsof the 13th International Conference on Availability, Reliability andSecurity, 2018, pp. 6–11, doi: 10.1145/3230833.3232801
6. Y. Nozaki, T. Iwase, Y. Ikezaki, and M. Yoshikawa, "DifferentialElectromagnetic Analysis for PRESENT and its Evaluation with SeveralSelection Functions,"Journal of International Council on ElectricalEngineering, vol. 7, no. 1, pp. 137–141, 2017, doi: 10.1080/22348972.2017.1344014