Lightweight Cryptography for the Internet of Things

Masanobu Katagi and Shiho Moriai

Sony Corporation

Abstract. This paper gives an overview of the state-of-the-art technology and standardization status of lightweight cryptography, which can be implemented efficiently in constrained devices. This technology enables secure and efficient communication between networked smart objects.

1 Introduction

On a new computing environment called "Internet of Things (IoT)" or "Smart Object" networks, a lot of constrained devices are connected to the Internet. The devices interact with each other through the network and provide new experience to us. In order to enjoy this new environment, security of constrained end nodes is important. If one of the nodes were compromised, the network might be suffered seriously. However, it is not easy to implement sufficient cryptographic functions on constrained devices due to the limitation of their resources.

2 Lightweight Cryptography

Cryptographic technologies are advancing: new techniques on attack, design and implementation are extensively studied. One of the state-of-the-art techniques is "Lightweight Cryptography (LWC)". Lightweight cryptography is a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, health-care devices and so on.

The properties of lightweight cryptography have already been discussed in ISO/IEC 29192 in ISO/IEC JTC 1/SC 27. ISO/IEC 29192 is a new standardization project of lightweight cryptography, and the project is in process of standardization. In ISO/IEC 29192, lightweight properties are described based on target platforms. In hardware implementations, chip size and/or energy consumption are the important measures to evaluate the lightweight properties. In software implementations, the smaller code and/or RAM size are preferable for the lightweight applications. From the view of the implementation properties, the lightweight primitives are superior to conventional cryptographic ones, which are currently used in the Internet security protocols, e.g. IPsec, TLS.

Lightweight cryptography also delivers adequate security. Lightweight cryptography does not always exploit the security-efficiency trade-offs. We report recent technologies of lightweight cryptographic primitives.

2.1 Symmetric Key Cryptography

Block ciphers. Since the Advanced Encryption Standard (AES) was selected, many block ciphers with lightweight properties have been proposed. Among them, CLEFIA [8] and PRESENT [3] are well-studied about their security and implementation. Both algorithms are under consideration in ISO/IEC 29192 "Lightweight Cryptography". The ciphers are ready to use in practical systems.

Stream ciphers. ECRYPT II eSTREAM project [10] held from 2004 to 2008 selected a portfolio of promising new stream ciphers. The current eSTREAM portfolio contains 7 algorithms. Grain v1, MICKEY v2, and Trivium have lightweight properties among these algorithms.

Hash functions. NIST's new cryptographic hash algorithm "SHA-3" competition attracts many people's attention. SHA-3 is expected to be a general-purpose hash function, and none of the current finalists do not satisfy lightweight properties. Research on lightweight dedicated hash functions has been just started [2]. They are too immature to adopt now. It is possible to construct lightweight hash functions based on lightweight block ciphers.

2.2 Public Key Cryptography

While lightweight public key primitives are in demand for key management protocols in smart objects networks, the required resource for public key primitives is much larger than that of symmetric key primitives. At this time, there are no promising primitives that meet enough security and lightweight properties compared with the conventional primitives such as RSA and ECC. Some public key primitives (e.g. ECC) can be implemented with relatively small footprint, but they cannot execute within a reasonable time.

3 Why is lightweight cryptography required for IoT?

We propose to adopt new advancing technology, "Lightweight Cryptography", in the IoT. We describe two reasons that support our proposal.

1. Efficiency of end-to-end communication
   In order to achieve end-to-end security, end nodes have an implementation of a symmetric key algorithm. For the low resource-devices, e.g. battery-powered devices, the cryptographic operation with a limited amount of energy consumption is important. Application of the lightweight symmetric key algorithm allows lower energy consumption for end devices.
2. Applicability to lower resource devices
   The footprint of the lightweight cryptographic primitives is smaller than the conventional cryptographic ones. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices.

A comparison of the lightweight properties with the conventional cryptographic primitives is shown in Appendix. The comparison in Appendix focuses on hardware properties. Some end nodes might be able to embed general-purpose micro-processors and software properties are considered important in such platforms. However, lowest cost devices can embed only application-specific ICs due to limited cost and power consumption, where hardware properties are crucially important.

4 Conclusion

Lightweight cryptography contributes to the security of smart objects networks because of its efficiency and smaller footprint. We believe that lightweight primitives should be considered to be implemented in the networks. Especially, lightweight block ciphers are practical to use now.

References

1. T. Akishita and H. Hiwatari, "Compact Hardware Implementations of the 128-bit Blockcipher CLEFIA." in *Proceedings of Symposium on Cryptography and Information Security –SCIS 2011 (in Japanese)*, 2011.
2. J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A Lightweight Hash." in *CHES 2010*, no. 6225 in LNCS, pp. 1–15, Springer-Verlag, 2010.
3. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher." in *CHES 2007*, no. 4727 in LNCS, pp. 450–466, Springer-Verlag, 2007.

4. M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES Implementation on a Grain of Sand." *IEE Proceedings Information Security*, vol. 152, pp. 13 – 20, 2005.
5. P. Hämäläinen, T. Alho, M. Hännikäinen, and T. D. Hämäläinen, "Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core." in *DSD 2006*, pp. 577–583, IEEE Computer Society, 2006.
6. A. Poschmann, "Lightweight Cryptography – Cryptographic Engineering for a Pervasive World." in *IACR ePrint archive 2009/516*, 2009.
7. A. Satoh and S. Morioka, "Hardware-focused performance comparison for the standard block ciphers AES,Camellia, and Triple-DES." in *Proceedings of ISC 2003* (C. Boyd and W. Mao, eds.), no. 2851 in LNCS, pp. 252–266, Springer-Verlag, 2003.
8. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA." in *Proceedings of Fast Software Encryption – FSE'07* (A. Biryukov, ed.), no. 4593 in LNCS, pp. 181–195, Springer-Verlag, 2007.
9. T. Sugawara, N. Homma, T. Aoki, and A. Satoh, "High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA." in *ISCAS2008*, pp. 2925–2928, 2008.
10. "The eSTREAM project." 2004–2008. `http://www.ecrypt.eu.org/stream/`.

Appendix A Hardware Properties of Lightweight Block Ciphers

Gate Efficiency

Figure 1 shows hardware efficiency of 128-bit block ciphers. Hardware efficiency is defined as the ratio of throughput (speed) to gate size (area). In this graph, higher slope (marked yellow area) indicates higher efficiency, which leads to low energy consumption. This figure compares a lightweight block cipher CLEFIA with conventional block ciphers: AES (FIPS197), Camellia (RFC3713), and SEED (RFC4269). These ciphers are also used in TLS/IPsec. CLEFIA has an advantage in hardware gate efficiency over these ciphers.

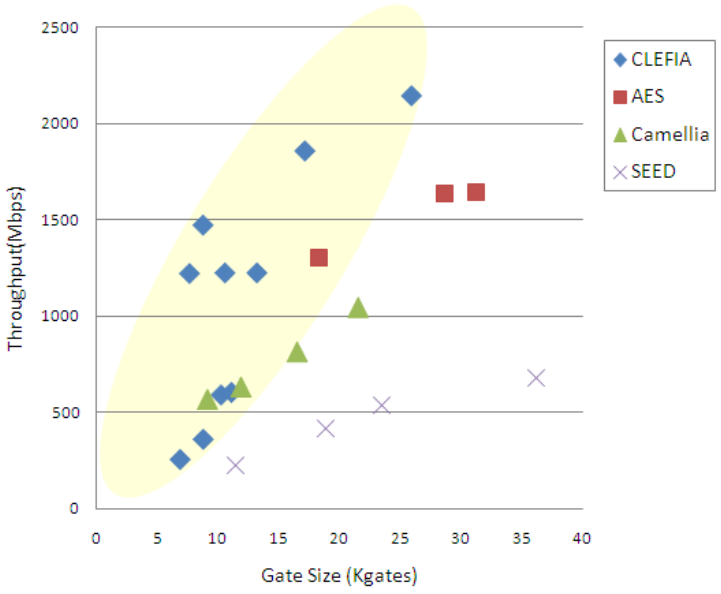

Figure 1. Gate efficiency (ASIC): CLEFIA and TLS/IPsec ciphers [9]

Hardware Performance

Hardware performance of the lightweight block ciphers is shown in Table 1. PRESENT and CLEFIA are the lightweight block ciphers proposed and under consideration in ISO/IEC 29192-2. For reference, the results of AES are shown in the table. The "area" is a metric for cost and power consumption when the chip is clocked at a low frequency of a few hundred kHz. The product of "area" and "cycle" is a metric for energy consumption. Table 1 shows that the lightweight ciphers can be implemented with smaller area and less energy consumption. Note that PRESENT is a 64-bit block cipher while CLEFIA and AES are 128-bit block ciphers. Generally speaking, 64-bit block ciphers can be implemented with smaller gate counts, but there are certain security limitations.

Table 1. Results on Hardware Performance (ASIC): PRESENT and CLEFIA

	mode	block size [bits]	key size [bits]	cycle	area [GE]	frequency [MHz]	throughput [Mbps]	technology [μm]
Serialized Implementation (Area Optimization)								
PRESENT [6]	enc	64	80	547	1075	0.1	0.0117	0.18
PRESENT [6]	enc	64	128	559	1391	0.1	0.0115	0.18
CLEFIA [1]	enc	128	128	176	2893	67	49	0.13
CLEFIA [1]	enc/dec	128	128	176	2996	61	44	0.13
AES [5]	enc	128	128	177	3100	152	110	0.13
AES [4]	enc/dec	128	128	1032	3400	80	10	0.35
Round-based Implementation (Efficiency Optimization)								
PRESENT [6]	enc	64	80	32	1570	0.1	0.20	0.18
PRESENT [6]	enc	64	128	32	1884	0.1	0.20	0.18
CLEFIA [8]	enc/dec	128	128	36	4950	201.3	715.69	0.09
CLEFIA [8]	enc/dec	128	128	18	5979	225.8	1605.94	0.09
AES [7]	enc/dec	128	128	11	12454	145.4	1691.35	0.13
AES [7]	enc/dec	128	128	54	5398	131.2	311.09	0.13