Performance Evaluation of NIST LWC Finalists on AVR ATmega and ARM Cortex-M3 Microcontrollers

Yuhei Watanabe[1,3], Hideki Yamamoto[1,2], Hirotaka Yoshida[1,3]

[1] SEI-AIST Cyber Security Cooperative Research Laboratory
[2] Sumitomo Electric Industries, Ltd. (SEI)
[3] National Institute of Advanced Industrial Science and Technology (AIST)

Abstract. This paper presents results of performance evaluation of NIST Lightweight Cryptography standardization finalists which are implemented by us. Our implementation method puts on the target to reduce RAM consumption on embedded devices. Our target microcontrollers are AVR ATmega 128 and ARM Cortex-M3. We apply our implementation method to five AEAD schemes which include four finalists of the NIST lightweight cryptography standardization and demonstrate the performance evaluation on target microcontrollers. From our performance evaluation of the RAM size, we have achieved 117-byte TinyJAMBU-128 on ATmega 128 and 140-byte TinyJAMBU-128 on ARM Cortex-M3. Our implementation of TinyJAMBU-128 has the smallest RAM of all the target AEAD schemes.

Keywords: RAM-optimized implementation · NIST Lightweight Cryptography Standardization · ATmega 128 · ARM Cortex-M3

1 Introduction

With the spread of IoT devices in several products, secure communication becomes an important issue in IoT devices. Since IoT devices often have restricted resources, there have been many studies about lightweight ciphers which can be performed with low computational resources. The research activity has led to an industrial standardization development project. In 2015, NIST have initiated the lightweight cryptography standardization process to standardize Authenticated Encryption with Associated Data (AEAD) and hashing schemes. NIST have announced ten finalists of this standardization process in 2021.

Regarding platforms for embedded devices for IoT applications, the AVR architectures and the ARM architectures are important architectures. The microcontrollers employed these architectures are used in several studies of performance evaluation of symmetric cryptographic primitives [EGG+12, BEE+12, PV13, SAK18, DBG+, SS16]. The performance evaluation of NIST standardization candidates also use these architectures [dSGB19, Gou19, Tea, Wea, RPM20]. There are several microcontrollers employing these architectures. For instance, the ATmega and the ARM Cortex-M3 are employed in various microcontrollers having different resources of the memory and/or frequency [Atm, Mica, Micb, Tex, NXP, Sil]. In ATmega48PA [Mica], there is 512 bytes of SRAM. There is a case that a cryptographic technique is applied to IoT devices employing such restricted microcontroller.

It is considered that a security protection function is one of the various functions which are worked on IoT devices. When a security protection technique is applied to resource constrained IoT devices, it would be important that the security protection

Table 1: Our results of the RAM size when taking 16-byte associated data and 16-byte message as input

Architecture	Scheme	RAM (ENC) [byte]	RAM (DEC) [byte]
ATmega 128	ASCON-128	157	181
	Grain-128AEADv2	145	147
	TinyJAMBU-128	117	119
	Xoodyak	167	183
ARM Cortex-M3	ASCON-128	196	212
	Grain-128AEADv2	224	232
	TinyJAMBU	140	140
	Xoodyak	208	232

technique is implemented with small resources in order to build all functions on the IoT device. There are multiple elements in cryptographic mechanisms to establish the secure communication. A cryptographic primitive is the basic element for the security protection. By implementing a cryptographic primitive with small resources, amount of resources for the security protection becomes small. As mentioned before, since there is the microcontroller which has small RAM, we consider that the reduction of the RAM consumption for the cryptographic primitive would be important.

Our contribution. This paper shows the results of the performance evaluation of finalists on the NIST lightweight cryptography standardization process. Our study explores the RAM-optimized software implementation technique on microcontrollers. Our target microcontrollers are ATmega 128 and ARM Cortex-M3. We evaluate the performance of AEAD schemes which are included in NIST standardization finalists. Our target primitives are AES-128-GCM, ASCON-128 [DEMS21], Grain-128AEADv2 [HJM+21], TinyJAMBU-128 [WH21], and Xoodyak [DHM+21]. We apply our implementation technique to target primitives. Table 1 shows the summary of the RAM size obtained by our evaluation. In our evaluation, we achieve 117-byte TinyJAMBU-128 on ATmega 128 and 140-byte TinyJAMBU-128 on ARM Cortex-M3. Our implementation of TinyJAMBU-128 has the smallest RAM of all the target AEAD schemes.

2 Target architectures

2.1 AVR ATmega Architecture

An AVR ATmega microcontroller is developed by Atmel, and now manufactured by Microchip Technology. This microcontroller is applied to devices for the IoT system or the automotive system. This microcontroller uses a CPU with an advanced RISC architecture. Most of instructions can be executed in single clock cycle. There are 32 8-bit general purpose registers. Let `R0`, `R1`, ..., `R31` be general purpose registers. Six of the 32 registers such as (`R26`, `R27`), (`R28`, `R29`), (`R30`, `R31`) can be used as three 16-bit indirect address register pointers for Data Space addressing. These added function registers are the X-register, Y-register, and Z-register.

There are many microcontrollers employing the ATmega architecture. They have several resources of Flash and SRAM. For instance, there is 128 KB of Flash and 4KB of SRAM in ATmega 128 [Atm], 4KB of Flash and 512 bytes of SRAM in ATmega48PA [Mica], and 8KB of Flash and 1024 bytes of SRAM in ATmega808 [Micb].

2.2 ARM Cortex-M3 Architecture

An ARM Cortex-M3 microcontroller is a well-known 32-bit RISC microcontroller. This microcontroller is applied to IoT devices or smart home devices. There are many microcontrollers employing the ARM Cortex-M3 CPU. They have several resources of Flash and RAM. For instance, there is 320 KB of Flash and 16 KB of RAM in TI TMS470MF03107 [Tex], 32 KB of Flash and 8 KB of RAM in NXP LPC1751 [NXP], and 4 KB of Flash and 2 KB of RAM in Silicon Labs EFM32TG108F4-QFN24 [Sil]. The 32-bit Atmel SAM3X8 Cortex-M3 CPU is employed in the Arduino Due board [Ard]. In its Harvard memory architecture, there is 512 KB of Flash and 96 KB of SRAM.

3 Performance Evaluation of NIST LWC Candidates

3.1 Implementation approach

Our target AEAD schemes are ASCON-128, Grain-128AEADv2, TinyJAMBU-128, and Xoodyak. We implement target AEAD schemes to evaluate their performance on microcontrollers. For comparison, we also implement AES-128-GCM and evaluate it. In our implementation, we try to reduce the RAM consumption by exploring the relationship between the RAM consumption and the structure of the target architecture.

3.2 Evaluation enviroment

In order to evaluate performance of AEAD schemes, we extend the FELICS framework [Cry]. FELICS is the free and open-source benchmarking tool designed for software implementations of lightweight cryptographic primitives on the microcontrollers. There are two previous works. FELICS-AEAD [dSGB19] and FELICS-AE [Gou19] are frameworks which extend FELICS to evaluate performance of AEAD schemes. FELICS-AEAD has quite different APIs from NIST APIs for AEAD schemes. Since evaluation results published from FELICS-AE is the rough, this framework would be not suited for detailed evaluation. Therefore, we extend the FELICS framework by ourselves. We introduce the evaluation framework for AEAD schemes into FELICS. Our framework evaluates the ROM size, the RAM size, and the number of cycles in both of encryption and decryption process in AEAD scheme.

3.3 Performance evaluation of target AEAD schemes

We evaluate the performance of our implementations of target AEAD schemes when taking 16-byte associated data and 16-byte message as input. Table 2 and 3 show the results of our evaluation on target devices. Note that we obtain these results by using the compiler option -O3. Figure 1 and 2 show the summary of the RAM consumption in the encryption process on each microcontroller.

3.4 Observations

According to Table 2 and 3, TinyJAMBU-128 has the smallest memory consumption in evaluated AEAD schemes on each target microcontroller. In our evaluation, TinyJAMBU-128 requires 117 RAM bytes for the encryption, 119 RAM bytes for the decryption, and 3890 ROM bytes on ATmega 128, and requires 140 RAM bytes for encryption/decryption and 2096 ROM bytes on ARM Cortex-M3. Xoodyak is the fastest primitive in evaluated AEAD schemes on each microcontroller.

According to Table 2, ASCON-128 on ATmega 128 requires the largest ROM in evaluated primitives. On the other hand, the third largest ROM is required by ASCON-128

Table 2: Evaluation results on AVR ATmega 128 with 16-byte associated data and 16-byte message as input

Name	ROM [byte]	RAM (ENC) [byte]	RAM (DEC) [byte]	# cycles (ENC) @16MHz	# cycles (DEC) @16MHz	Time (ENC) [ms]	Time (DEC) [ms]
ASCON-128	9732	157	181	93452	93821	5.84	5.86
Grain-128AEADv2	6098	145	147	124927	125334	7.81	7.83
TinyJAMBU-128	3890	117	119	163210	163276	10.20	10.20
Xoodyak	4306	167	183	52026	51639	3.25	3.23
AES-128-GCM	7358	259	264	175810	176061	10.99	11.00

Table 3: Evaluation results on ARM Cortex-M3 with 16-byte associated data and 16-byte message as input

Name	ROM [byte]	RAM (ENC) [byte]	RAM (DEC) [byte]	# cycles (ENC) @84MHz	# cycles (DEC) @84MHz	Time (ENC) [ms]	Time (DEC) [ms]
ASCON-128	4764	196	212	25488	25737	0.30	0.31
Grain-128AEADv2	6680	224	232	49919	49701	0.59	0.59
TinyJAMBU-128	2096	140	140	28427	28441	0.34	0.34
Xoodyak	3572	208	232	16212	16070	0.19	0.19
AES-128-GCM	5724	432	416	159651	159750	1.90	1.90

on ARM Cortex-M3. According to Table 2 and 3, while TinyJAMBU-128 on ATmega 128 is the slowest primitive except for AES-128-GCM, it on ARM Cortex-M3 shows almost same speed with ASCON-128. Since our implementation is optimized for the RAM consumption, these events would be caused from tradeoffs between metrics on each architecture.

4 Limitation

Implementations secure against side channel attacks such as timing attacks and simple/differential power analysis can be important in certain class of IoT applications but are not provided in our paper.

5 Related works

There are several studies of the software performance evaluation of candidates of the NIST standardization project. NIST LWC Team presents the benchmarking framework and shows the evaluation results on several microcontrollers such as AVR ATmega and ARM Cortex-M [Tea]. In [Wea], the evaluation results on 8-bit AVR platforms and ARM Cortex-M3 are shown. The performance evaluation on AVR, ARM, and RISC-V microcontrollers is shown in [RPM, RPM20]. In [CJL+20], the evaluation results on RISC-V are presented. Two AEAD evaluation frameworks based on FELICS [Cry] are proposed in [dSGB19] and [Gou19].

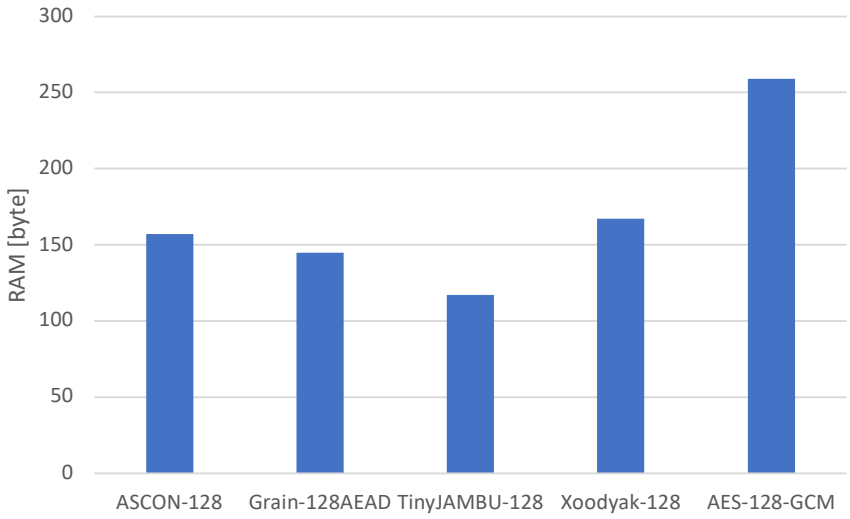

Figure 1: Comparison of RAM consumption for encryption on ATmega 128

6 Conclusion

This paper presented the results of the performance evaluation of the NIST Lightweight Cryptography standardization finalists. Our target primitives were AES-128-GCM, ASCON-128, Grain-128AEADv2, TinyJAMBU-128, and Xoodyak, and our target devices were ATmega 128 and ARM Cortex-M3. We implemented target primitives in terms of the optimization of the RAM consumption. From our performance evaluation, TinyJAMBU-128 required 117 RAM bytes on ATmega 128 and required 140 RAM bytes on ARM Cortex-M3. These results were the smallest RAM of all the target AEAD schemes.

References

[Ard] Arduino. Arduino due. Available: https://store.arduino.cc/usa/due.

[Atm] Atmel. ATmega128/L Datasheet. http://ww1.microchip.com/downloads/en/DeviceDoc/doc2467.pdf.

[BEE+12] Josep Balasch, Baris Ege, Thomas Eisenbarth, Benoît Gérard, Zheng Gong, Tim Güneysu, Stefan Heyse, Stéphanie Kerckhof, François Koeune, Thomas Plos, Thomas Pöppelmann, Francesco Regazzoni, François-Xavier Standaert, Gilles Van Assche, Ronny Van Keer, Loïc van Oldeneel tot Oldenzeel, and Ingo von Maurich. Compact implementation and performance evaluation of hash functions in attiny devices. In Smart Card Research and Advanced Applications - 11th International Conference, CARDIS 2012, Revised Selected Papers, volume 7771 of Lecture Notes in Computer Science, pages 158–172. Springer, 2012.

[CJL+20] Fabio Campos, Lars Jellema, Mauk Lemmen, Lars Müller, Daan Sprenkels, and Benoît Viguier. Assembly or optimized C for lightweight cryptography on risc-v? In Cryptology and Network Security - 19th International Conference, CANS 2020, Proceedings, volume 12579 of Lecture Notes in Computer Science, pages 526–545. Springer, 2020.

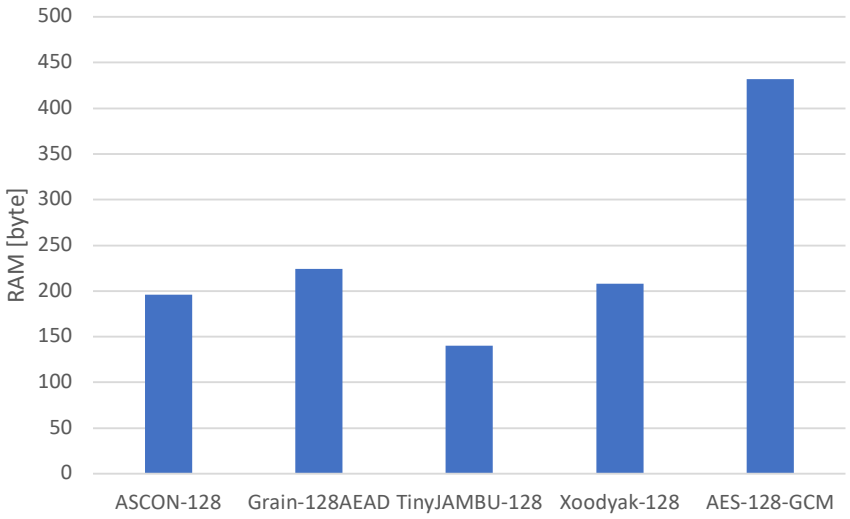

Figure 2: Comparison of RAM consumption for encryption on ARM Cortex-M3

[Cry] CryptoLUX. FELICS - fair evaluation of lightweight cryptographic systems. https://www.cryptolux.org/index.php/FELICS.

[DBG+] Daniel Dinu, Alex Biryukov, Johann Großschädl, Dmitry Khovratovich, Yann Le Corre, and Léo Perrin. FELICS - fair evaluation of lightweight cryptographic systems. NIST Lightweight Cryptography Workshop 2015, 2015.

[DEMS21] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf, 2021.

[DHM+21] Joan Daemen, Seth Hoffert, Silvia Mella, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Xoodyak, a lightweight cryptographic scheme. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/xoodyak-spec-final.pdf, 2021.

[dSGB19] Luan Cardoso dos Santos, Johann Großschädl, and Alex Biryukov. Felics-aead: Benchmarking of lightweight authenticated encryption algorithms. NIST Lightweight Cryptography Workshop 2019, 2019.

[EGG+12] Thomas Eisenbarth, Zheng Gong, Tim Güneysu, Stefan Heyse, Sebastiaan Indesteege, Stéphanie Kerckhof, François Koeune, Tomislav Nad, Thomas Plos, Francesco Regazzoni, François-Xavier Standaert, and Loïc van Oldeneel tot Oldenzeel. Compact implementation and performance evaluation of block ciphers in attiny devices. In Progress in Cryptology - AFRICACRYPT 2012 - 5th International Conference on Cryptology in Africa. Proceedings, volume 7374 of Lecture Notes in Computer Science, pages 172–187. Springer, 2012.

[Gou19] Kévin Le Gouguec. Felics-ae: a framework to benchmark lightweight autheticated block ciphers. NIST Lightweight Cryptography Workshop 2019, 2019.

[HJM+21] Martin Hell, Thomas Johannsson, Alexander Maximov, Willi Meier, Jonathan Sönnerup, and Hirotaka Yoshida. Grain-128aeadv2 - a lightweight aead stream cipher. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/grain-128aead-spec-final.pdf, 2021.

[Mica] Microchip Technology. ATmega48PA. https://www.microchip.com/wwwproducts/en/ATmega48PA.

[Micb] Microchip Technology. ATmega808. https://www.microchip.com/wwwproducts/en/ATMEGA808.

[NXP] NXP Semiconductors. Lpc1700 series: Scalable mainstream microcontrollers (mcus) based on arm cortex-m3 cores. Available: https://www.nxp.com/products/processors-and-microcontrollers/arm-based-processors-and-mcus/lpc-cortex-m-mcus/lpc1700-cortex-m3:MC_1403790745385#/.

[PV13] Konstantinos Papagiannopoulos and Aram Verstegen. Speed and size-optimized implementations of the PRESENT cipher for tiny AVR devices. In Radio Frequency Identification - Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Revised Selected Papers, volume 8262 of Lecture Notes in Computer Science, pages 161–175. Springer, 2013.

[RPM] Sebastian Renner, Enrico Pozzobon, and Jürgen Mottok. Nist lwc software performance benchmarks on microcontrollers. Available: https://lwc.las3.de/.

[RPM20] Sebastian Renner, Enrico Pozzobon, and Jürgen Mottok. A hardware in the loop benchmark suite to evaluate NIST LWC ciphers on microcontrollers. In Weizhi Meng, Dieter Gollmann, Christian Damsgaard Jensen, and Jianying Zhou, editors, Information and Communications Security - 22nd International Conference, ICICS 2020, Proceedings, volume 12282 of Lecture Notes in Computer Science, pages 495–509. Springer, 2020.

[SAK18] Hwajeong Seo, Kyuhwang An, and Hyeokdong Kwon. Compact LEA and HIGHT implementations on 8-bit AVR and 16-bit MSP processors. In Information Security Applications - 19th International Conference, WISA 2018, Revised Selected Papers, volume 11402 of Lecture Notes in Computer Science, pages 253–265. Springer, 2018.

[Sil] Silicon Laboratories. Efm32 tiny gecko 32-bit microcontroller. Available: https://www.silabs.com/products/mcu/32-bit/efm32-tiny-gecko.

[SS16] Peter Schwabe and Ko Stoffelen. All the AES you need on cortex-m3 and M4. In Selected Areas in Cryptography - SAC 2016 - 23rd International Conference, Revised Selected Papers, volume 10532 of Lecture Notes in Computer Science, pages 180–194. Springer, 2016.

[Tea] NIST LWC Team. Benchmarking of lightweight cryptographic algorithms on microcontrollers. Available: https://github.com/usnistgov/Lightweight-Cryptography-Benchmarking.

[Tex] Texas Instruments Incorporated. Microcontrollers (mcu) other mcus - products arm-cortex-m3. Available: http://www.ti.com/microcontrollers/other-mcus/products.html#p887=ARM-Cortex-M3.

[Wea] Rhys Weatherley. Lightweight cryptography primitives. Available: https://rweather.github.io/lightweight-crypto/.

[WH21] Hongjun Wu and Tao Huang. Tinyjambu: A family of lightweight authenticated encryption algorithms (version 2). Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf, 2021.