Preliminary Design of a Novel Lightweight Authenticated Encryption Scheme based on the Sponge Function

HakJu Kim and Kwangjo Kim
School of Computing
KAIST
Daejeon, Republic of Korea
{ndemian, kkj}@kaist.ac.kr

***Abstract*—The authenticated encryption plays a key cryptographic primitive that provides confidentiality, integrity, and authenticity in an efficient manner. This paper presents a preliminary design of a novel lightweight authenticated encryption scheme based on the duplex construction of the sponge function supporting the most required features of the authenticated encryption schemes.**

Keywords-Authenticated Encryption, Symmetric Key Cryptography, Sponge Function, CAESAR

To ensure the system security, the latest research was focused to develop the required cryptographic primitives to provide many security requirements especially CIA (Confidentiality, Integrity, Availability), independently. Cryptographic primitives like AES (Advanced Encryption Standard) and SHA-family (Secure Hash Algorithm) were developed to efficiently provide the security requirements like confidentiality and integrity, but each of them ensures only one aspect of the security requirements. Thus, modern IT systems are required to equip many different security algorithms like encryption, hash, IDS (Intrusion Detection System), etc. to meet all security requirements. The implementation of each security algorithm consumes the resources of the system, and the resource consumption can be reduced if one cryptographic primitive can provide two or more security requirements together.

Authenticated encryption is one of important cryptographic primitives using symmetric key cryptosystem to provide confidentiality, integrity, and authenticity at the same time. Some early authenticated encryption schemes like AES-CCM [1], AES-GCM [2], OCB [3] are standardized and recommended by many standardization organizations like NIST (National Institute of Standards and Technology). Furthermore, the research to develop more secure, efficient, and robust authenticated encryption scheme has been sparked. Bernstein and other cryptography researchers has launched the CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) competition [4] to select the next generation authenticated encryption scheme.

From the analysis of the authenticated encryption schemes submitted to the CAESAR competition [5], the supportability of features like provable security, parallelizability, onlineness, inverse-freeness, incremental AD/AE(Associated Data and Authenticated Encryption), intermediate tag, nonce-MR (nonce-Misuse Resistance), decryption-MR (decryption-Misuse Resistance), and no ciphertext expansion is important for the authenticated encryption.

We believe that the duplex construction of the sponge function is attractive to design an efficient authenticated encryption scheme supporting the most of the required features, because the performance and the security of the sponge function is proven rigorously and many features are included in the basic design of the duplex construction. Our design of the authenticated encryption scheme based on the sponge function is believed to support all of the most required features, and we include an efficient implementation of intermediate tag, nonce-MR, and decryption-MR to the design of the scheme.

The performance of the sponge-based authenticated encryption scheme is determined by the performance of the permutation block and the size of the bitrate in the sponge function. We propose that the lightweight authenticated encryption scheme based on the sponge function can be designed by using the efficient permutation block, which can be built with the combination of efficient nonlinear and linear layers. The multipermutation explained in [6] can be used to build an efficient linear layer.

According to [5, 7], IND-CPA and INT-CTXT are essential to consider an authenticated encryption scheme to be secure. The security of the sponge function is proven theoretically in [8], and the duplex construction inherits the security proof of the sponge function. In addition, Jovanovic *et al.* [9] prove a new security bound of the authenticated encryption scheme based on the sponge function and claim that the performance of the scheme can be improved without degrading the security bound by increasing the bitrate and by decreasing the capacity of the sponge function. Thus, our design maximizes the size of the bitrate and minimizes the size of the capacity to boost the performance.

The proposed authenticated encryption scheme based on the duplex construction of the sponge function is implemented in software, and we will analyze and compare the performance of the scheme with other authenticated encryption schemes submitted to the CAESAR competition. The security proof of the scheme is inherited from [8, 9], and the robustness of the permutation block will be analyzed via various cryptanalysis techniques.

978-1-4799-1989-5/15 $31.00 © 2015 IEEE
DOI 10.1109/AsiaJCIS.2015.24

ACKNOWLEDGMENT

This work was partly supported by the ICT R&D program of MSIP/IITP, Republic of Korea. [1391104001, Research on Communication Technology using Bio-inspired Algorithm] and the KUSTAR-KAIST Institute, KAIST, Korea.

REFERENCES

[1] D. Whiting, R. Housley, and N. Ferguson, "Counter with cbc-mac (CCM),". RFC 3610, September 2003.

[2] M. Dworkin, "NIST special publication 800-38D," NIST special publication, vol. 800, pp. 38D, 2007.

[3] P. Rogaway, M. Bellare, and J. Black, "OCB: A block-cipher mode of operation for efficient authenticated encryption," ACM Transactions on Information and System Security (TISSEC), vol. 6, no. 3, pp. 365-403, 2003.

[4] D. J. Bernstein, "CAESAR - competition for authenticated encryption: security, applicability, and robustness," 2014. [online]. Available at: http://competitions.cr.yp.to/caesar.html.

[5] F. Abed, C. Forler, and S. Lucks, "Classification of the CAESAR candidates," IACR Cryptology ePrint Archive, 2014.

[6] A. Mileva, "Multipermutations in crypto world: different faces of the perfect diffusion layer," Cryptology ePrint Archive, no. 85, 2014.

[7] M. Bellare and C. Namprempre, "Authenticated encryption: relations among notions and analysis of the generic composition paradigm," Journal of Cryptology, vol. 21, no. 4, pp. 469-491, 2008.

[8] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Duplexing the sponge: single-pass authenticated encryption and other applications," Selected Areas in Cryptography, Springer Berlin Heidelberg, pp. 320-337, 2012.

[9] P. Jovanovic, A. Luykx, and B. Mennink, "Beyond $2^{c/2}$ security in sponge-based authenticated encryption modes," Advances in Cryptology–ASIACRYPT 2014, Springer Berlin Heidelberg, pp. 85-104, 2014.