SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

September 2018, Vol. 61 098104:1–098104:3
https://doi.org/10.1007/s11432-017-9253-9

Efficient beyond-birthday-bound secure authenticated encryption modes

Ping ZHANG[1,2], Honggang HU[1,2*] & Peng WANG[3]

[1]*School of Information Science and Technology, University of Science and Technology of China, Hefei* 230027*, China;*
[2]*Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, Hefei* 230027*, China;*
[3]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100049*, China*

Received 9 June 2017/Accepted 20 September 2017/Published online 23 April 2018

Citation Zhang P, Hu H G, Wang P. Efficient beyond-birthday-bound secure authenticated encryption modes. Sci China Inf Sci, 2018, 61(9): 098104, https://doi.org/10.1007/s11432-017-9253-9

The privacy and authenticity of user information have received increasing attention, because information security incidents have occurred more frequently in recent years, such as the PRISM scandal and blackmail virus. In this context, privacy (also referred to as confidentiality) ensures that user information is not obtained by unauthorized third parties. Authenticity (also referred to as integrity) prevents unauthorized third parties from tampering, forging, or forwarding user information. An authenticated encryption (AE) mode is a cryptographic scheme that provides both privacy and authenticity simultaneously.

Most AE schemes simply offer birthday bound security, i.e., their privacy and authenticity ensure at most approximately $\frac{n}{2}$-bit security, where n is the block size. The current widely used block cipher is Advanced Encryption Standard (AES). If AES (block size $n = 128$) is used as the underlying primitive of an AE mode, then 128-bit security degrades to at most approximately 64-bit security. This means that the security insurance of this AE mode is lost after 2^{64} adversarial queries or forgery attempts, which is often unacceptable in some special environments. Similarly, for the current widely used hash functions SHA-256 and SHA-512, the birthday-bound-secure bottleneck still exists. Therefore, it is very important to design AE modes that provide beyond-birthday-bound (BBB) security. The so-called BBB security means that an AE mode guarantees at most approximately $\frac{rn}{r+1}$-bit security, where $r > 1$ is an integer. If r is sufficiently large, we consider that it provides asymptotically optimal security. If $r \to \infty$, we consider that it provides optimal security, i.e., this AE mode is secure up to approximately 2^n adversarial queries and approximately 2^n forgery attempts. In recent years, AE modes that provide BBB security appeared endless. According to the underlying primitive classification, this includes blockcipher-based BBB-secure AE modes (e.g., GCM-SIVr [1]), tweakable-blockcipher-based BBB-secure AE modes (e.g., SCT [2] and SIVx [3]), and permutation-based BBB-secure AE modes (e.g., NORX [4]). However, it remains an open problem to construct a BBB-secure AE mode based on a keyed compression function.

Contributions. This article addresses the above open problem. First, we describe the first keyed-function-based BBB-secure parallelizable AE mode RWCTR, which combines a modified Randomized Wegman-Carter-Shoup Message Authentication Code (RWMAC) [5] construction and a new randomized CTR-like mode. We utilize a $2n$-bit input and n-bit output keyed compression function, an n-bit random initial vector (IV), and a universal hash function with n-bit output to build RWCTR. RWCTR is provably BBB-secure up to approximately 2^{n-2} adversarial queries and

* Corresponding author (email: hghu2005@ustc.edu.cn)

approximately $2^n/n$ forgery attempts if the underlying keyed compression function is a secure pseudorandom function (PRF). RWCTR is also the first keyed-function-based AE mode that provides close-to-optimal security. The privacy and authenticity of RWCTR guarantee at most approximately $(n-2)$- and $(n-\log n)$-bit security, respectively. We also propose a more practical AE mode RWCTRN that utilizes a nonce IV or an arbitrary IV to replace the impractical random IV. RWCTRN provides provable security up to a close-to-optimal bound in the nonce IV scenario and achieves security up to the birthday bound in the arbitrary IV scenario.

Scheme 1: RWCTR. RWCTR was inspired by RWMAC [5] and BTM [6]. First, the authentication part of RWCTR takes two keys (L, K), an n-bit random IV U, associated data A, and a message M as input and yields an authentication tag T, i.e.,

$$S = H_L(A, M) \oplus U \text{ and } T = F_K(U, S), \quad (1)$$

where H is an ϵ-uniform almost-XOR-universal (AXU) hash function (Appendix B) and F is a keyed compression function. The authentication part of RWCTR is a modified RWMAC mode that provides BBB security. Then, we construct a new random IV-based CTR-like mode that takes key K, authentication tag T, random IV U, and message $M = M_1||\cdots||M_l$ as input and returns the corresponding ciphertext $C = C_1||\cdots||C_l$, i.e.,

$$C_i = F_K(U, T+i) \oplus M_i, \text{ where } 1 \leqslant i \leqslant l. \quad (2)$$

Unlike BTM [6], we replace the block cipher with the keyed compression function and utilize a random IV U. This makes the encryption part of RWCTR BBB-secure. An overview of RWCTR is given in Figure 1(a). The RWCTR encryption and decryption algorithms are shown in Appendix C.1. The privacy and authenticity of RWCTR are described as follows.

Theorem 1. Let $\mathcal{A}$ be an adversary that makes at most q encryption queries and q_v forgery attempts to RWCTR and runs in at most t time. Then, there exists an adversary $\mathcal{B}$ against the PRF-security of F that makes at most σ oracle queries and runs in at most $t' = t + O(n\sigma)$ time. For $q \leqslant \min\{2^{n-2}, \sqrt{2^n\epsilon^{-1}}\}$, we have

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{RWCTR[F]}}(\mathcal{A}) \leqslant \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{q^2\epsilon}{2^{n+1}} + \frac{3\sigma}{2^{n+1}}, \quad (3)$$

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{RWCTR[F]}}(\mathcal{A}) \leqslant \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{q^2\epsilon}{2^{n+1}} + \frac{3\sigma}{2^{n+1}} + q_v(n-1)\epsilon + \frac{2q_v}{2^n}. \quad (4)$$

According to Theorem 1, assume that F is a secure PRF, i.e., $\mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B})$ is negligible, and let $\epsilon \simeq 2^{-n}$, then the privacy of RWCTR is secure up to $q = O(2^{n-2})$ adversarial queries, and the authenticity of RWCTR is secure up to $q = O(2^{n-2})$ adversarial queries and $q_v = O(2^n/n)$ forgery attempts. In other words, the privacy of RWCTR ensures at most approximately $(n-2)$-bit security and the authenticity of RWCTR ensures at most approximately $\min\{(n-2), (n-\log n)\} = (n-\log n)$-bit security. RWCTR achieves close-to-optimal security in the information-theoretic setting. The security proof of Theorem 1 is presented in Appendix C.2.

Scheme 2: RWCTRN. The random IV used in RWCTR is impractical. In the real world, we typically use a nonce IV or arbitrary IV to replace a random IV. The nonce IV N can be converted to a random-like IV U by invoking an extra keyed compression function F_K, i.e., $U = F_K(N, 0^n)$. Therefore, we improve RWCTR and propose a more practical AE mode RWCTRN. An overview of RWCTRN is given in Figure 1(b). The RWCTRN encryption and decryption algorithms are shown in Appendix D.1. The privacy and authenticity of RWCTRN are described as follows.

Theorem 2. Let $\mathcal{A}$ be an adversary that makes at most q encryption queries and q_v forgery attempts to RWCTRN and runs in at most t time. Then, there exists an adversary $\mathcal{B}$ against the PRF-security of F that makes at most σ oracle queries and runs in at most $t' = t + O(n\sigma)$ time.

(1) In the nonce IV scenario, for $q \leqslant \min\{2^{n-2}, \sqrt{2^n\epsilon^{-1}}\}$, we have

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{RWCTRN[F]}}(\mathcal{A}) \leqslant \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{q^2\epsilon}{2^{n+1}} + \frac{2\sigma}{2^n}, \quad (5)$$

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{RWCTRN[F]}}(\mathcal{A}) \leqslant \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{q^2\epsilon}{2^{n+1}} + \frac{2\sigma}{2^n} + q_v(n-1)\epsilon + \frac{2q_v}{2^n}; \quad (6)$$

(2) In the arbitrary IV scenario, we have

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{RWCTRN[F]}}(\mathcal{A}) \leqslant \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{q^2\epsilon}{2} + \frac{\sigma^2}{2^n}, \quad (7)$$

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{RWCTRN[F]}}(\mathcal{A}) \leqslant \mathrm{Adv}^{\mathrm{prf}}_{F}(\mathcal{B}) + \frac{q^2\epsilon}{2} + \frac{\sigma^2}{2^n} + q_vq\epsilon + \frac{2q_v}{2^n}. \quad (8)$$

According to Theorem 2, assume that F is a secure PRF and $\epsilon \simeq 2^{-n}$, then, (1) in the nonce IV scenario, RWCTRN is proven secure up to

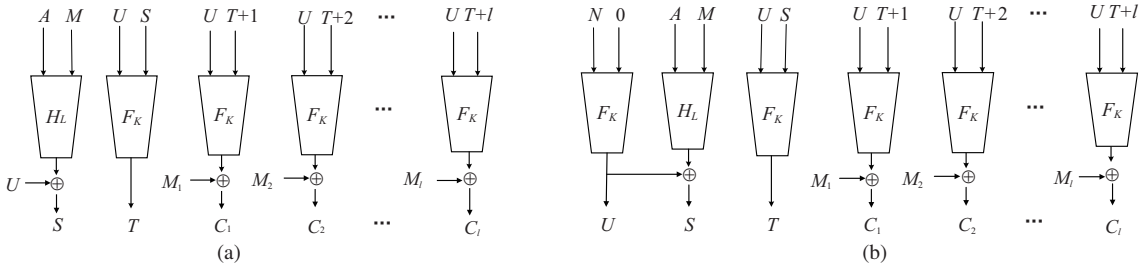

Figure 1 Keyed-function-based BBB-secure AE modes. (a) RWCTR with random IV U; (b) RWCTRN with nonce IV or arbitrary IV N.

$q = O(2^{n-2})$ adversarial queries and $q_v = O(2^n/n)$ forgery attempts, and, (2) in the arbitrary IV scenario, RWCTRN is proven secure up to $q = O(2^{n/2})$ adversarial queries and $q_v = O(2^{n/2})$ forgery attempts. In other words, the privacy of RWCTRN yields at most approximately $(n-2)$-bit security and the authenticity of RWCTRN ensures at most approximately $(n - \log n)$-bit security in the nonce IV scenario, while the privacy and authenticity of RWCTRN offer at most about $n/2$-bit security in the arbitrary IV scenario. The security proof of Theorem 2 is presented in Appendix D.2.

Discussion. RWCTR and RWCTRN are designed as AE modes for a compression function. From a security and efficiency perspective, RWCTR and RWCTRN are better than other keyed-function-based AE schemes under the same conditions. Details are available in Appendix E.

If the underlying keyed compression function is instantiated with a widely used hash function (e.g., SHA-256 and SHA-512), we can obtain some instances of our schemes. The instantiations of RWCTR and RWCTRN are shown in Appendix F.

In the arbitrary IV scenario, RWCTRN only ensures security up to the birthday bound. We leave it as an open problem to construct an efficient keyed-function-based AE mode that provides BBB-security and even optimal security for the arbitrary IV scenario.

Conclusion. In this article, we have discussed two efficient keyed-function-based BBB-secure parallelizable AE modes, i.e., RWCTR for a random IV and RWCTRN for a nonce or arbitrary IV. From a security perspective, if the underlying keyed compression function is a secure PRF, RWCTR provides close-to-optimal security, while RWCTRN provides close-to-optimal security in the nonce IV scenario and guarantees security up to the birthday bound in the arbitrary IV scenario. From an efficiency perspective, RWCTR minimizes the total number of underlying keyed compression function invocations. Our schemes have wide applications in cryptography. For example, they can be used in big data security, cloud security, network security, and many other settings.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61522210, 61632013).

Supporting information Appendixes A–F. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Iwata T, Minematsu K. Stronger security variants of GCM-SIV. IACR Trans Symmetric Cryptol, 2016, 2016: 134–157
2 Peyrin T, Seurin Y. Counter-in-tweak: authenticated encryption modes for tweakable block ciphers. In: Proceedings of the 36th Annual International Cryptology Conference, Santa Barbara, 2016. 33–63
3 List E, Nandi M. Revisiting full-PRF-secure PMAC and using it for beyond-birthday authenticated encryption. In: Proceedings of the Cryptographer's Track at the RSA Conference, San Francisco, 2017. 258–274
4 Jovanvic P, Luykx A, Mennink B. Beyond $2^{c/2}$ security in sponge-based authenticated encryption modes. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 85–104
5 Minematsu K. How to thwart birthday attacks against MACs via small randomness. In: Proceedings of the 17th International Workshop on Fast Software Encryption, Seoul, 2010. 230–249
6 Iwata T, Yasuda K. BTM: a single-key, inverse-cipher-free mode for deterministic authenticated encryption. In: Proceedings of the 16th Annual International Workshop on Selected Areas in Cryptography, Calgary, 2009. 313–330