A Blockcipher Based Authentication Encryption

Rashed Mazumder[2(✉)], Atsuko Miyaji[1,2,3], and Chunhua Su[1]

[1] Graduate School of Engineering, Osaka University, Osaka, Japan
{miyaji,su}@comm.eng.osaka-u.ac.jp
[2] Japan Advanced Institute of Science and Technology, Nomi, Japan
{miyaji,s1420213}@jaist.ac.jp
[3] Japan Science and Technology Agency (JST) CREST, Tokyo, Japan

Abstract. Authentication encryption (AE) is a procedure that satisfies both privacy and authenticity on the data. It has many applications in the field of secure data communication such as digital signatures, ip-security, data-authentication, e-mail security, and security of pervasive computing. Additionally, the AE is a potential primitive of security solution for IoT-end device, RfID, and constrained device. Though there are many constructions of AE, but the most important argument is whether the AE is secure under nonce-reuse or nonce-respect. As far our understanding, the McOE is the pioneer construction of nonce-reuse AE. Following that, many schemes have been proposed such as APE, PoE, TC, COPA, ElmE, ElmD, COBRA, and Minalphar. However, Hoang et al. (OAE1) claimed that the concept of nonce-reuse in the AE is not secure and proper. Hence, a door is re-opened for the nonce-respect AE. Moreover, the construction of AE should satisfies the properties of efficiency and upper security bound due to limitation of power and memory for the constrained device. Therefore, we propose a blockcipher based AE that satisfies upper privacy security bound $\left(\text{Priv} = O\left(2^{2n/3}\right)\right)$ and it operates in parallel mode. It doesn't need decryption oracle in the symmetric encryption module of the AE. The proposed construction satisfies padding free encryption. Furthermore, the efficiency-rate of the proposed scheme is 1.

Keywords: Blockcipher · Constrained device · Authentication · Compression function

1 Introduction

Authentication encryption (AE) is a procedure, where a sender sends data to a receiver in such a way that the receiver can identify whether the data is altered

This work is partially supported by the Grant-in-Aid for Scientific Research (C)(15K00183) and (15K00189) and Japan Science and Technology Agency, CREST and Infrastructure Development for Promoting International S&T Cooperation.
C. Su — JSPS Grant-in-Aid for Young Scientists (15K16005).

F. Buccafurri et al. (Eds.): CD-ARES 2016, LNCS 9817, pp. 106–123, 2016.
DOI: 10.1007/978-3-319-45507-5_8

or not [1–3]. Additionally, the AE checks the originality of the sender including message. There are many applications of AE in the field of secure communication such as digital signatures, ip-security, data-authentication, e-mail security, and IoT [18–21]. Furthermore, the AE is a potential primitive of cryptographic solutions for resource constrained device, and IoT-end device [36–38]. For example, there are numerous bunch of senders and receivers in the domain of data communication [4–8]. Hence, it is infeasible and expensive to establish private network for all parties [2,3,6–8]. Under this circumstance, the only way is to implement such a security solution under public network that ensures the privacy and authenticity of the data. Generally, the AE has two components such as symmetric encryption (SE) and message authentication code (MAC) [1–3,7]. The grammar of SE is $SE(K, M) \rightarrow C$, where K, M, and C means key, message and ciphertext respectively [2,3,9,10,30]. Moreover, the MAC inherits tag (T) and verification such as $MAC(K, C) \rightarrow T$ and $\mathsf{Verf}(K, C, T) \rightarrow M$ or $\perp$. Usually, the symmetric encryption ensures the privacy of data. In addition, the authenticity of the data is preserved by MAC [2,3,30]. For example, a doctor $\mathcal{D}_1$ needs to send medical report of a patient ($\mathcal{P}$) to doctor $\mathcal{D}_2$ for consulting (Fig. 1). Under this circumstance, it is mandatory to protect the confidentiality of the patient's report and record. Moreover, the originality of doctor $\mathcal{D}_1$ is also needed to verify as a valid sender. The combined form of the two different components of AE can achieve both the goals. Therefore, the summery of the functions of AE are:

– receiver can perceive the altered data
– infeasible for adversary to get success in forgery
– infeasible for adversary to retrieve the entire message

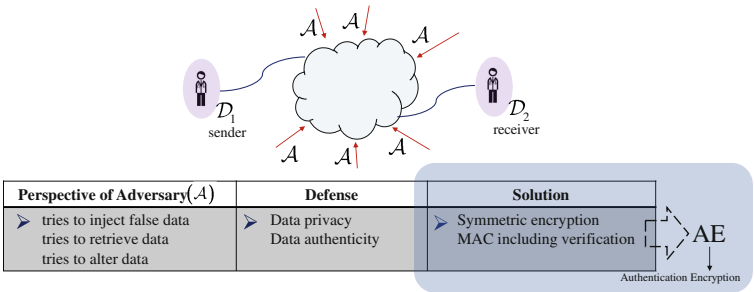

Fig. 1. Simple concept of AE

The AE is constructed through a scratch or blockcipher [2,3,16–19]. Usually, the blockcipher based AE is more suitable than the scratch based AE because of direct implementation of blockcipher rather than the encryption function [20–23]. Now-a-days, the applications of IoT-end device, RfID, and resource constrained

device are increasing exponentially [11–15]. However, these devices have certain drawbacks of limited memory, power, and processor [7,12,12,20,21]. Therefore, the blockcipher based AE is more relevant due to light operation [21,24, 36,37]. On the contrary, there are certain ISO standards of cryptographic primitive for IoT-end device or resource constrained device such as ISO/IEC29192-1, ISO/IEC29192-2, ISO/IEC29192-3, ISO/IEC29192-4 [31–33]. In addition, the ISO standard of ISO/IEC29192-2 directs the blockcipher as a core cryptographic primitive for low-resource devices. Furthermore, a certain size of blockciphers, security parameters, and resource utilizations have been emphasized according to the above standardizations. Later, the standard of ISO/IEC 29192-5 emphasized the encrypted length as 80, 128, 160, 256 bits for IoT-end device and resource constrained device [32,33]. Usually, the traditional blockcipher and lightweight-cipher satisfies the above encryption size [31–33]. Thus, an efficient and upper security bounded construction of blockcipher based authentication encryption is required.

Table 1. Comparison study of the proposed scheme and others [18–26,35–38]

Scheme name	Mode	D.O.	FME	Padding	r	PRF. Security	$\#E$ blockciphers
McOE	S	Y	N	Y	1	$O\left(2^{n/2}\right)$	$a+m+1$
OTR	P	N	Y	N	1	$O\left(2^{n/2}\right)$	$a+m+2$
COPA	P	Y	N	Y	1/2	$O\left(2^{n/2}\right)$	$a+m+2$
PoE	P	Y	N	Y	1	$O\left(2^{n/2}\right)$	$a+m+1$
OAE1,2	S	Y	N	Y	1	$O\left(2^{n/2}\right)$	–
OCB	P	Y	Y	N	1	$O\left(2^{n/2}\right)$	$a+m+2$
COBRA	S	N	N	Y	1	$O\left(2^{n/2}\right)$	$m+5$
CLOC	S	N	N	Y	1	$O\left(2^{n/2}\right)$	$a+m+1$
SILC	S	N	N	Y	1	$O\left(2^{n/2}\right)$	$a+m+1$
Proposed	P	N	Y	N	1	$O\left(2^{2n/3}\right)$	$m+3$

FME: Flexible size of message encryption per iteration, r: Efficiency-rate
P, S: Parallel or Serial operational mode, D.O.: Decryption oracle
$\#E$: total number of used blockciphers, a, m: each block of associate data and message
Y: Yes, N: No

1.1 Motivation

There are many schemes of authentication encryption (AE) such as McOE, OCB, OTR, COPE, PoE, OAE1,2, COBRA, CLOC, and SILC [18–24,34–37]. Among these, the OCB is one of the pioneer construction. It is based on blockcipher also [22]. The strong features of the OCB are parallel and efficiency ($r = 1$). The privacy security of this scheme is bounded by $O\left(2^{n/2}\right)$. However, the OCB needs decryption oracle which increases the overhead-cost of authentication encryption process [38]. Hence, the actual efficiency of the OCB has been decreased [38]. On the evaluation of OCB, Minematsu proposed a scheme of OTR [38] that overcomes the above drawback (decryption oracle) of the OCB. Furthermore,

the OTR satisfies an upper efficiency-rate ($r = 1$) including a reasonable privacy security bound $\left(\text{Priv} = O\left(2^{n/2}\right)\right)$. In addition, the OCB and OTR follows none-respecting construction. On the other hand, the McOE scheme brings a breakthrough in the domain of nonce reusing AE [21]. Thereafter, a bunch of schemes have been proposed based on the properties of the McOE such as COPA, PoE, APE, and ELmE [20,35]. However, Hoang et al. showed that the concept of nonce reusing is no more secure for any online authentication scheme [35]. In addition, Hoang et al. claimed that the online characteristic is a parameter of efficiency [35]. Therefore, a window is re-opened for off-line and nonce respecting AE. Furthermore, the McOE needs decryption oracle and it's privacy security is bounded by $O\left(2^{n/2}\right)$. Most recently, there are two more proposals such as CLOC and SILK [36,37]. The constructions of CLOC and SILK are good for short message. Additionally, these two schemes are free of decryption oracle. However, the operation mode of CLOC and SILK is serial.

According to Table 1 and the above discussions, the most of the authentication scheme's privacy security are bounded by $O\left(2^{n/2}\right)$. Furthermore, many schemes need decryption oracle. Additionally, a padding mechanism is necessary for symmetric encryption module of AE when message and blocklength is not equal. However, the padding technology itself has certain dis-advantages [2,3]. Usually, there is a common attack that is called length extension attack [2,3,26,27]. Therefore, we outline our motivations in the following way:

- higher efficiency and upper security bound
- competitive mode
- free of decryption oracle in encryption and decryption module
- allowed flexible size of message encryption
- no padding
- minimization of blockcipher calling
- efficient and low-cost primitive

1.2 Contribution

In this paper, we present a construction of authentication encryption. Our proposed scheme is based on blockcipher based compression function. Furthermore, our scheme is nonce respecting authentication encryption including associate data. The symmetric encryption module of the proposed scheme is a variant of OCB. Furthermore, the module of MAC follows a variant of PMAC plus. The achievements of the proposed scheme are listed below:

- ▶ efficiency-rate = 1
- ▶ parallel mode
- ▶ free of decryption oracle in encryption and decryption module
- ▶ allowed flexible size of message encryption (FME)
- ▶ no padding
- ▶ $\text{Priv} = O\left(2^{2n/3}\right)$
- ▶ supports less call of blockcipher calling
- ▶ blockcipher based compression function
- ▶ nonce respecting including associate data

1.3 Organization

We define preliminaries in Sect. 2. The propose scheme's definition and corresponding security notions are available in Sect. 3. We mention the security proof of the proposed construction in Sect. 4. Furthermore, the summaries are given in Sect. 5.

2 Preliminaries Including Security Notions

2.1 Fundamental Notations

Let X and Y are finite length of strings under the set of $\mathcal{X}$ and $\mathcal{Y}$. Additionally, $\mathcal{C}, \mathcal{T}$ are set of uniform distribution for the strings of ciphertext (C) and MAC (T : tag). Let N, AD, and $\mathcal{M}$ direct the space for Nonce, Associate data, and Message. Furthermore, K and n means key and block-length. In addition, there are certain operators used in the proposed authentication encryption such as $\oplus$ (XOR). Additionally, we use a defined function operator $CS(\cdot)$ in encryption and decryption module. The operation of $CS(\cdot)$ is complement including bitwise left-shift. For example, we generate α and β before encryption or decryption (Fig. 2). The value of α and β need to use in each iteration of encryption or decryption module. Furthermore, these values should be different in every iteration for tight security bound [18,19,22,38]. Thus, it can be used as counter or unique nonce and associate data. Literally, the function operator of $CS(\cdot)$ takes the value of α and returns one bit left-shift after complement when $i = 1|i$: number of iteration. If i increases then left-shift also will be increased bitwise according to the value of i. In each iteration, the output of $CS_i(\alpha)$ and $CS_i(\beta)$ are defined as p_i and q_i, where $i \leq l$ (Fig. 2). Our defined another parameter is τ, which is created as a by-product of encryption/decryption module. Generally, the τ_i is created in each iteration. Thereafter, the XOR values of all τ_i are used for tag generation (Fig. 3).

2.2 Blockcipher

A blockcipher (n, k) consists of a pair of algorithm such as $E = \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ and $E^{-1} = \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n (n, k$: block and key length). Usually, query of blockcipher is (m, k) and output is c, where key is randomly permuted. Hence, a triplet is the combine form of m, k, and c as (m, k, c). Additionally, the blockcipher oracle doesn't permit for similar query or triplet in principle. For example, if $(m_1, k_1) = c_1$ is queried to oracle then $(c_1, k_1) = m_1$ is not permitted for asking to oracle. Let $\mathsf{block}(n, k)$ is the set of all blockciphers of (n, k) according to the ICM [28,29]. Generally, adversary $\mathcal{A}$ tries to explore encrypted plaintext under a given key. However, to retrieve the information of the desire plaintext using different key set is infeasible for adversary. Moreover, to find an actual plaintext or message is infeasible for $\mathcal{A}$ if blockcipher changes [28–30]. Usually, a PRP security comes from the property of blockcipher [22–24]. Hence, the PRP-security of a blockcipher $\mathsf{block}(n, k)$ is defined as the

success probability of adversary, where $\mathcal{A}$ tries to distinguish between the output of blockcipher oracle and random permutation oracle [22–24,28–30].

2.3 Authentication Encryption

The authentication encryption is noted as AE. Generally, there are two algorithms of encryption and decryption (MAC included for both the algorithms) under the AE. Furthermore, Algorithm 1 is noted as $\mathcal{E}$-AE and $\mathcal{E}$-DE. In addition, the algorithm of $\mathcal{E}$-AE consists of nonce and associate data including message and returns ciphertext. Moreover, the message exploration and tag verification process are executed under the module of $\mathcal{D}$-AE. If verification process is valid then return message or $\perp$. In this section, we define the basic encryption and decryption module only. Later, the modified version of $\mathcal{E}$-AE and $\mathcal{D}$-AE (Algorithm 1) will be used in symmetric encryption module of the proposed construction.

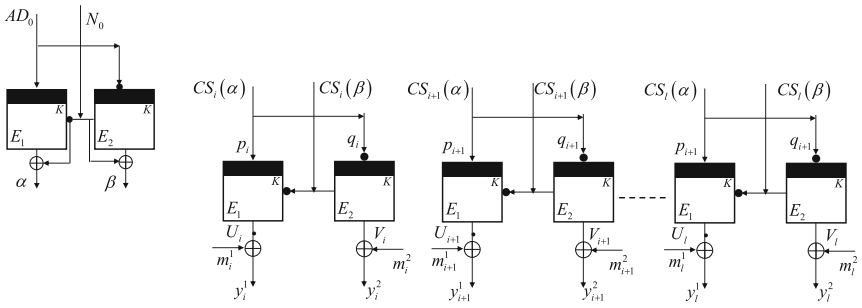

Fig. 2. Encryption procedure of AE

2.4 PRF Security

Let $F_K : K \times X \rightarrow Y$ be a pseudo-random function (keyed), where $K \rightarrow^{\$} \{0,1\}^k$ is a secret key space. On the contrary, a random function is defined as F_R, which is chosen randomly and uniquely from all functions of $X \rightarrow Y$ according to the similar domain-range of F_K. The PRF security is defined as the success probability of distinguishing between F_K and F_R. For example, there is a distinguish-er Dt that can can interplay with both the oracle of F_K and F_R. Hence, the advantage of PRF security of F_K over F_R is defined as follows:

$$\mathrm{Adv}_{\mathrm{PRF}}[\mathsf{Dt}] = \Pr\left[\mathsf{Dt}^{F_K} \Rightarrow 1\right] - \Pr\left[\mathsf{Dt}^{F_R} \Rightarrow 1\right] \tag{1}$$

The first probability of (1) is based on $K \rightarrow^{\$} \{0,1\}^k$ and the second probability is taken over $F_R : X \rightarrow^{\$} Y$. Thus, F_K is PRF secure iff the advantage of Dt is small. Moreover, F_K and F_R are respectively considered as real and ideal world.

Algorithm 1. Encryption Module and Decryption Module (Basic Module)

Encrypt $\mathcal{M}$
partitioning $m_i^j \in \mathcal{M}$ s. t. $\left(m_1^1, m_1^2\right), \ldots, \left(m_l^1, m_l^2\right)$, where $j \in \{1,2\}, i \leq l$
initialization: $\alpha \leftarrow E_{AD_0 \oplus K_1}\left(\overline{N_0}\right) \oplus \overline{N_0}, \beta \leftarrow E_{\overline{AD}_0 \oplus K_2}\left(N_0\right) \oplus N_0$
for $i = 1$ to l **do**

$$U_i \leftarrow E_{CS_i(\alpha) \oplus K_1}\left(\overline{CS_i}\left(\beta\right)\right), V_i \leftarrow E_{\overline{CS_i}(\alpha) \oplus K_2}\left(CS_i\left(\beta\right)\right),$$
$$y_i^1 \leftarrow U_i \oplus m_i^1,\ y_i^2 \leftarrow V_i \oplus m_i^2$$

end for
$\mathcal{C} \leftarrow \left(y_i^1 \oplus y_i^2 \oplus \ldots \oplus y_l^1 \oplus y_l^2\right) \wedge$ return $\mathcal{C}$
Decrypt $\mathcal{C}$
partitioning $y_i^j \in \mathcal{C}$ s. t. $\left(y_1^1, y_1^2\right), \ldots, \left(y_l^1, y_l^2\right)$, where $j \in \{1,2\}, i \leq l$
initialization: $\alpha \leftarrow E_{AD_0 \oplus K_1}\left(\overline{N_0}\right) \oplus \overline{N_0}, \beta \leftarrow E_{\overline{AD}_0 \oplus K_2}\left(N_0\right) \oplus N_0$
for $i = 1$ to l **do**

$$U_i \leftarrow E_{CS_i(\alpha) \oplus K_1}\left(\overline{CS_i}\left(\beta\right)\right), V_i \leftarrow E_{\overline{CS_i}(\alpha) \oplus K_2}\left(CS_i\left(\beta\right)\right),$$
$$m_i^1 \leftarrow U_i \oplus y_i^1,\ m_i^2 \leftarrow V_i \oplus y_i^2$$

end for
$\mathcal{M} \leftarrow \left(m_i^1 \oplus m_i^2 \oplus \ldots \oplus m_l^1 \oplus m_l^2\ \right) \wedge$ return $\mathcal{M}$

2.5 PRP Security

Let blockcipher $\mathsf{block}\,(n,k)$ is a pseudo-random permutation, where $E = \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. Furthermore, $\{0,1\}^k \leftarrow^{\$} K_E$ is a keyed and ideal permutation of blockcipher. On the other hand, there is a random permutation RP s. t. $RP \leftarrow^{\$} \mathrm{Pm}\,(n)$ |Pm : Permutation. Therefore, the PRP security means the winning probability of differentiating between $\mathsf{block}\,(n,k)$ and RP. We assume that dT is a distinguish-er that can interact with the oracle of $\mathsf{block}\,(n,k)$ and RP. Thus, the advantage of PRP security is defined as follows:

$$\mathrm{Adv}_{\mathrm{PRP}}\left[\mathsf{dT}\right] = \Pr\left[\mathsf{dT}^{E(\cdot)} \Rightarrow 1\right] - \Pr\left[\mathsf{dT}^{RP(\cdot)} \Rightarrow 1\right] \tag{2}$$

The first probability depends on $\{0,1\}^k \leftarrow^{\$} K_E$ and later one is based on $RP \leftarrow^{\$} \mathrm{Pm}\,(n)$.

3 Proposed Authentication Encryption Scheme

We define our proposed construction of blockcipher based authentication encryption as $\mathrm{AE}_T^{\mathrm{P}}$ (P: parallel, T : tag). The proposed $\mathrm{AE}_T^{\mathrm{P}}$ has three modules of M_1, M_2, and M_3. The informal definition of M_1, M_2, and M_3 are respectively initialization of nonce and associate data, encryption including tag generation, and decryption including verification. Formally, the proposed scheme looks

$\mathrm{AE}_T^{\mathrm{p}} = (\mathsf{M}_1|\ \text{Initialization}, \mathcal{E}\text{-}\mathrm{AE}_T^{\mathrm{p}}, \mathcal{D}\text{-}\mathrm{AE}_T^{\mathrm{p}})$. Furthermore, the key, nonce, associate data, message, ciphertext, and tag are respectively come from the spaces of $K_{\mathrm{AE}_T^{\mathrm{p}}}, N_{\mathrm{AE}_T^{\mathrm{p}}} AD_{\mathrm{AE}_T^{\mathrm{p}}}, M_{\mathrm{AE}_T^{\mathrm{p}}}, C_{\mathrm{AE}_T^{\mathrm{p}}},$ and $T_{\mathrm{AE}_T^{\mathrm{p}}}$. On the contrary, our scheme is a variant of OCB, where symmetric key encryption module follows CTR mode using unique nonce and AD. Moreover, the tag generation or MAC function follows the variation of a PMAC plus construction.

We use three Algorithms of 2, 3, and 4 for the formal definition of M_1, M_2, and M_3. Additionally, the basic of encryption and decryption module comes from the Algorithm 1. In addition, we use two key sets of K_1 and K_2 for encryption and decryption module. Thereafter, K_3 and K_4 key sets are used in tag generation and verification process. Though, the decryption oracle doesn't need in the entire procedure of the proposed AE, but it needs for verification process of re-tag generation only.

3.1 Privacy Notion of $\mathrm{AE}_T^{\mathrm{p}}$

The privacy notion is based on $\mathrm{AE}_T^{\mathrm{p}} = (\mathcal{E}\text{-}\mathrm{AE}_T^{\mathrm{p}},\ \mathcal{D}\text{-}\mathrm{AE}_T^{\mathrm{p}})$. We assume an adversary $\mathcal{A}$ is unique nonce, AD based game and it has access to the encryption oracle and decryption oracle of $\mathrm{AE}_T^{\mathrm{p}}$. On the contrary, adversary $\mathcal{A}$ is

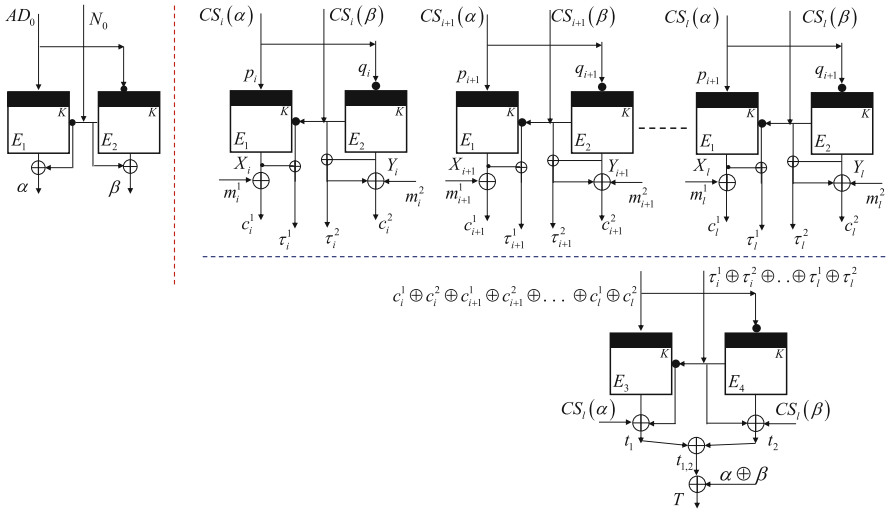

Fig. 3. Proposed construction of $\mathrm{AE}_T^{\mathrm{p}}$

Algorithm 2. Module $\mathsf{M}_1(\alpha, \beta)$ of $\mathrm{AE}_T^{\mathrm{p}}$

1: initialization of N_0 and AD_0
2: $\alpha \leftarrow E_{AD_0 \oplus K_1}\left(\overline{N}_0\right) \oplus \overline{N}_0$
3: $\beta \leftarrow E_{\overline{AD}_0 \oplus K_1}\left(N_0\right) \oplus N_0$
4: return (α, β)

Algorithm 3. Module $\mathsf{M}_2\,(C,T)$ of $\mathcal{E}$-AE$_T^{\mathrm{p}}$: Encryption and tag Generation

Input $\mathcal{M}$|set of message
Call M_1 s. t. $\mathsf{M}_1 \rightarrow (\alpha,\beta)$
$M_i^j \in \mathcal{M}$ s. t. $\left(M_1^1, M_1^2\right), \ldots, \left(M_l^1, M_l^2\right)$, where $j \in \{1,2\}, i \leq l$
for $i = 1$ to l **do**

$$\begin{cases} X_i \leftarrow E_{CS_i(\alpha)\oplus K_1}\left(\overline{CS}_i\,(\beta)\right), \\ Y_i \leftarrow E_{\overline{CS}_i(\alpha)\oplus K_2}\left(CS_i\,(\beta)\right) \end{cases}$$
$$C_i^1 \leftarrow X_i \oplus M_i^1, C_i^2 \leftarrow Y_i \oplus M_i^2,$$
$$\tau_i^1 \leftarrow X_i \oplus \overline{CS}_i\,(\beta), \tau_i^2 \leftarrow Y_i \oplus CS_i\,(\beta)$$

end for
$\mathcal{C} \leftarrow C_i^1 \oplus C_i^2 \oplus \ldots \oplus C_l^1 \oplus C_l^2$
$\gamma \leftarrow \tau_i^1 \oplus \tau_i^2 \oplus \tau_{i+1}^1 \oplus \tau_{i+1}^2 \oplus \ldots \oplus \tau_l^1 \oplus \tau_l^2$
$t_1 \leftarrow E_{C\oplus K_3}\left(\bar{\gamma}\right) \oplus \bar{\gamma} \oplus CS_l\,(\alpha)\,,\ t_2 \leftarrow E_{\overline{C}\oplus K_4}\left(\gamma\right) \oplus \gamma \oplus CS_l\,(\beta)$
$t_{1,2} \leftarrow t_1 \oplus t_2$
$T \leftarrow t_{1,2} \oplus (\alpha \oplus \beta)$
return $(\mathcal{C}, T)$

Algorithm 4. Module $\mathrm{M}_3\,(M$ or $\perp)$ of $\mathcal{D}$-AE$_T^{\mathrm{p}}$: Decryption including Verification

Call M_1 s. t. $\mathsf{M}_1 \rightarrow (\alpha,\beta)$
Call M_2 s. t. $\mathsf{M}_2 \rightarrow (\mathcal{C}, T)$
$C_i^j \in \mathcal{C}$ s. t. $\left(C_1^1, C_1^2\right), \ldots, \left(C_l^1, C_l^2\right)$, where $j \in \{1,2\}, i \leq l$
for $i = 1$ to l **do**

$$X_i \leftarrow E_{CS_i(\alpha)\oplus K_1}\left(\overline{CS}_i\,(\beta)\right) \oplus \overline{CS}_i\,(\beta),$$
$$Y_i \leftarrow E_{\overline{CS}_i(\alpha)\oplus K_2}\left(CS_i\,(\beta)\right) \oplus CS_i\,(\beta)$$
$$M_i^1 \leftarrow X_i \oplus C_i^1,\ M_i^2 \leftarrow Y_i \oplus C_i^2$$
$$\tau_i^1 \leftarrow X_i \oplus \overline{CS}_i\,(\beta),\ \tau_i^2 \leftarrow Y_i \oplus CS_i\,(\beta)$$

end for
$\mathcal{M} \leftarrow M_i^1 \oplus M_i^2 \oplus \ldots \oplus M_l^1 \oplus M_l^2$
$\gamma \leftarrow \tau_i^1 \oplus \tau_i^2 \oplus \tau_{i+1}^1 \oplus \tau_{i+1}^2 \oplus \ldots \oplus \tau_l^1 \oplus \tau_l^2$
$t'_1 \leftarrow {E^{-1}}_{\mathcal{C}\oplus K_3}\left(\bar{\gamma}\right) \oplus \bar{\gamma} \oplus CS_l\,(\alpha)\,, t'_2 \leftarrow {E^{-1}}_{\overline{\mathcal{C}}\oplus K_4}\left(\gamma\right) \oplus \gamma CS_l\,(\beta)$
$t'_{1,2} \leftarrow t'_1 \oplus t'_2$
$T' \leftarrow t'_{1,2} \oplus (\alpha \oplus \beta)$
if $T = T'$ **then**
    return $\mathcal{M}$ is valid and explore
else
    $\perp$
end if

inclusively bounded for encryption oracle ($\mathcal{E}$-AE$_T^{\mathrm{p}}$) and random-bits oracle. Thus the encryption oracle takes input as $(N, A, M) \in N_{\mathrm{AE}_T^{\mathrm{p}}} \times AD_{\mathrm{AE}_T^{\mathrm{p}}} \times M_{\mathrm{AE}_T^{\mathrm{p}}}$ and

returns $(C,T) \leftarrow \mathcal{E}\text{-AE}_T^{\mathrm{p}}(N,A,M)$. The random-bits oracle and \$ oracle inherit $(N,A,M) \in N_{\mathrm{AE}_T^{\mathrm{p}}} \times AD_{\mathrm{AE}_T^{\mathrm{p}}} \times M_{\mathrm{AE}_T^{\mathrm{p}}}$, where the output is $(C,T) \leftarrow^{\$} \{0,1\}^{|M|+T}$. Therefore, the privacy advantage is defined as follows:

$$\mathrm{Adv}_{\mathrm{AE}_T^{\mathrm{p}}}^{\mathrm{priv}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathcal{E}\text{-AE}_T^{\mathrm{p}}(.,.,.)} = 1\right] - \Pr\left[\mathcal{A}^{\$(.,.,.)} = 1\right],$$

where the first probability comes from $K \leftarrow^{\$} K_{\mathrm{AE}_T^{\mathrm{p}}}$ and second one is based on random-bits oracle including randomness of $\mathcal{A}$. Furthermore, adversary is based on unique nonce and associate data. In principle, adversary can't make duplicate query.

3.2 Authenticity Notion of $\mathrm{AE}_T^{\mathrm{p}}$

The authenticity notion is based on $\mathrm{AE}_T^{\mathrm{p}} = (\mathcal{E}\text{-AE}_T^{\mathrm{p}}, \mathcal{D}\text{-AE}_T^{\mathrm{p}})$. Let adversary $\mathcal{A}$ has access on encryption and decryption oracle of $\mathcal{E}\text{-AE}_T^{\mathrm{p}}$ and $\mathcal{D}\text{-AE}_T^{\mathrm{p}}$. The input of encryption oracle is $(N,A,M) \in N_{\mathrm{AE}_T^{\mathrm{p}}} \times AD_{\mathrm{AE}_T^{\mathrm{p}}} \times M_{\mathrm{AE}_T^{\mathrm{p}}}$. Thus the output is $(C,T) \leftarrow \mathcal{E}\text{-AE}_T^{\mathrm{p}}(N,A,M)$. Furthermore, the decryption oracle invokes $(N,A,C,T) \in N_{\mathrm{AE}_T^{\mathrm{p}}} \times AD_{\mathrm{AE}_T^{\mathrm{p}}} \times C_{\mathrm{AE}_T^{\mathrm{p}}} \times T_{\mathrm{AE}_T^{\mathrm{p}}}$. Hence, the feedback is $M \leftarrow \mathrm{AE}_T^{\mathrm{p}}(N,A,C,T)$ or $\perp$. The advantage of authenticity is defined as follows:

$$\mathrm{Adv}_{\mathrm{AE}_T^{\mathrm{p}}}^{\mathrm{auth}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathcal{E}\text{-AE}_T^{\mathrm{p}},\mathcal{D}\text{-AE}_T^{\mathrm{p}}} \text{ forges}\right],$$

where the probability is taken from $K \leftarrow^{\$} K_{\mathrm{AE}_T^{\mathrm{p}}}$ and randomness of $\mathcal{A}$. Furthermore, $\mathcal{A}$ forges if decryption oracle returns message strings for a query (N,A,C,T), when (C,T) didn't part of encryption oracle. More specifically, adversary gets success for the condition of $(N_i,A_i,C_i,T_i) \neq (N_j,A_j,C_j,T_j)$. In principle, adversary doesn't make query (N',A',C',T') to decryption oracle if $(C',T') \leftarrow (N',A',M')$ was feedback of encryption oracle. Additionally, adversary is based on unique nonce and AD.

4 Security Analysis

4.1 Privacy Security Analysis

Privacy of $\mathrm{AE}_T^{\mathrm{p}}$ is defined as the success probability of distinguish between the ciphertext and uniform distribution of string by adversary $\mathcal{A}$. Furthermore, $\mathcal{A}$ is based on unique nonce and associated data. The privacy security is formalized through a set of games. Thereafter, we take a pair of games for each segment. Gradually, we forward by taking pair of games and find the success probability of distinguish between two games. Thus we will show that the difference between two oracles are nominal. Let $\mathcal{A}$ be an adversary that makes q queries such as $(N_1,A_1,M_1)\ \ldots\ (N_l,A_l,M_l)$. Moreover, $\mathcal{A}$ is nonce-respecting and unique AD based adversary. The total length of message is σ_{2l}, where l is the number of iteration (two blocks message/iteration). In principle, we follow the proof technique of [22–24,39] according to our scheme properties.

Theorem 1. *Let* AE_T^p *be the proposed authenticated encryption including encryption algorithm* $\mathcal{E}$-$\mathrm{AE}_T^{\mathrm{p}}$*, where* $n \geq 1$*. An adversary* $\mathcal{A}$ *is allowed to access random-bits oracle and* $\mathcal{E}$-$\mathrm{AE}_T^{\mathrm{p}}$*. Furthermore, adversary* $\mathcal{A}$ *can query upto* q*. The total message length is* σ_{2l}*. Thus the advantage of* $\mathcal{A}$ *is to distinguish between* $\mathcal{E}$-$\mathrm{AE}_T^{\mathrm{p}}$ *from random oracle-bits and* \$*. Hence, the advantage is of adversary is bounded as follows:*

$$\mathrm{Adv}_{\mathrm{AE}_T^{\mathrm{p}}}^{\mathrm{priv}}(\mathcal{A}) \leq \sigma(\sigma+1) \Big/ 2^{2n}+3/2^n$$

Proof. We use certain sequential games that have different targets and goals. In addition, the final goal is to locate the advantage of adversary for privacy of the proposed AE. Our approach is very simple such as to implement a game $\mathcal{G}_{\mathcal{A}}$, which performs the proposed scheme $\mathrm{AE}_T^{\mathrm{p}}$. Moreover, our final game is $\mathcal{G}_{\mathrm{E}}$. The task of $\mathcal{G}_{\mathrm{E}}$ is to inherit random oracle. We move forward by taking pair of consecutive games. Our target is to distinguish the pair of games. The success probability of distinguishing the two consecutive games is defined as the advantage of adversary. In this way, we reach into the final game of $\mathcal{G}_{\mathrm{E}}$. Thus, we show that the adversarial advantage of distinguishing the most recent game and the last game is nominal. Moreover, we take the all probability values of success. Thereafter, we calculate the union bound of these values and get the provable privacy security bound of the proposed scheme.

Our construction is based on blockcipher compression function. Therefore, the output of each iteration including input should be unique. If current output collides with previous entry then the adversary wins. Furthermore, an event is created as $\mathcal{WIN}$ in the aspect of adversarial win. Moreover, the new and fresh value comes from the random oracle if $\mathcal{WIN}$ occurs. In addition, the collide data/value needs to eliminate from the oracle of the proposed scheme $\mathrm{AE}_T^{\mathrm{p}}$. Thereafter, the success probability of the event ($\mathcal{WIN}$) indicates the advantage of adversary for distinguishing the consecutive pair of games. Additionally, we use PRF/PRP switch method in the given security proof [34].

On the contrary, we use a variant of PMAC-plus for MAC generation [23]. Therefore, two blockciphers are used to generate a tag (T). For better security, we actually use two sets of key under two blockciphers. The generation of MAC depends on the ex-or values of all ciphertext (C_i) and XOR values of all τ_i. Actually, these two are used as input of blockcipher. Thereafter, the output (size: $2n$-bits) is produced and XOR with the most recent values of $CS(\cdot)$. Thus, the security can be achieved better than the birthday bound. Generally, the collision resistance of blockcipher is defined as to find a similar output for different two input is infeasible for adversary [1–3]. Under this section, we play with the games through pairwise. Furthermore, the success probability of the adversary is given by the event of $\mathcal{WIN}$. At first, we take the proposed scheme and game $\mathcal{G}_{\mathcal{A}}$.

GAME $\mathcal{G}_{\mathcal{A}}$. $\mathcal{G}_{\mathcal{A}}$ inherits the proposed scheme $\mathrm{AE}_T^{\mathrm{p}}$. Moreover, $\mathcal{G}_{\mathcal{A}}$ invokes N, A, M as parameter of input. Thus, the corresponding responses are C, T. On the contrary, the queries of $\mathrm{AE}_T^{\mathrm{p}}$ uses random function. Therefore,

$$\Pr\left[\mathcal{A}_{RP}^{\mathrm{AE}_T^{\mathrm{p}}}=1\right]=\Pr\left[\mathcal{A}^{\mathcal{G}_{\mathcal{A}}}=1\right] \tag{3}$$

GAME $\mathcal{G}_{\mathcal{B}}$. Let the queries of RP belongs to random function. Thus, the game $\mathcal{G}_{\mathcal{B}}$ provides random output. However, the uniqueness of output can't be confirmed due to random function. Furthermore, if any collision occurs with previous any response then an event $\mathcal{WIN}$ is called. Therefore, the advantage of adversary is to distinguish between the game $\mathcal{G}_{\mathcal{B}}$ and $\mathcal{G}_{\mathcal{A}}$. The success probability of the event $\mathcal{WIN}$ is the advantage of adversary. All queries of RP for $\mathrm{AE}_T^{\mathrm{p}}$ are stored in the database of $D_{\mathrm{AE}_T^{\mathrm{p}}}$, where RP is queried by σ times by $\mathrm{AE}_T^{\mathrm{p}}$. Therefore, the advantage of adversary is:

$$\Pr\left[\mathcal{A}^{\mathcal{G}_{\mathcal{B}}}=1\right]-\Pr\left[\mathcal{A}^{\mathcal{G}_{\mathcal{A}}}=1\right]\leq {}^{\sigma}/_{2^n} \tag{4}$$

GAME $\mathcal{G}_{\mathcal{C}}$. In this section, the proposed scheme $\mathrm{AE}_T^{\mathrm{p}}$ inherits random function. Furthermore, the database $D_{\mathrm{AE}_T^{\mathrm{p}}}$ is updated and synchronized. Therefore, the game $\mathcal{G}_{\mathcal{C}}$ and $\mathcal{G}_{\mathcal{B}}$ are in-distinguishable in the aspect of adversary. As a result, the advantage of adversary is as follows:

$$\Pr\left[\mathcal{A}^{\mathcal{G}_{\mathcal{C}}}=1\right]=\Pr\left[\mathcal{A}^{\mathcal{G}_{\mathcal{B}}}=1\right] \tag{5}$$

GAME $\mathcal{G}_{\mathcal{D}}$. We will use PRF/PRP switch theme [34] in this section. The ciphertext should be indistinguishable in respect of random oracle. According to our AE construction definition, the ciphertext is created by the ex-or values of blockcipher compression output and message. Though, adversary can control message, but it can't control the output of blockcipher output. In addition, the nonce and associate data are unique. Therefore, there are four cases for collision occurred (Figs. 4 and 5). If collision occurs then an event ($\mathcal{WIN}$) is re-called in the respect of adversary.

- Case-1. In this section, we evaluate the probability of collision under blockcipher output. For example, the pair of output is X_i and Y_i ($i \leq l$). Thus, two types of collision can be occurred such as query of double and single query.
  - SubCase-1 (query of double). The requirements of collision under this SubCase are two different queries for the iteration of i, j ($i \geq j$) and similar output for input of any two queries. For example, the output are X_i and Y_i for the iteration of i. In addition, X_j and Y_j are the output of j-th iteration. Thus, there is a chance to collide with $X_i = X_j, Y_j$ or $Y_i = X_j, Y_j$ (Fig. 4). If collision occurs then an event is called. Moreover, the random and uniform values come from the set of $\mathcal{X}$ and $\mathcal{Y}$. Thereafter, these new values are replaced by collide values. The success probability of the event $\mathcal{WIN}$ is:

$$\begin{aligned}&\Pr\left[\mathcal{WIN}\right]=\Pr\left[\mathcal{WIN}_1\vee\mathcal{WIN}_2\vee\ldots\mathcal{WIN}_\sigma\right]\\&\leq\Pr\left[\mathcal{WIN}_1\right]+\Pr\left[\mathcal{WIN}_2\right]+\ldots\Pr\left[\mathcal{WIN}_\sigma\right]\\&\leq\sigma\left(\sigma-1\right)/2^{2n}\end{aligned} \tag{6}$$

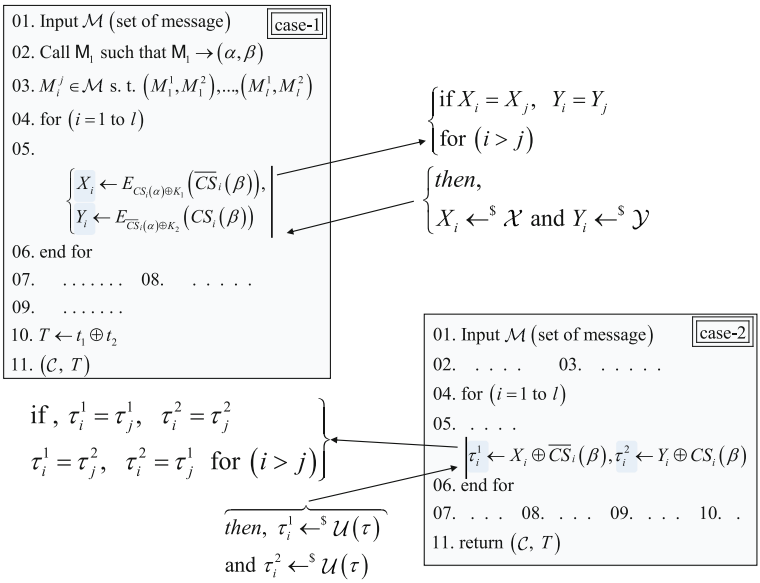

Fig. 4. Under the game $\mathcal{G}_{\mathcal{D}}$

- SubCase-2 (single query). The output of i-th iteration are X_i and Y_i. Therefore, there is a chance to make a collision between $X_i = Y_i$. Thereafter, an event $\mathcal{WIN}$ is called in the aspect of adversarial success. Moreover, the collide values are replaced by the random and uniform values (Fig. 4). For example, $X_i \leftarrow \mathcal{X}$, $Y_i \leftarrow \mathcal{Y}$. The success probability of $\mathcal{WIN}$ under this SubCase is:

$$\begin{aligned} &\Pr[\mathcal{WIN}] = \Pr[\mathcal{WIN}_1 \vee \mathcal{WIN}_2 \vee ... \mathcal{WIN}_\sigma] \\ &\leq \Pr[\mathcal{WIN}_1] + \Pr[\mathcal{WIN}_2] + ... \Pr[\mathcal{WIN}_\sigma] \\ &\leq \sigma \cdot (1/2^n) \end{aligned} \tag{7}$$

▶ Case-2. According to our construction definition, the nonce is unique for each iteration. Thus, the ex-or values blockcipher output and nonce is random. However, there is a chance to occur collision such as $\tau_i^1 = \tau_j^1, \tau_j^2$ and $\tau_i^2 = \tau_j^1, \tau_j^2$. The event $\mathcal{WIN}$ is defined if collision occurs. Thereafter, the collide values are replaced by random and uniform distribution of $\mathcal{U}(\tau)$ (Fig. 4). So, the success probability of the event $\mathcal{WIN}$ is:

$$\begin{aligned} &\Pr[\mathcal{WIN}] = \Pr[\mathcal{WIN}_1 \vee \mathcal{WIN}_2 \vee ... \mathcal{WIN}_\sigma] \\ &\leq \Pr[\mathcal{WIN}_1] + \Pr[\mathcal{WIN}_2] + ... \Pr[\mathcal{WIN}_\sigma] \\ &\leq 2\sigma/2^{2n} \end{aligned} \tag{8}$$

▶ Case-3. This section is responsible for evaluation of tag collision. Generally, two different blockciphers including two unique key sets are used to generate tag. For example, the random value of ciphertext $(\mathcal{C})$ and most recent $CS(\cdot)$

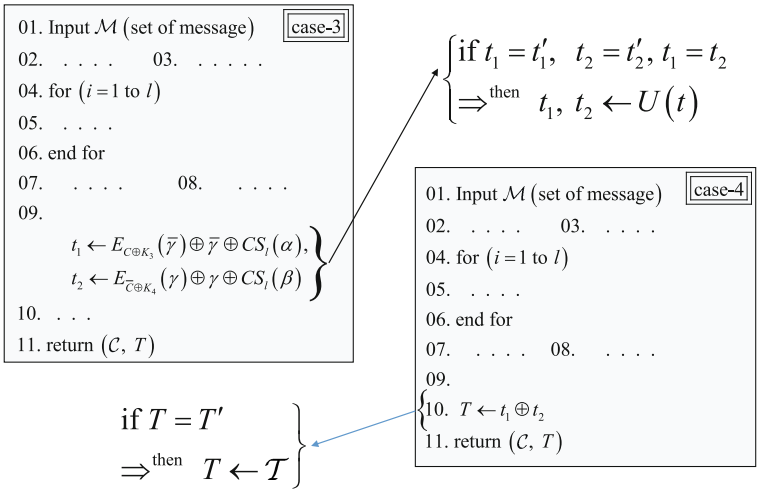

Fig. 5. Under the game $\mathcal{G}_{\mathcal{D}}$

value are used to generate tag. Therefore, there is a chance to collide between t_1 and t_2 (Fig. 5). If collision occurs then an event is defined as $\mathcal{WIN}$. The advantage of adversary is to find the probability of the event $\mathcal{WIN}$. Therefore, the advantage is:

$$\Pr[\mathcal{WIN}] = 2/2^n \tag{9}$$

- Case-4. The final tag is produced by the ex-or values of t_1, t_2 and $(\alpha \oplus \beta)$. If t_1 and t_2 are random then the ex-or output of T is also random. However, there is a chance to make collision such as $T = T'$. Hence, the probability of the event $\mathcal{WIN}$ is:

$$\Pr[\mathcal{WIN}] = 1/2^n \tag{10}$$

Adding the value of 6, 7, 8. 9 and 10, we get the advantage of distinguishing the game of $\mathcal{G}_{\mathcal{C}}$ and $\mathcal{G}_{\mathcal{D}}$.

GAME $\mathcal{G}_{\mathrm{E}}$. The $\mathcal{G}_{\mathrm{E}}$ simulates the random oracle model. The database $D_{\mathrm{AE}_T^{\mathrm{p}}}$ is updated and synchronized after the operation of game $\mathcal{G}_{\mathcal{D}}$. Therefore, the current all entries are random and uniformly distributed. Hence, the game of $\mathcal{G}_{\mathcal{D}}$ and $\mathcal{G}_{\mathrm{E}}$ are identical in the aspect of adversary. So, the advantage of the adversary to distinguish the game of $\mathcal{G}_{\mathrm{E}}$ and $\mathcal{G}_{\mathcal{D}}$ is:

$$\Pr\left[\mathcal{A}^{\mathcal{G}_{\mathrm{E}}} = 1\right] = \Pr\left[\mathcal{A}^{\mathcal{G}_{\mathcal{D}}} = 1\right] \tag{11}$$

Therefore, taking the union bound of 4, 6, 7, 8, 9, and 10, Theorem 1 satisfies.

4.2 Authenticity Security Analysis

The authenticity of $\mathrm{AE}_T^{\mathrm{p}}$ scheme is based on both oracle of encryption and decryption. The authenticity is said to be broken when adversary can inject

under the condition of N', A', C', T' $(N', A', C', T') \neq (N, A, C, T)$. For example, encryption queries are $(N_1, A_1, M_1), \ldots, (N_q, A_q, M_q)$. Moreover, list of decryption queries are $(N'_1, A'_1, C'_1, T'_1) \ldots (N'_q, A'_q, C'_q, T'_q)$. The total length of message for encryption and decryption are respectively σ^{2l} and $\sigma^{2l'}$. Let there is an experiment $\mathcal{EXP}^{\mathrm{p}}_{\mathrm{auth}}$, which outputs 1 iff the adversary successfully forges N', A', C', T' for $M'|M \neq M'$. Therefore,

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{AE}^{\mathrm{p}}_{T}}(\mathcal{A}) = \Pr\left[\mathcal{EXP}^{\mathrm{p}}_{\mathrm{auth}}(\mathcal{A}) = 1\right] \tag{12}$$

Theorem 2. *Let* AE^{sim}_{T} *be the proposed authenticated encryption, where* $\mathcal{E}$-$\mathrm{AE}^{\mathrm{sim}}_{T}$ *and* $\mathcal{D}$-$\mathrm{AE}^{\mathrm{sim}}_{T}$ *be the encryption and decryption algorithm. Furthermore, adversary* $\mathcal{A}$ *is allowed to access both the oracles. Thus the advantage of* $\mathcal{A}$ *is success probability of injecting false data instead of valid data through the defined experiment* $\mathcal{EXP}$*. Therefore, the advantage of adversary is bounded as follows:*

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{AE}^{\mathrm{p}}_{T}}(\mathcal{A}) \leq \sigma(\sigma+1)\Big/2^{2n}{+}5/2^{n} + \sigma^{2}/2^{n+1}$$

5 Conclusion

In this paper, we have studied the familiar constructions of authentication encryption (AE). Moreover, the applications of AE have been evaluated. Recently, the AE has been considered as an important cryptographic tool/primitive for the security solution of IoT-end device, RfID, and resource constrained device. Thus, the AE should satisfies the properties of efficiency and better security. Though there are many constructions such as OCB, OTR, CLOC, SILK, APE, McOE, PoE, COPA, and COBRA but most of the scheme's privacy security are bounded by $O\left(2^{n/2}\right)$. Moreover, decryption oracle is necessary for all constructions except the OCB, OTR, CLOC, and SILK. Therefore, we have presented a blockcipher based AE that satisfies upper privacy security bound $\left(\mathrm{Priv} = O\left(2^{n/2}\right)\right)$. Our proposed scheme operates without decryption oracle in the module of encryption and decryption. Furthermore, the efficiency-rate is 1 and the operation mode is parallel. Moreover, the proposed construction can support flexible message encryption without padding. Our proposed scheme is a variant of OCB. More specifically, the symmetric encryption module follows the CTR mode and the MAC module follows the PMAC Plus construction. However, the proposed scheme can't support small domain encryption including format preserving encryption. Furthermore, decryption module is not online. Therefore, our target is to overcoming these limitations in future.

References

1. Rogaway, P.: Evaluation of Some Blockcipher Modes of Operation (2011). http://web.cs.ucdavis.edu/rogaway/papers/modes.pdf
2. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography, 5th edn. CRC Press, Boca Raton (2001)

3. Stallings, W.: Data & Computer Communications, 10th edn. Pearson, Boston (2013)
4. Hanaoka, G., Zheng, Y., Imai, H.: LITESET: a light-weight secure electronic transaction protocol. In: Boyd, C., Dawson, E. (eds.) ACISP 1998. LNCS, vol. 1438, pp. 215–226. Springer, Heidelberg (1998)
5. Kim, H., Kim, T.: Design on mobile secure electronic transaction protocol with component based development. In: Laganá, A., Gavrilova, M.L., Kumar, V., Mun, Y., Tan, C.J.K., Gervasi, O. (eds.) ICCSA 2004. LNCS, vol. 3043, pp. 461–470. Springer, Heidelberg (2004)
6. Cao, L.-C.: Improving security of SET protocol based on ECC. In: Gong, Z., Luo, X., Chen, J., Lei, J., Wang, F.L. (eds.) WISM 2011, Part I. LNCS, vol. 6987, pp. 234–241. Springer, Heidelberg (2011)
7. Lorenz, M.: Authentication and transaction security in e-business. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds.) The Future of Identity in the Information Society, vol. 262, pp. 175–197. Springer, Heidelberg (2008)
8. Bailey, D.V., Brainard, J., Rohde, S., Paar, C.: Wireless authentication and transaction-confirmation token. In: Obaidat, M.S., Filipe, J. (eds.) ICETE 2009. CCIS, vol. 130, pp. 186–198. Springer, Heidelberg (2011)
9. Subpratatsavee, P., Kuacharoen, P.: Transaction authentication using HMAC-based one-time password and QR code. In: Park, J.J.J.H., Stojmenovic, I., Jeong, H.Y., Yi, G. (eds.) Computer Science and Its Applications. LNEE, vol. 330, pp. 93–98. Springer, Heidelberg (2015)
10. Zhang, L., Wu, W., Wang, P.: Extended models for message authentication. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 286–301. Springer, Heidelberg (2009)
11. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010). Elsevier
12. Zhou, Z., Tsang, K.F., Zhao, Z., Gaalou, W.: Data intelligence on the Internet of Things. Pers. Ubiquit. Comput. **20**, 277–281 (2016). doi:10.1007/s00779-016-0912-1. Springer
13. Coppola, P., Mea, V.D., Gaspero, L.D., Lomuscio, R., Mischis, D., Mizzaro, S., Nazzi, E., Scagnetto, I., Vassena, L.: AI techniques in a context-aware ubiquitous environment. In: Hassanien, A.E., Abawajy, J.H., Abraham, A., Hagras, H. (eds.) Pervasive Computing. Computer Communications and Networks. Springer, Heidelberg (2009)
14. Zhao, K., Ge, L.: A survey on the internet of things security. In: 9th CIS, pp. 663–667. IEEE (2013). ISBN 978-1-4799-2548-3
15. Mennink, B.: Embedded security for internet of things. In: 2nd NCETACS, pp. 1–6. IEEE (2011). ISBN 978-1-4244-9578-8
16. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. IEEE Internet Things J. **1**(1), 22–32 (2014)
17. Özen, O., Stam, M.: Another glance at double-length hashing. In: Parker, M.G. (ed.) Cryptography and Coding 2009. LNCS, vol. 5921, pp. 176–201. Springer, Heidelberg (2009)
18. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013)

19. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., Yasuda, K.: APE: authenticated permutation-based encryption for lightweight cryptography. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 168–186. Springer, Heidelberg (2015)
20. Abed, F., Fluhrer, S., Forler, C., List, E., Lucks, S., McGrew, D., Wenzel, J.: Pipelineable on-line encryption. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 205–223. Springer, Heidelberg (2015)
21. Fleischmann, E., Forler, C., Lucks, S.: McOE: a family of almost foolproof on-line authenticated encryption schemes. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 196–215. Springer, Heidelberg (2012)
22. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004)
23. Yasuda, K.: A new variant of PMAC: beyond the birthday bound. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 596–609. Springer, Heidelberg (2011)
24. Naito, Y.: Full PRF-secure message authentication code based on tweakable block cipher. In: Chakraborty, S. (ed.) ProvSec 2015. LNCS, vol. 9451, pp. 167–182. Springer, Heidelberg (2015). doi:10.1007/978-3-319-26059-4_9
25. Yau, A.K.L., Paterson, K.G., Mitchell, C.J.: Padding Oracle attacks on CBC-mode encryption with secret and random IVs. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 299–319. Springer, Heidelberg (2005)
26. Lee, T., Kim, J.-S., Lee, C.-H., Sung, J., Lee, S.-J., Hong, D.: Padding oracle attacks on multiple modes of operation. In: Park, C., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 343–351. Springer, Heidelberg (2005)
27. Paterson, K.G., Yau, A.K.L.: Padding oracle attacks on the ISO CBC mode encryption standard. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 305–323. Springer, Heidelberg (2004)
28. Black, J.A., Rogaway, P., Shrimpton, T.: Black-box analysis of the block-cipher-based hash-function constructions from PGV. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 320–335. Springer, Heidelberg (2002)
29. Black, J.A., Rogaway, P., Shrimpton, T., Stam, M.: An analysis of the blockcipher-based hash functions from PGV. J. Cryptol. **23**, 519–545 (2010)
30. Miyaji, A., Mazumder, R.: A new (n, 2n) double block length hash function based on single key scheduling. In: AINA, pp. 564–570. IEEE (2015)
31. Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., Yoshida, H.: A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-LW. In: Rhee, K.-H., Nyang, D.H. (eds.) ICISC 2010. LNCS, vol. 6829, pp. 151–168. Springer, Heidelberg (2011)
32. Shirai, Taizo, Shibutani, Kyoji, Akishita, Toru, Moriai, Shiho, Iwata, Tetsu: The 128-bit blockcipher CLEFIA (Extended Abstract). In: Biryukov, Alex (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). IACR archive, https://www.iacr.org/archive/fse2007/45930182/45930182.pdf
33. Yoshida, H.: On the standardization of cryptographic application techniques for IoT devices in ITU techniques for IoT devices in ITU-T and ISO/IEC JTC 1 T and ISO/IEC JTC1 (2015). https://www.ietf.org/proceedings/94/slides/slides-94-saag-2.pdf,
34. Bellare, M., Rogaway, P.: The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006)

35. Hoang, V.T., Reyhanitabar, R., Rogaway, P., Damian, V.: Online authenticated-encryption and its nonce-reuse misuse-resistance. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015. LNCS, vol. 9215, pp. 493–517. Springer, Heidelberg (2015)
36. Iwata, T., Minematsu, K., Guo, J., Morioka, S.: CLOC: authenticated encryption for short input. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 149–167. Springer, Heidelberg (2015)
37. Iwata, T., Minematsu, K., Guo, J., Morioka, S., Kobayashi, E.: SILC: SImple Lightweight CFB. DIAC Competitions. https://competitions.cr.yp.to/round2/silcv2.pdf
38. Minematsu, K.: Parallelizable rate-1 authenticated encryption from pseudorandom functions. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 275–292. Springer, Heidelberg (2014)
39. Chang, D., R., S.M., Sanadhya, S.K.: PPAE: practical parazoa authenticated encryption family. In: Au, M.-H., Miyaji, A. (eds.) ProvSec 2015. LNCS, vol. 9451, pp. 198–211. Springer, Heidelberg (2015). doi:10.1007/978-3-319-26059-4_11