ITC 4/48
Information Technology and Control
Vol. 48 / No. 4 / 2019
pp. 579-589
DOI 10.5755/j01.itc.48.4.23454

A Novel CCA-Secure Verifiable Authenticated Encryption Scheme Using BSDH and *q*-SDH Assumptions

Received 2019/05/29 | Accepted after revision 2019/09/30

http://dx.doi.org/10.5755/j01.itc.48.4.23454

A Novel CCA-Secure Verifiable Authenticated Encryption Scheme Using BSDH and *q*-SDH Assumptions

Han-Yu Lin

Department of Computer Science and Engineering, National Taiwan Ocean University; 2, Beining Road, Keelung, 202, Taiwan; phone: +886-2-2462-2192 ext 6656; fax: +886-2-2462-3249; e-mail: lin.hanyu@msa.hinet.net

Corresponding author: lin.hanyu@msa.hinet.net

When it comes to secure transactions online, the requirements of confidentiality and authenticity are usually concerned the most. The former prevents unauthorized reading, while the latter ensures authorized access. Hybrid cryptographic mechanisms such as authenticated encryption (AE) schemes, simultaneously combine the functions of public key encryption and digital signature. Some AE schemes also provide a cost-free arbitration mechanism to deal with the signer's later repudiation. Such schemes have been found to have numerous practical applications like on-line credit card transactions, confidential contract signing and the protection of digital evidence, etc. However, a designated verifier should also have the ability to convince any third party that he/she is indeed the intended recipient. In this paper, the author presents a novel verifiable authenticated encryption (VAE) scheme with the functionality of recipient proof. Furthermore, the paper shows that the proposed VAE scheme is non-delegatable and provably secure under the random oracle proof models. A non-delegatable hybrid cryptographic scheme provides a higher security level even if the shared common key is compromised. Specifically, the author of the paper will demonstrate that the designed construction is proved secure against adaptive chosen-ciphertext attacks (CCA2) assuming the hardness of Bilinear Square Diffie-Hellman Problem (BSDHP) and secure against adaptive chosen-message attacks (CMA) assuming the hardness of *q*-Strong Diffie-Hellman Problems (*q*-SDHP).

KEYWORDS: verifiable authenticated encryption, non-delegatable, bilinear square Diffie-Hellman problem, *q*-strong Diffie-Hellman problem, public key system.

1. Introduction

A digital signature [5, 18] is an important mechanism of public key cryptosystems [4] and serves the same functionality as the hand-written signature. In a digital signature scheme, a signer owning a private key can create a signature for his/her chosen message such that any person can authenticate the signature with the signer's public key. Moreover, a signer cannot deny previous signing behavior, which is referred to as the property of no-repudiation [19]. However, for some e-commerce transactions, it is necessary that a digital signature should further satisfy the security requirement of confidentiality. At the same time, the signature can only be verified by a privileged person rather than anyone. Traditionally, the two-step method could achieve this purpose, i.e., first create a signature and then encrypt it with the symmetric manner. In such a way, a designated recipient who possesses the correct decryption key can verify the encrypted signature. It is evident that this method will result in complex processes and higher computational efforts. Therefore, it might be unsuitable for the application scenario which is involved with a large number of online transactions.

To provide a better solution, in 1994, Horster et al. [6] integrated the mechanisms of conventional digital signatures and public key encryptions [4] to introduce a hybrid system called authenticated encryption (AE). It simultaneously satisfies the security properties of authenticity [21] along with confidentiality [7, 10]. In such a scheme, a signer utilizes two keys, i.e., his/her private key and the verifier's public key, for creating an authenticated ciphertext and only the intended person owning the correct private key can decrypt it to verify the original signature. Nevertheless, whenever a designated verifier comes across the circumstance that an untruthful signer denies his/her signing behavior, the designated verifier is unable to persuade anyone of the fact.

In general, a secure AE system should satisfy the following properties:

1. *Confidentiality:* Only a designated verifier owning the correct private key has the privilege to decrypt the resulted ciphertext and validate the signature.
2. *Integrity:* A designated verifier can ensure the integrity of decrypted message if its corresponding signature is valid.
3. *Unforgeability:* Except for the original signer, it is computationally infeasible for any attacker to forge a valid signature.
4. *Undeniability:* When an original signer denies his/her signing behavior, the designated recipient is capable of non-interactively converting the authenticated ciphertext into a publicly verifiable signature.
5. *Non-delegatability:* Even if the shared common key between a signer and the designated recipient is compromised, any attacker cannot decrypt information in the transmitted ciphertext.

1.1. Related Works

For preventing the dispute over repudiation, in 1999, Araki et al. [1] proposed a new signature system named Convertible Limited Verifier Signature. Their scheme supports the functionality of a later arbitration to settle repudiation disputes. Yet, this approach must be interactively carried out by the original signer and the designated verifier. In case that a dishonest signer refuses to cooperate, the situation of disputes remains unsolved. Moreover, Zhang and Kim [30] demonstrated that Araki et al.'s system is subjected to the notorious universal forgery attacks on arbitrary chosen messages.

In 2002, Wu and Hsu [26] put forward a convertible AE protocol which permits a designated verifier to non-interactively output a transformed signature that could be publicly verified when encountered with a repudiation dispute. A crucial characteristic of their protocol is that the signature conversion mechanism is cost-free, as the designated verifier needs to convert the signature before verifying it during the normal decryption procedures. In the next year, Huang and Chang [9] presented a more efficient variant. Unfortunately, Lv et al. [17] disclosed that these schemes [9, 26] fail to fulfill the essential security property of confidentiality. In 2009, Lee et al. [11] further introduced the ElGamal-based AE scheme with convertible property. Utilizing the famous RSA assumption, Wu and Lin [27] together with Arshad and Ikram [16] separately built new convertible AE schemes with provable security in the random oracle models. Thinking of the benefits of message link-

age in practical applications, Yoon and Yoo proposed two improved variants [28, 29] to fulfill the property of forward secrecy and support message linkages for message flows.

In 2011, Hsu and Lin [8] adopted key-insulated systems to propose an AE scheme suitable for multi-signer environments. In the next year, Lu et al. [16] presented another variant supporting multi-verifier. In 2014, Lin [13] introduced a convertible AE scheme which enables a signer to select flexible signing policies. Considering the multi-signer applications, in 2016, Tahat [23] proposed a convertible multi-AE scheme based on elliptic curve discrete logarithm problem (ECDLP). In 2017, the functionality of proxy delegation is realized in a group-oriented AE scheme [14]. Tsai et al. [24] further presented a publicly verifiable AE scheme based on factoring and discrete logarithms. Even if one of the two cryptographic problems is broken, their scheme could still maintain essential security. Similarly, in 2018, Tahat and Abdallah [22] introduced a hybrid AE variant using chaotic maps and factoring problems. Recently, Lin [15] proposed a novel dual AE scheme suitable for social networking services such as Skype, Line and Facebook Messenger.

However, existing AE schemes and their variants with different functionalities primarily rely on the standard cryptographic assumptions such as the Discrete Logarithm (DL) or the Computational Diffie-Hellman (CDH). In addition, these schemes lack of either interactive or non-interactive recipient proof mechanism to protect the designated verifier's benefits. This motivates us to think the possibility of constructing an ideal AE scheme providing the functionality of recipient proof and with provable security.

1.2. Contributions

In this paper, the author will come up with a novel verifiable AE (a.k.a. VAE) scheme utilizing the Bilinear Square Diffie-Hellman (BSDH) and the q-Strong Diffie-Hellman (q-SDH) assumptions. The contributions of the proposed work are listed below:

1. This scheme supports the functionality of recipient-proof.
2. The requirement of non-delegatability is fulfilled in the proposed scheme.
3. The proposed scheme is proved secure against adaptive chosen-ciphertext attacks (CCA2) under the hardness of Bilinear Square Diffie-Hellman Problem (BSDHP).
4. The proposed scheme is secure against adaptive chosen-message attacks (CMA) under the hardness of q-Strong Diffie-Hellman Problems (q-SDHP).
5. Compared with related systems, the proposed scheme is a better alternative owing to a higher security level and better functionalities.

The rest of this paper is organized as follows. In the preliminary section, the author reviews some cryptographic assumptions and the mathematical backgrounds. The composition of the proposed VAE system is introduced in Section 3. A concrete construction is presented in Section 4. The security proofs and comparisons are detailed in Section 5. Finally, a concluding remark is given in Section 6.

2. Preliminaries

For facilitating the introduction of the proposed scheme, the author first states some preliminaries and the underlying cryptographic assumptions.

Bilinear Pairing

Let q be a large prime and $(\boldsymbol{G}_1, \boldsymbol{G}_2)$ denote two multiplicative groups of order q. There is a bilinear map e such that e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$. Some properties of bilinear map are stated as follows:

1. ***Bilinearity***:

$e(p_1p_2, q) = e(p_1, q)e(p_2, q)$;

$e(p, q_1q_2) = e(p, q_1)e(p, q_2)$;

2. ***Non-degeneracy:***

If g is a generator of $\boldsymbol{G}_1$, then $e(g, g)$ is a generator of $\boldsymbol{G}_2$.

3. ***Computability***:

Given $p, q \in \boldsymbol{G}_1$, there is a polynomial-time algorithm that can efficiently compute the value $e(p, q)$.

q-Strong Diffie-Hellman Problem; q-SDHP

Given an instance $(g, g^x, g^{x^2}, ..., g^{x^q}) \in \boldsymbol{G}_1^{q+1}$ where $x \in Z_q^*$, output $(c, g^{1/(x+c)})$ for some $c \in Z_q$.

q-Strong Diffie-Hellman (q-SDH) Assumption

For all probabilistic polynomial-time algorithm $\mathcal{A}$, the advantage for $\mathcal{A}$ to solve the q-SDHP is negligible.

Bilinear Diffie-Hellman Problem; BDHP

Given an instance $(g, g^a, g^b, g^c) \in \boldsymbol{G}_1^4$ for some $a, b \in Z_q^*$, compute $e(g, g)^{abc} \in \boldsymbol{G}_2$.

Bilinear Diffie-Hellman (BDH) Assumption

For all probabilistic polynomial-time algorithm $\mathcal{A}$, the advantage for $\mathcal{A}$ to solve the BDHP is negligible.

Bilinear Square Diffie-Hellman Problem; BSDHP

Given an instance $(g, g^a, g^b) \in \boldsymbol{G}_1^3$ for some $a, b \in Z_q^*$, compute $e(g, g)^{a^2 b} \in \boldsymbol{G}_2$.

Bilinear Square Diffie-Hellman (BSDH) Assumption

For all probabilistic polynomial-time algorithm $\mathcal{A}$, the advantage for $\mathcal{A}$ to solve the BSDHP is negligible.

According to the research of Zhang et al. [31], the BSDH assumption is as hard as that of BDH, i.e., they are polynomial-time equivalent. This paper shows that BDHP could be reduced to BSDHP. That is, BDHP can be solved by using the capability of breaking BSDHP. Let three BSDHP instances be (g, g^a, g^c), (g, g^c, g^b) and (g, g^{a+b}, g^c), respectively. By breaking these BSDHP instances, $e(g, g)^{a^2 c}$, $e(g, g)^{b^2 c}$ and $e(g, g)^{(a+b)^2 c}$ could be obtained. Then an BDHP instance (g, g^a, g^b, g^c) could be solved by computing

$$\begin{aligned}(e(g,g)^{(a+b)^2 c} / e(g,g)^{a^2 c} \cdot e(g,g)^{b^2 c})^{1/2} \\ = (e(g,g)^{(a^2 c + 2abc + b^2 c) - (a^2 c + b^2 c)})^{1/2} \\ = (e(g,g)^{2abc})^{1/2} \\ = e(g,g)^{abc}.\end{aligned}$$

3. Composition of VAE Scheme

Seeing that most existing AE schemes and related variants are based on the assumption of either RSA or (elliptic curve) discrete logarithm, it is unknown whether a secure AE variant could be constructed using different computational assumptions. Motivated by the reason, the author of the present paper employed the BSDH and the q-SDH assumptions to propose a novel VAE scheme in this paper. There are three main participated parties in a VAE scheme including a system authority, a signer and a designated verifier. The system authority is responsible for initializing the system and setting public parameters. A signer can produce an authenticated ciphertext for an intended receiver. When receiving a ciphertext, a designated verifier could decrypt and verify it with his/her private key. If necessary, the receiver also has the ability to convince anyone that he/she is the designated verifier without compromising his/her private key. Specifically, a VAE scheme is constituted by eight general algorithms defined as follows:

- **Setup**(1^k)**:** Given a security parameter k, this algorithm outputs public parameters.
- **Keygen**(i)**:** Given an index i, this algorithm outputs the corresponding private-and-public key pair.
- **SEnc**(m, x_s, y_v)**:** Given a message m, the public key y_v of the designated recipient and the private key x_s of signer, the algorithm will output a ciphertext δ.
- **SDec**(δ, x_v, y_s)**:** Given a ciphertext δ, the private key x_v of designated recipient and the public key y_s of signer, the algorithm will output a decrypted message m together with its signature Ω.
- **SVerify**(m, Ω, y_s)**:** Given a message m, a signature Ω, and the public key y_s of signer, the algorithm will return **True** if the signature is valid. Otherwise, an error symbol $\perp$ is returned instead.
- **Eval1**(δ, u)**:** Given a ciphertext δ and a random number u, the algorithm will output a recipient proof challenge D.
- **Eval2**(D, x_v)**:** Given a recipient proof challenge D and the private key x_v of designated recipient, the algorithm will output a recipient proof Λ.
- **Judge**$(\delta, \Omega, u, \Lambda)$**:** Given a ciphertext δ, a signature Ω, a random number u and a recipient proof Λ, the algorithm will return **True** if the recipient proof is correct. Otherwise, an error symbol $\perp$ is returned instead.

4. Construction of the Proposed Scheme

According to the composition of VAE scheme, the author of this paper presents a concrete construction using bilinear pairings. Some utilized notations are defined as Table 1.

- **Setup**(1^k)**:** On inputting a security parameter k, the Setup algorithm selects two groups $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ of the same prime order q. Let g be a generator of order q over $\boldsymbol{G}_1$, $e: \boldsymbol{G}_1 \times \boldsymbol{G}_1 \to \boldsymbol{G}_2$ a bilinear pairing and $h_1: \{0,1\}^k \times \boldsymbol{G}_1 \to Z_q$, $h_2: \boldsymbol{G}_1^2 \times \boldsymbol{G}_2 \to \{0,1\}^k$ and $h_3: \boldsymbol{G}_1 \to \boldsymbol{G}_1$ collision resistant hash functions. The algorithm outputs

public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, g, e, \mu = e(g, g), h_1, h_2, h_3\}$.

Keygen(i)**:** On inputting an index i, the Keygen algorithm chooses a private key $x_i \in Z_q$ and computes the corresponding public key $y_i = g^{x_i}$.

Table 1
Used symbol notations

k	a security parameter
q	a large prime
$\boldsymbol{G}_1, \boldsymbol{G}_2$	two multiplicative group of order q
g	a generator of $\boldsymbol{G}_1$
μ	a generator of $\boldsymbol{G}_2$ such that $\mu = e(g, g)$
Z_q^*	multiplicative group of integers modulo q
$x \in Z_q^*$	element x in set Z_q^*
$x \leftarrow Z_q^*$	sampling element x uniformly in set Z_q^*
e	a bilinear pairing satisfying that $e: \boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$
$\oplus$	logical operation XOR
x_i	the private key of U_i
y_i	the public key of U_i
δ	a ciphertext
Ω	a transformed signature
$\|x\|$	the bit-length of x
$\Pr[E]$	probability of event E occurring

– **SEnc**(m, x_s, y_v)**:** On inputting a message m, the public key y_v of the designated recipient and the private key x_s of signer, the algorithm chooses $t \in Z_q^*$ to compute

$$T = y_v^{\,t}, \tag{1}$$

$$R = g^t, \tag{2}$$

$$z = e(y_v^{\,x_s}, h_3(R)), \tag{3}$$

$$\sigma = g^{1/(x_s + h_1(m, R))}, \tag{4}$$

$$r = m \oplus h_2(R, \sigma, z), \tag{5}$$

and then outputs the authenticated ciphertext $\delta = (T, \sigma, r)$.

– **SDec**(δ, y_s, x_v)**:** On inputting an authenticated ciphertext $\delta = (T, \sigma, r)$, the private key x_v of designated recipient and the public key y_s of signer, the algorithm computes

$$R = T^{x_v^{-1}}, \tag{6}$$

$$z = e(y_s^{\,x_v}, h_3(R)), \tag{7}$$

and recovers the message m as

$$m = r \oplus h_2(R, \sigma, z). \tag{8}$$

The transformed signature for m is $\Omega = (R, \sigma)$.

Theorem 1. *A* designated *verifier can correctly recover the original message with Eq. (8).*

Proof: From the right-hand side of Eq. (8), it can be derived that

$$\begin{aligned}
&r \oplus h_2(R, \sigma, z) \\
&= r \oplus h_2(R, \sigma, e(y_s^{\,x_v}, h_3(R))) && \text{(by Eq. (7))} \\
&= r \oplus h_2(R, \sigma, e(y_s^{\,x_v}, h_3(T^{x_v^{-1}}))) && \text{(by Eq. (6))} \\
&= r \oplus h_2(R, \sigma, e(y_s^{\,x_v}, h_3(y_v^{\,tx_v^{-1}}))) && \text{(by Eq. (1))} \\
&= r \oplus h_2(R, \sigma, e(y_v^{\,x_s}, h_3(g^t))) && \text{(by Eq. (3))} \\
&= r \oplus h_2(R, \sigma, z) \\
&= m && \text{(by Eq. (5))}
\end{aligned}$$

which leads to the left-hand side of Eq. (8).

– **SVerify**(m, Ω, y_s)**:** On inputting a message m, a signature $\Omega = (R, \sigma)$, and the public key y_s of signer, the algorithm verifies the signature by checking if

$$e(\sigma, g^{h1(m, R)} y_s) = \mu. \tag{9}$$

If it holds, the algorithm returns **True**; else, an error symbol $\perp$ is returned as a result.

Theorem 2. *A designated verifier can correctly verify the signer's signature with Eq. (9).*

Proof: From the left-hand side of Eq. (9), it can be obtained that

$$\begin{aligned}
&e(\sigma, g^{h1(m, R)} y_s) \\
&= e(g^{1/(x_s + h1(m, R))}, g^{h1(m, R)} y_s) && \text{(by Eq. (4))} \\
&= e(g, g) \\
&= \mu
\end{aligned}$$

which leads to the right-hand side of Eq. (9).

– **Eval1**(δ, u)**:** On inputting a ciphertext $\delta = (T, \sigma, r)$ and a random number u, the algorithm computes a

recipient proof challenge D as

$$D = T^u. \quad (10)$$

– **Eval2**(D, x_v)**:** On inputting a recipient proof challenge D and the private key x_v of designated recipient, the algorithm computes a recipient proof Λ as

$$\Lambda = D^{x_v^{-1}}. \quad (11)$$

– **Judge**$(\delta, \Omega, u, \Lambda)$**:** On inputting a ciphertext $\delta = (T, \sigma, r)$, a signature $\Omega = (R, \sigma)$, a random number u and a recipient proof Λ, the algorithm verifies whether

$$\Lambda = R^u. \quad (12)$$

If it holds, the algorithm returns **True**; else, an error symbol $\perp$ is returned as a result.

5. Security Proof and Efficiency

In this section, the author first proves the security of the proposed scheme and then evaluate the efficiency of this system. Some comparisons with previous mechanisms in terms of security properties and functionalities are also made.

5.1. Security Proofs

The underlying security assumptions of this work are BSDH and q-SDH. The former is a variant of the well-known intractable BDH assumption that has been adopted in many cryptographic schemes while the latter is introduced by Boneh and Boyen [3] in 2008. According to their literature, the q-SDH assumption could be regarded as a discrete logarithm analogue of the Strong RSA assumption. Therefore, it can be suggested that it is difficult for any adversary to break either the BSDH or the q-SDH assumption with any technique of computing attacks.

Definition1. (Confidentiality) *A VAE scheme is secure against adaptive chosen-ciphertext attacks (CCA2) in the random oracle model if no probabilistic polynomial-time adversary $\mathcal{A}$ having a non-negligible advantage to beat a challenger $\mathcal{B}$ in the following game:*

Setup: The challenger $\mathcal{B}$ first delivers public parameters *params* to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ is permitted to submit several queries adaptively below.

- *Keygen query* $\langle i \rangle$*:* Whenever $\mathcal{A}$ asks a Keygen query $\langle i \rangle$, $\mathcal{B}$ returns $(y_i, Cert_i)$ to $\mathcal{A}$.
- *SEnc query* $\langle m, y_i, y_j \rangle$*:* Whenever $\mathcal{A}$ asks an SEnc query for some message m with respect to the public keys (y_i, y_j), $\mathcal{B}$ returns a corresponding ciphertext δ to $\mathcal{A}$.
- *SDec query* $\langle \delta, y_i, y_j \rangle$*:* Whenever $\mathcal{A}$ asks an SDec query for some ciphertext δ with respect to the public keys (y_i, y_j), $\mathcal{B}$ returns a decrypted message along with a transformed signature Ω.
- *SVerify query* $\langle m, \Omega, y_i \rangle$*:* Whenever $\mathcal{A}$ asks an SVerify query for some message m, a transformed signature Ω with respect to the public key y_i, $\mathcal{B}$ returns either **True** or an error symbol $\perp$ depending on the validity of the signature Ω.
- *Eval1 query* $\langle \delta, u \rangle$*:* Whenever $\mathcal{A}$ asks an Eval1 query for some ciphertext δ and a random number u, $\mathcal{B}$ returns a recipient proof challenge D.
- *Eval2 query* $\langle D, y_j \rangle$*:* Whenever $\mathcal{A}$ asks an Eval2 query for some recipient proof challenge D and the public key y_j of designated recipient, $\mathcal{B}$ returns a recipient proof Λ.
- *Judge query* $\langle \delta, \Omega, u, \Lambda \rangle$*:* Whenever $\mathcal{A}$ asks a Judge query for some ciphertext δ, a transformed signature Ω, a random number u and a recipient proof Λ, $\mathcal{B}$ returns either **True** or an error symbol $\perp$ depending on the validity of the recipient proof Λ.

Challenge: $\mathcal{A}$ picks up two messages of the same length, say m_0 and m_1. The challenger $\mathcal{B}$ will create an authenticated ciphertext δ^* for m_λ which is determined by an internal flipped coin $\lambda \leftarrow \{0, 1\}$ and then the ciphertext δ^* is returned to $\mathcal{A}$ as a challenge.

Phase 2: $\mathcal{A}$ submits new queries as those described in Phase 1. Note that any SDec query in relation to the target challenge is not allowed.

Guess: At the end of this game, $\mathcal{A}$ outputs a bit λ'. It can be said that $\mathcal{A}$ is the winner of the game on condition that $\lambda' = \lambda$. The advantage of $\mathcal{A}$ is thus could be defined as $Adv(\mathcal{A}) = |\Pr[\lambda' = \lambda] - 1/2|$.

Theorem 3. (Proof of Confidentiality) *The proposed VAE scheme can resist adaptive chosen-ciphertext attacks (CCA2) in the random oracle model if no probabilistic polynomial-time adversary having a non-negligible advantage to break the BSDHP.*

Proof: Assume there is a probabilistic polynomial-time adversary $\mathcal{A}$ who has a non-negligible advan-

tage ε to plot the adaptive chosen-ciphertext attacks for breaking the proposed VAE scheme. The adversary $\mathcal{A}$ will submit at most q_i queries for each kind of oracle i. In this case, one could build another algorithm $\mathcal{B}$ that would have a non-negligible advantage to break the BSDHP by employing $\mathcal{A}$'s advantage. The goal of the algorithm $\mathcal{B}$ is to compute $e(g, g)^{a^2b}$ by inputting a problem instance (g, g^a, g^b). In the following proof, a challenger will be acted by $\mathcal{B}$ for answering the queries of $\mathcal{A}$.

Setup: The challenger $\mathcal{B}$ first performs the Setup(1^k) algorithm and then delivers public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, g, e, \mu = e(g, g)\}$ to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ is granted to adaptively submit the following oracle queries:

- h_1 *oracle:* When being queried with an $h_1(m, R)$ oracle, $\mathcal{B}$ first looks a matched record up in the h_1-list. If not, $\mathcal{B}$ chooses $v_1 \in_R Z_q$, keeps (m, R, v_1) in the h_1-list and then returns v_1.
- h_2 *oracle:* When being queried with an $h_2(R, \sigma, z)$ oracle, $\mathcal{B}$ first looks a matched record up in the h_2-list. If not, $\mathcal{B}$ seeks an entry of the form $(R, \sigma,$ NULL, $v_2)$ and then replaces NULL with z. Otherwise, $\mathcal{B}$ chooses $v_2 \in_R \{0, 1\}^k$, keeps (R, σ, z, v_2) in the h_2-list and then returns v_2.
- h_3 *oracle:* When being queried with an $h_3(R)$ oracle, $\mathcal{B}$ first looks a matched record up in the h_3-list. If not, $\mathcal{B}$ chooses $v_3 \in_R \boldsymbol{G}_1$, keeps (R, v_3) in the h_3-list and then returns v_3.
- *Keygen query* $\langle i \rangle$*:* When being queried with a Keygen query $\langle i \rangle$, $\mathcal{B}$ responds as follows. If $i = U_s$, $\mathcal{B}$ returns y_s $(= g^a)$. If $i = U_v$, $\mathcal{B}$ returs y_v $(= g^b)$. Otherwise, $\mathcal{B}$ returns $y_i \leftarrow$ Keygen(i) to $\mathcal{A}$.
- *SEnc query* $\langle m, y_i, y_j \rangle$*:* When being queried with an SEnc query for some message m with respect to the public keys (y_i, y_j), $\mathcal{B}$ returns $\delta \leftarrow$ SEnc(m, x_i, y_j) if $y_i \neq g^a$. Whenever $y_i = g^a$, $\mathcal{B}$ would abort.
- *SDec query* $\langle \delta, y_i, y_j \rangle$*:* When being queried with an SDec query for some ciphertext δ with respect to the public keys $(y_i, y_j \neq g^b)$, $\mathcal{B}$ returns $(m, \Omega) \leftarrow$ SDec(δ, y_i, x_j) to $\mathcal{A}$. In case that $y_j = g^b$, $\mathcal{B}$ searches all records containing (R, σ) in the h_2-list. As long as any v_2 satisfies the equality of $e(\sigma, g^{h_1(r \oplus v_2, R)} y_s) = \mu$, $\mathcal{B}$ returns $\{m = r \oplus v_2, \Omega = (R, \sigma)\}$; else, $\mathcal{B}$ would abort.
- *SVerify query* $\langle m, \Omega, y_i \rangle$*:* When being queried with an SVerify query for some $\langle m, \Omega, y_i \rangle$, $\mathcal{B}$ returns the result of SVerify(m, Ω, y_i) to $\mathcal{A}$.
- *Eval1 query* $\langle \delta, u \rangle$*:* When being queried with an Eval1 query for some $\langle \delta, u \rangle$, $\mathcal{B}$ returns a recipient proof challenge $D \leftarrow$ Eval1(δ, u) to $\mathcal{A}$.
- *Eval2 query* $\langle D, y_j \rangle$*:* When being queried with an Eval2 query for some $\langle D, y_j \rangle$ where $y_j \neq g^a$ or g^b, $\mathcal{B}$ returns a recipient proof $\Lambda \leftarrow$ Eval2(D, x_j) to $\mathcal{A}$. Otherwise, $\mathcal{B}$ would abort.
- *Judge query* $\langle \delta, \Omega, u, \Lambda \rangle$*:* When being queried with a Judge query for some $\langle \delta, \Omega, u, \Lambda \rangle$, $\mathcal{B}$ returns the result of Judge$(\delta, \Omega, u, \Lambda)$ to $\mathcal{A}$.

Challenge: $\mathcal{A}$ picks up two messages of the same length, say m_0 and m_1. The challenger $\mathcal{B}$ creates an authenticated ciphertext δ^* for m_λ which is determined by an internal flipped coin $\lambda \leftarrow \{0, 1\}$ as follows:

Step 1 Choose $d, t, v_1 \in_R Z_q^*, \sigma^* \in_R \boldsymbol{G}_1$ and $v_2 \in_R \{0, 1\}^k$;

Step 2 Compute $T^* = g^{bt}$ and $R^* = g^t$;

Step 3 Compute $r^* = m_\lambda \oplus v_2$;

Step 4 Add the entry (m_λ, R^*, v_1) into h_1-list;

Step 5 Add the entry (R^*, g^{ad}) into h_3-list;

Step 6 Add the entry $(R^*, \sigma^*,$ NULL, $v_2)$ into h_2-list.

The ciphertext $\delta^* = (T^*, \sigma^*, r^*)$ is viewed as a target challenge for $\mathcal{A}$.

Phase 2: $\mathcal{A}$ could ask new queries just like those of Phase 1.

Output: At the end of this game, $\mathcal{A}$ outputs a bit λ' and $\mathcal{B}$ randomly selects a value z of some record in the h_2-list to compute $z^{d^{-1}}$ as its answer to the BSDHP.

Analysis of the game: On the basis of SDec algorithm defined above, the adversary $\mathcal{A}$ getting the challenge $\delta^* = (T^*, \sigma^*, r^*)$ would try to decrypt it for recovering the original message m_λ. To accomplish this job, $\mathcal{A}$ has to query an $h_2(R^*, \sigma^*, z^*)$ oracle. Meanwhile, in the challenge phase, $\mathcal{B}$ has set $h_3(R^*) = g^{ad}$ and designated the value v_2 as the output of $h_2(R^*, \sigma^*, z^*)$ is which $z^* = e(y_s^{x_v}, g^{ad}) = e((g^a)^b, g^{ad}) = e(P, P)^{a^2bd}$. As long as the adversary $\mathcal{A}$ submits the above expected h_2 oracle query during phase 2, it is clear that $\mathcal{B}$ would have a non-negligible advantage to break the inputted instance of BSDHP. Although it is possible for the adversary $\mathcal{A}$ to successfully guess the correct value of an h_2 oracle query, it can be claimed that the probability for such an event occurring is not greater than 2^{-k}. It also implies that the probability of the desired value z^* stored in the h_2-list is not less than $(\varepsilon - 2^{-k})$. By randomly selecting a value z from the h_2-list to compute $z^{d^{-1}}$ as

the problem answer, $\mathcal{B}$ would have the chance of $q_{h_2}^{-1}$ to get the correct z^*, i.e., $\Pr[z = z^*]$ could be expressed as $q_{h_2}^{-1}$. Thus, it can be claimed that $\mathcal{B}$ breaks the instance of BSDHP with a non-negligible advantage $(q_{h_2}^{-1})(\varepsilon - 2^{-k})$ in polynomial-time assuming the entire interactive game is perfectly simulated without accidentally termination.

Definition2. (Unforgeability) *A VAE scheme is secure against adaptive chosen-message attacks (CMA) in the random oracle model if no probabilistic polynomial-time adversary $\mathcal{A}$ having a non-negligible advantage to beat a challenger $\mathcal{B}$ in the following game:*

Setup: The challenger $\mathcal{B}$ first delivers public parameters *params* to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ is permitted to submit Keygen, SEnc, SVerify, Eval1, Eval2 and Judge queries as those described in Definition 1 adaptively.

Forgery: $\mathcal{A}$ finally chooses a message m^* and then forges an authenticated ciphertext δ^*. It can be said that $\mathcal{A}$ is the winner of the game on condition that δ^* is valid. It should be noted that δ^* cannot be obtained from any SEnc query.

Theorem 4. (Proof of Unforgeability) *The proposed VAE scheme can resist adaptive chosen-message attacks (CMA) in the random oracle model if no probabilistic polynomial-time adversary having a non-negligible advantage to break the q-SDHP.*

Proof: Assume there is a probabilistic polynomial-time adversary $\mathcal{A}$ who has a non-negligible advantage ε to plot the adaptive chosen-message attacks for breaking the proposed VAE scheme. The adversary $\mathcal{A}$ will submit at most q_i queries for each kind of oracle i. In this case, one could build another algorithm $\mathcal{B}$ that would have a non-negligible advantage to break the q-SDHP by employing $\mathcal{A}$'s advantage. The goal of the algorithm $\mathcal{B}$ is to compute $(c, g^{1/(a+c)})$ for some $c \in Z_q$ by inputting a problem instance $(g, g^a, g^{a^2}, ..., g^{a^q}) \in \boldsymbol{G}_1^{q+1}$. In the following proof, a challenger will be acted by $\mathcal{B}$ for answering $\mathcal{A}$'s queries.

Setup: The challenger $\mathcal{B}$ first initializes the Setup(1^k) algorithm and then delivers public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, g, e, \mu = e(g, g)\}$ to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{A}$ is granted to adaptively submit h_1, h_2 and h_3 oracles and SEnc, SVerify, Eval1, Eval2 and Judge queries as those of Theorem 1. Note that when $\mathcal{A}$ makes a Keygen query $\langle i \rangle$ for $i = U_s$, $\mathcal{B}$ returns y_s $(= g^a)$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ returns $y_i \leftarrow$ Keygen(i) to $\mathcal{A}$.

Forgery: $\mathcal{A}$ outputs a forged authenticated ciphertext $\delta^* = (T^*, \sigma^*, r^*)$ for some message m^* with respect to the public keys (y_i, y_j).

Output: At the end of this game, $\mathcal{B}$ outputs $(h_1(m^*, R^*), \sigma^*)$ as the answer to the q-SDHP instance.

Analysis of the game: If the forged ciphertext $\delta^* = (T^*, \sigma^*, r^*)$ for some message m^* is valid and in relation to the public keys (y_i^*, y_j^*) where $y_i^* = g^a$, one can know that $\sigma^* = g^{1/(x_i + h_1(m^*, R^*))} = g^{1/(a+c)}$ for $c = h_1(m^*, R^*)$. Consequently, $(h_1(m^*, R^*), \sigma^*)$ is a correct answer to the q-SDHP instance. By utilizing $\mathcal{A}$'s non-negligible advantage ε, $\mathcal{B}$ would also a non-negligible advantage $n\varepsilon$ (where n is the likelihood for $y_i^* = g^a$) to solve the q-SDHP instance in polynomial-time.

In accordance with Theorem 4, it is evident that the proposed VAE scheme could withstand existential forgery attacks. Provided that there is no probabilistic polynomial-time adversary that could steal or forge a valid signing key, a signer cannot deny his/her signing behavior. Therefore, the following corollary can be obtained.

Corollary 1. *The proposed VAE scheme is secure in terms of the security characteristic of non-repudiation.*

5.2. Efficiency

For evaluating the performance of the proposed VAE system, some adopted operations and their notations are first defined below:

B: To compute a bilinear pairing operation;

H: To compute a secure one-way hash function;

E: To compute an exponentiation computation in $\boldsymbol{G}_1$.

Other operations like the exclusive-OR and the addition are neglected since these operations are relatively insignificant. The detailed computational and communicational evaluation results are demonstrated in Tables 2 and 3.

In order to make sure the practical feasibility of the proposed VAE system, the author of the paper further compare it with several previous mechanisms including Tsai et al.'s (a.k.a. TLT) [24], the Tahat-Abdallah (a.k.a. TA) [22], Tahat's [23] and Lin's [15] works. For convenience, some evaluated parts are first defined below:

C1: Convertible Signature

C2: Recipient Proof

C3: Non-delegatable

C4: CCA-Secure

C5: Security Assumptions

C6: Random Oracle Model Security Proof.

Table 2
Computational evaluation of the proposed VAE system

Algorithm	Complexity
Keygen	E
SEnc	3H + 4E + B
SDec	2H + 2E + B
SVerify	H + E + B
Eval1	E
Eval2	E
Judge	E

Table 3
Communicational evaluation of the proposed VAE system

Item	Evaluation
Ciphertext Length	$2\|\boldsymbol{G}_1\| + \|k\|$
Signature Length	$2\|\boldsymbol{G}_1\|$

Table 4
Comparisons of the proposed and previous schemes

	TLT	TA	Tahat	Lin	Proposed
C1	√	√	√	√	√
C2	×	×	×	×	√
C3	√	√	√	√	√
C4	Δ*	Δ*	Δ*	√	√
C5	DL & FA	FA & Chaotic map	ECDL	BDH & ECDL	BSDH & q-SDH
C6	×	×	×	√	√

Remark*: The symbol Δ stands for unknown, as the authors did not provide related security proofs.

Itemized comparisons in the light of functionalities and security are summarized as Table 4. According to this table, it could be seen that the proposed VAE system not only provides better functionalities, but is also more secure.

6. Conclusions

Authenticated encryption schemes played an important role in the applications of the digital world such as on-line auctions, confidential transactions and the protection of digital evidence, etc. In this paper, the author put the emphasis on the security requirement of non-delegatability along with the functionality of recipient proof and then proposed a novel verifiable AE (a.k.a. VAE) scheme based on the computational assumptions of BSDH and q-SDH. Unlike previous mechanisms which only provide heuristic security analyses, the paper formally prove that the proposed VAE scheme is secure under the attacking game models of adaptive chosen-ciphertext (CCA2) and adaptive chosen-message (CMA). The results of the computational evaluation of the proposed scheme reveal that the SEnc, the SDec and the SVerify algorithms only require to perform the time-consuming bilinear pairing computation once, which makes the proposed system suitable for practical implementation. As compared with previous similar approaches, the proposed VAE construction not only has a higher security level, but also supports better functionality.

Acknowledgement

This work was supported in part by the Ministry of Science and Technology of Republic of China under the contract number MOST 108-2221-E-019-027.

References

1. Araki, S., Uehara, S., Imamura, K. The Limited Verifier Signature and Its Application. IEICE Transactions on Fundamentals, 1999, E82-A(1), 63-68.
2. Arshad, R., Ikram, N. A Novel Convertible Authenticated Encryption Scheme Based on RSA Assumption. Information Assurance and Security Letters, 2010, 1, 041-046.
3. Boneh, D., Boyen, X. Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups. Journal of Cryptology, 2008, 21(2), 149-177. https://doi.org/10.1007/s00145-007-9005-7
4. Diffie, W., Hellman, M. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976, IT-22(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638
5. ElGamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, 1985, IT-31(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074

6. Horster, P., Michel, M., Peterson, H. Authenticated Encryption Schemes with Low Communication Costs. Electronics Letters, 1994, 30(15), 1212-1213. https://doi.org/10.1049/el:19940856
7. Hou, F., Wang, Z., Tang, Y., Liu, Z. Protecting Integrity and Confidentiality for Data Communication. Proceedings of the 9th International Symposium on Computers and Communications (ISCC), 2004, 1(28), 357-362. https://doi.org/10.1109/ISCC.2004.1358430
8. Hsu, C. L., Lin, H. Y. New Identity-Based Key-Insulated Convertible Multi-Authenticated Encryption Scheme. Journal of Network and Computer Applications, 2011, 34(5), 1724-1731. https://doi.org/10.1016/j.jnca.2011.06.005
9. Huang, H. F., Chang, C. C. An Efficient Convertible Authenticated Encryption Scheme and Its Variant. Proceedings of the 5th International Conference on Information and Communications Security (ICICS2003), Springer-Verlag, Berlin, 2003, 382-392. https://doi.org/10.1007/978-3-540-39927-8_35
10. Jacob, J. A Uniform Presentation of Confidentiality Properties. IEEE Transactions on Software Engineering, 1991, 17(11), 1186-1194. https://doi.org/10.1109/32.106973
11. Lee, C. C., Hwang, M. S., Tzeng, S. F. A New Convertible Authenticated Encryption Scheme Based on the ElGamal Cryptosystem. International Journal of Foundations of Computer Science, 2009, 20(2), 351-359. https://doi.org/10.1142/S0129054109006607
12. Li, F., Sun, X., Zhang, X., Wan, L., Yan, S. A New Authenticated Encryption Schemes Without Using Hash and Redundancy Functions. Proceedings of 2010 the 2nd International Conference on Industrial Mechatronics and Automation, 2010, 1, 378-381. https://doi.org/10.1109/ icindma.2010.5538129
13. Lin, H. Y. Group-Oriented Data Access Structure Using Threshold-CAE Scheme and Its Extension. Information Technology and Control, 2014, 43(3), 252-263. https://doi.org/10.5755/j01.itc.43.3.5708
14. Lin, H. Y. PCMAE: A Proxy Convertible Multi-AE Scheme and Its Variant. Information Technology and Control, 2017, 46(4), 530-545. https://doi.org/10.5755/j01.itc.46.4.15819
15. Lin, H. Y. A Novel Dual Authenticated Encryption Scheme Suitable for Social Networking Services. Applied Sciences, 2019, 9(7-1452), 1-11. https://doi.org/10.3390/app9071452
16. Lu, C. F., Hsu, C. L., Lin, H. Y. Provably Convertible Multi-Authenticated Encryption Scheme for Generalized Group Communications. Information Sciences, 2012, 199(15), 154-166. https://doi.org/10.1016/j.ins.2012.02.051
17. Lv, J., Wang, X., Kim, K. Practical Convertible Authenticated Encryption Schemes Using Self-Certified Public Keys. Applied Mathematics and Computation, 2005, 169(2), 1285-1297. https://doi.org/10.1016/j.amc.2004.10.057
18. Rivest, R., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978, 21(2), 120-126. https://doi.org/10.1145/357980.358017
19. Schneider, S. Formal Analysis of a Non-Repudiation Protocol. Proceedings of 11th IEEE Computer Security Foundations Workshop, IEEE Press, Piscataway, USA, 1998, 54-65. https://doi.org/10.1109/CSFW.1998.683155
20. Sekhar, M. R. Signatures Scheme with Message Recovery and Its Applications. International Journal of Computer Mathematics, 2004, 81(3), 285-289. https://doi.org/10.1080/00207160410001661294
21. Stallings, W. Cryptography and Network Security: Principles and Practices, 4th Ed., Pearson, 2005.
22. Tahat, N., Abdallah, E. Hybrid Publicly Verifiable Authenticated Encryption Scheme Based on Chaotic Maps and Factoring Problems. Journal of Applied Security Research, 2018, 13(3), 304-314. https://doi.org/10.1080/19361610.2018.1463135
23. Tahat, N. Convertible Multi-Authenticated Encryption Scheme with Verification Based on Elliptic Curve Discrete Logarithm Problem. International Journal of Computer Applications in Technology, 2016, 54(3), 229-235. https://doi.org/10.1504/IJCAT.2016.10000490
24. Tsai, C. Y., Liu, C. Y., Tsaur, S. C., Hwang, M. S. A Publicly Verifiable Authenticated Encryption Scheme Based on Factoring and Discrete Logarithms. International Journal of Network Security, 2017, 19(3), 443-448.
25. Tzeng, S. F., Tang, Y. L., Hwang, M. S. A New Convertible Authenticated Encryption Scheme with Message Linkages. Computers and Electrical Engineering, 2007, 33(2), 133-138. https://doi.org/10.1016/j.compeleceng.2006.02.005
26. Wu, T. S., Hsu, C. L. Convertible Authenticated Encryption Scheme. The Journal of Systems and Software, 2002, 62(3), 205-209. https://doi.org/10.1016/S0164-1212(01)00143-1

27. Wu, T. S., Lin, H. Y. Secure Convertible Authenticated Encryption Scheme Based on RSA. Informatica, 2009, 33(4), 481-486. https://doi.org/ 10.31449/inf.v33i4.265

28. Yoon, E. J., Yoo, K. Y. A Practical Convertible Authenticated Encryption Scheme with Message Linkages and Forward Secrecy. Proceedings of 2011 14th IEEE International Conference on Computational Science and Engineering, 2011, 339-342. https://doi.org/10.1109/CSE.2011.117

29. Yoon, E. J., Yoo, K. Y. Improved Hwang et al.'s Convertible Authenticated Encryption Scheme with Message Linkages for Message Flows. Proceedings of 2011 the 2nd International Conference on Networking and Distributed Computing, 2011, 183-186. https://doi.org/10.1109/ICNDC.2011.44

30. Zhang, F., Kim, K. A Universal Forgery on Araki et al.'s Convertible Limited Verifier Signature Scheme. IEICE Transactions on Fundamentals, 2003, E86-A(2), 515-51.

31. Zhang, F., Safavi-Naini, R., Susilo, W. An Efficient Signature Scheme from Bilinear Pairings and Its Applications. Proceedings of Public Key Cryptography (PKC 2004), Springer, 2004, 277-290. https://doi.org/10.1007/978-3-540-24632-9_20