applied sciences

MDPI

Article

A Novel Dual Authenticated Encryption Scheme Suitable for Social Networking Services

Han-Yu Lin

Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung 202, Taiwan; hanyu@mail.ntou.edu.tw

Received: 16 March 2019; Accepted: 4 April 2019; Published: 6 April 2019

Abstract: Nowadays there are many social networking services supporting three-party communication such as Skype, Line, and Facebook Messenger. To ensure the message security, a cryptographic encryption scheme is a commonly adopted measure. However, the traditional asymmetric encryption only allows one designated recipient to decrypt the ciphertext with his/her private key. It is thus difficult for two parties to share the same ciphertext without exposing their private keys. In this paper, the author comes up with a novel dual authenticated encryption (DAE) scheme designed for three-party communication environments. Specifically, a DAE scheme enables a party to generate a single ciphertext that could be solely decrypted by the other two participants without sharing their private keys. It is also formally shown that the proposed scheme achieves the crucial security properties using the random oracle proof model.

Keywords: dual authenticated encryption; three-party communication; bilinear pairing; public key; cryptography

1. Introduction

With the rise of the Internet, people have changed their behavior models in daily life. Needless to say, there have been more and more transactions made online. The traditional telephone is no longer the only way for people to communicate with others. E-mails, chat rooms, and all kinds of instant messenger software are available and better options for free. However, the online security also raises serious concerns. The public key cryptography (PKC) [1] introduced by Diffie and Hellman in 1976 can provide several security properties such as confidentiality [2,3], integrity, authenticity [4], and non-repudiation [5]. The cryptographic mechanisms of encryptions and digital signatures [6–8] are thus widely studied and adopted in various fields.

A conventional digital signature is publicly verifiable since the verification key is the signer's public key. To further control the capability of validating a given signature, a hybrid scheme that combines an encryption mechanism and a signature one is the commonly utilized approach. The so-called authenticated encryption (AE) scheme introduced by Horster et al. [9] is a representative of this approach. In such a scheme, the sender can designate an intended recipient as the only person who is able to decrypt the ciphertext and verify the corresponding signature. Later, Zheng [10] and Petersen and colleagues [11] also proposed different hybrid mechanisms called signcryption schemes, which employ the symmetric cryptographic operation to ensure confidentiality.

Since these hybrid systems only grant a designated recipient the access privilege to recover the message and verify its signature, a malicious sender can easily frame the recipient, resulting in a later dispute over repudiation. To deal with this problem, several researchers came up with various solutions. Zheng's work [12] adopted the technique of zero-knowledge proofs [13–15] along with a trusted tamper-resistant device. Araki et al.'s literature [16] required the sender to cooperatively perform the arbitration process with the recipient and will increase extra computational burdens.

Wu and Hsu [17] and Huang and Chang [18] further incorporated the functionality of signature conversion into AE schemes and could be viewed as ideal methods. Yet, Lv et al. [19] found out that both of their protocols fail to satisfy the semantic security. Specifically, an adversary can easily decrypt a ciphertext with only two candidate messages. Since then, many improved hybrid schemes [20–32] have been proposed.

In recent years, social networking services including Facebook, Line, and Skype are widely utilized by people of any age. In addition to traditional two-party communication, multi-party (especially three-party) communication is commonly seen due to the development of broadband networks. To guarantee confidentiality and authenticity in the above applications, the design of group-oriented cryptographic mechanisms becomes quite important. In 2011, Hsu and Lin [33] introduced a new AE scheme supporting a group of signers to cooperatively deliver a designated ciphertext. Moreover, the private key of each user is updateable with unlimited time periods. In 2012, Lu et al. [34] further addressed a variant by extending one designated verifier to a group of n participants. In 2014, Lin [35] generalized the signing policy using a threshold value, i.e., only when the number of joined parties is equal to or greater than the threshold value, can they create a valid authenticated ciphertext. Nevertheless, most existing literatures focus on either the conventional two-party setting or the cooperative group environments. This motivates us to design a better alternative for more and more social networking services of three-party communication where each entity usually runs independent processes without cooperation.

Three-party communication is a natural extension of conventional two-party settings when someone joins the latter. For example, the sales representatives of two enterprises might chat online using the Line messenger service. When an important procurement is going to be made, a legal representative will be asked to join the communication for ensuring the validity of this transaction. Unlike many multi-party communication environments where those participants belong to the same group sharing a common key, a three-party communication usually contains independent recipients. We hence concentrate on a specific protocol that is suitable for the case of just three independent parties.

Although some existing protocols employed in social networking services also supports three-party communication, they usually utilize the techniques of group key management or symmetric key encryption. On the other hand, our scheme eliminates the cost of generating a group key and solves the problem of symmetric key encryption in which a ciphertext is bound by only a specific private key. One might further consider that the technique of (multi-party) attribute-based encryptions is applicable to the above three-party scenario. Nevertheless, the attribute issuing, verification, and management will increase the complexity of practical environments. Additionally, it would be a troublesome issue of how to prevent the attribute-collusion attack.

2. Preliminaries

We describe essential mathematical backgrounds and related computational assumptions in this section.

Bilinear Pairing

Let $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ be an additive and a multiplicative group of the same prime order q, respectively. We utilize the symbol of e to denote a bilinear map, i.e., e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ and it has the following properties:

(i) **Bilinearity:**

$$e(A_1 + B_2, P) = e(A_1, P)e(B_2, P);$$

$$e(P, A_1 + A_2) = e(P, A_1)e(P, A_2);$$

(ii) **Non-degeneracy**: Let P be a generator of the group $\boldsymbol{G}_1$. Then we say that $e(P, P)$ would be a generator of the group $\boldsymbol{G}_2$.

(iii) **Computability:** For any $A_1, B_2 \in \boldsymbol{G}_1$, there is an efficient algorithm to compute $e(A_1, B_2)$.

Elliptic Curve Discrete Logarithm Problem; ECDLP

Given two points $P, Q \in \boldsymbol{G_1}^2$ where P is a base point and $Q = aP$ for some integer $a \in Z_q^*$, the ECDLP is to compute a.

Elliptic Curve Discrete Logarithm (ECDL) Assumption

The advantage of every probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$ to solve the ECDLP is negligible. More precisely, let $D(k)$ be every positive polynomial with all sufficiently large k. Then we can express the algorithm $\mathcal{A}$'s probability to solve an ECDLP instance (P, Q) as

$$\Pr[\mathcal{A}(P, Q = aP) = a; a \leftarrow Z_q^*, P, Q \leftarrow {G_1}^2] \leq 1/D(K).$$

The probability is evaluated over the uniformly and independently chosen instance and over the random choices of $\mathcal{A}$.

Bilinear Diffie–Hellman Problem (BDHP)

Given four points $P, P_1, P_2, P_3 \in \boldsymbol{G_1}^4$ where P is a base point, $P_1 = xP$, $P_2 = yP$ and $P_3 = zP$ for some integers $x, y, z \in Z_q^*$, the BDHP is to compute $e(P, P)^{xyz} \in \boldsymbol{G_2}$.

Bilinear Diffie–Hellman (BDH) Assumption

The advantage of every PPT algorithm $\mathcal{A}$ to solve the BDHP is negligible. More precisely, let $D(k)$ be every positive polynomial with all sufficiently large k. Then, we can express the algorithm $\mathcal{A}$'s probability to solve a BDHP instance (P, P_1, P_2, P_3) as

$$\Pr[\mathcal{A}(P_1 = xP, P_1 = yP, P_3 = zP) = e(P, P)^{abc}; x, y, z \leftarrow Z_q^*, P, P_1, P_2, P_3 \leftarrow {G_1}^4] \leq 1/D(K).$$

The probability is evaluated over the uniformly and independently chosen instance and over the random choices of $\mathcal{A}$.

3. Proposed DAE Scheme

We present the proposed construction of DAE scheme utilizing bilinear pairing groups. Initially, the participated parties and the definition of algorithms are stated below.

3.1. Participated Parties

A DAE scheme consists of three participants including a sender and two designated recipients. The sender first utilizes his/her private key to create an authenticated ciphertext and transfers it to the other two participants. Then, each of the two designated recipients can run sole processes to decrypt the ciphertext and verify the corresponding signature. A DAE scheme is correct if a valid ciphertext generated by one party can only be solely decrypted and verified by the other two designated recipients in a three-party communication environment.

3.2. Algorithms

We describe the constituted algorithms of the proposed DAE scheme as follows:

Setup: Taking a security parameter k as input, a system authority runs the algorithm to generate necessary public parameters *params*.

Keygen: The algorithm takes as input an index i, and then outputs a corresponding key-pair (x_i, Y_i) along with a public key certificate $Cert_i$. Note that a valid certificate $Cert_i$ should be issued by a Certificate Authority who also maintains a certificate revocation list (CRL) to store revoked public key certificates. Anyone obtaining a public key first requests its corresponding certificate to verify the public key validity.

AEncrypt: The algorithm accepts input of a message m, two public keys of designated recipients and the private key of sender. The output is a corresponding authenticated ciphertext δ.

ADecrypt: The algorithm takes three parameters as input including an authenticated ciphertext δ, one private key of designated recipients and the public key of sender. If the ciphertext δ is valid, it outputs the decrypted message m and its signature Ω. Otherwise, an error symbol $\perp$ is returned as a result.

3.3. Concrete Construction

Setup: Given a 512-bit security parameter k, the system authority first chooses an additive group $\boldsymbol{G}_1$ and a multiplicative group $\boldsymbol{G}_2$ of the same prime order q. There is a generator P of order q in $\boldsymbol{G}_1$ and a bilinear map e satisfying that $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$. Some utilized collision-resistant hash functions are defined below.

h_1: $\{0, 1\}^k \times \boldsymbol{G}_1 \rightarrow Z_q^*$,
h_2: $\boldsymbol{G}_1 \times Z_q^* \; \boldsymbol{G}_1 \rightarrow \{0, 1\}^k$,
h_3: $\boldsymbol{G}_2 \rightarrow \boldsymbol{G}_1$.

The public parameters *params* include $\{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e, h_1, h_2, h_3\}$.

Keygen: Given an index i, a party U_i runs this algorithm to obtain the corresponding key-pair ($x_i \in_R Z_q$, $Y_i = x_i P$) along with a public key certificate $Cert_i$.

AEncrypt: Assume that U_a, U_b and U_c are engaged in a three-party communication environment. To deliver a message m designated for U_b and U_c, U_a runs the algorithm choosing an integer $t \in Z_q^*$ to compute

$$R = tP, \tag{1}$$

$$\sigma = t - x_a h_1(m, R), \tag{2}$$

$$Z = h_3(e(tY_c, Y_b)), \tag{3}$$

$$r = m \oplus h_2(R, \sigma, Z). \tag{4}$$

Then, the generated authenticated ciphertext $\delta = (R, \sigma, r)$ is returned and sent to U_b and U_c.

ADecrypt: Upon receiving $\delta = (R, \sigma, r)$, U_b and U_c can employ his/her own private key to run this algorithm which first computes

$$Z = h_3(e(x_i R, Y_b)) \text{ if } x_i = x_c, \tag{5A}$$

$$Z = h_3(e(Y_c, x_i R)) \text{ if } x_i = x_b, \tag{5B}$$

and decrypts the original message m as

$$m = r \oplus h_2(R, \sigma, Z). \tag{6}$$

With the redundancy embedded in m, it is able to check the validity of the recovered message. Moreover, the corresponding signature can be verified by checking if

$$R = \sigma P + h_1(m, R) Y_a. \tag{7}$$

If the above equality holds, the algorithm returns the message m and its signature $\Omega = (R, \sigma)$; else, a symbol $\perp$ is outputted to denote invalid ciphertext.

We prove that Equations (6) and (7) work correctly. From the right-hand side of Equation (6), we have

$$\begin{aligned}
& r \oplus h_2(R, \sigma, Z) \\
&= r \oplus h_2(R, \sigma, h_3(e(x_c R, Y_b))) && \text{(by Equation (5A))} \\
&= r \oplus h_2(R, \sigma, h_3(e(x_c tP, Y_b))) && \text{(by Equation (1))} \\
&= r \oplus h_2(R, \sigma, h_3(e(tY_c, Y_b))) \\
&= r \oplus h_2(R, \sigma, Z) && \text{(by Equation (3))} \\
&= m && \text{(by Equation (4))}
\end{aligned}$$

which leads to the left-hand side of Equation (6).

If an authenticated ciphertext $\delta = (R, \sigma, r)$ is correct, it should pass the test of Equation (7). From the left-hand side of Equation (7), we have

$$\begin{aligned} & R \\ &= tP && \text{(by Equation (1))} \\ &= (\sigma + x_a h_1(m, R))P && \text{(by Equation (2))} \\ &= \sigma P + h_1(m, R)Y_a \end{aligned}$$

which leads to the right-hand side of Equation (7).

4. Security Proof

In this section, we demonstrate the security of our DAE scheme based on some intractable computational problems. Specifically, we will adopt the random oracle proof model to show the essential security requirements of our mechanism.

4.1. Security Model

We first describe the critical security models of confidentiality and unforgeability for the proposed DAE scheme as follows:

Definition 1. (Confidentiality) *In adaptive chosen-ciphertext attacks, a DAE scheme fulfills confidentiality against indistinguishability (IND-CCA2) if there is no probabilistic polynomial-time bounded adversary $\mathcal{A}$ having a non-negligible advantage in the following game played with a challenger $\mathcal{B}$:*

Setup: By initializing the Setup algorithm, the challenger $\mathcal{B}$ will return the system's public parameters *params* to the adversary $\mathcal{A}$.
Phase 1: To simulate the capability of the adversary $\mathcal{A}$, we define three oracles that $\mathcal{A}$ could issue and $\mathcal{B}$ would respond with a consistent result.

Keygen oracle: $\mathcal{A}$ submits a Keygen oracle on an index i and $\mathcal{B}$ responds with $(Y_i, Cert_i)$, i.e., $(Y_i, Cert_i) \leftarrow Keygen(i)$.

AEncrypt oracle: $\mathcal{A}$ submits an AEncrypt oracle on (m, Y_a, Y_b, Y_c), and $\mathcal{B}$ responds with a corresponding authenticated ciphertext δ, i.e., $\delta \leftarrow AEncrypt(m, Y_a, Y_b, Y_c)$.

ADecrypt oracle: $\mathcal{A}$ submits an ADecrypt oracle on (δ, Y_a, Y_b, Y_c). Then $\mathcal{B}$ responds with either an error symbol $\perp$ or the decrypted message m along with its signature Ω, i.e., ($\perp$ or (m, Ω)) $\leftarrow ADecrypt(\delta, Y_a, Y_b, Y_c)$.
Challenge: The adversary $\mathcal{A}$ sends $\mathcal{B}$ two messages, m_0 and m_1, of the same length. The challenger $\mathcal{B}$ will generate an authenticated ciphertext δ^* for m_λ which is determined by an internal flipped coin $\lambda \leftarrow \{0, 1\}$ and then return it to $\mathcal{A}$ as a challenge.
Phase 2: In this phase, the adversary $\mathcal{A}$ is allowed to submit new oracles as those defined in Phase 1. However, any ADecrypt oracle containing the target ciphertext δ^* is prohibited.
Guess: Finally, the adversary $\mathcal{A}$ will output a bit λ'. When $\lambda' = \lambda$, we say that $\mathcal{A}$ wins the game. Therefore, the advantage of $\mathcal{A}$ in the above game could be expressed as $Adv(\mathcal{A}) = |\Pr[\lambda' = \lambda] - 1/2|$.

Definition 2. (Unforgeability) *In adaptive chosen-message attacks, a DAE scheme is existentially unforgeable (EF-CMA) if there is no probabilistic polynomial-time bounded adversary $\mathcal{A}$ having a non-negligible advantage in the following game played with a challenger $\mathcal{B}$:*

Setup: By initializing the Setup algorithm, the challenger $\mathcal{B}$ will return the system's public parameters *params* to the adversary $\mathcal{A}$.
Phase 1: In this game, the capability of adversary $\mathcal{A}$ includes Keygen and AEncrypt oracles which are defined the same as those of Definition 1.

Forgery: After querying enough oracles, the adversary $\mathcal{A}$ will arbitrarily choose a message m^* and forge its corresponding ciphertext δ^*. It is not allowed for $\mathcal{A}$ to directly obtain δ^* from any AEncrypt oracle. If the forged ciphertext δ^* for m^* is valid, we say that the adversary $\mathcal{A}$ wins the game.

4.2. Security Proofs

Based on previously defined security models, we formally prove the security of our DAE scheme in the security notion of IND-CCA2 and EF-CMA.

Theorem 1. **(Proof of Confidentiality)** *In the IND-CCA2 security notion, the proposed DAE scheme is said to be (t, ε)-secure if no probabilistic polynomial-time bounded adversary having a non-negligible advantage ε′ breaks BDHP within the time t′, where*

$$\varepsilon' \geq (\frac{1}{q_{h_3}})(2\varepsilon - \frac{q_{ADecrypt}}{2^k}),$$

$$t' \approx t + t_\lambda.$$

Here, t_λ represents the required time of executing all oracles.

Proof: It is assumed that in the security notion of IND-CCA2, there is a probabilistic polynomial-time adversary $\mathcal{A}$ having a non-negligible advantage ε to break the proposed DAE scheme within the time t. The capability of the adversary $\mathcal{A}$ includes those stated in Definition 1 and h_i oracles (for i = 1, 2, and 3). Let q_O be the maximum times that $\mathcal{A}$ is allowed to query for each oracle O. The theorem is proven by the technique of contradiction, i.e., we will create a (t', ε')-algorithm $\mathcal{B}$ which utilizes the advantage of $\mathcal{A}$ to break an BDHP instance of (P, xP, yP, zP). The goal of the algorithm $\mathcal{B}$ is to compute $e(P, P)^{xyz}$. When $\mathcal{A}$ submits an oracle query, $\mathcal{B}$ also acts as a challenger to make a response.

Setup: By initializing the Setup algorithm, the challenger $\mathcal{B}$ returns the system's public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e\}$ to the adversary $\mathcal{A}$, who selects a target sender U_a and two participants U_b and U_c in the simulated three-party communication environment.

Phase 1: The interactions between the adversary $\mathcal{A}$ and the algorithm $\mathcal{B}$ are described below.

h_1 oracle: When $\mathcal{A}$ submits a fresh h_1 oracle on (m, R), $\mathcal{B}$ responds with an integer $v_1 \in_R Z_q$. The record (m, R, v_1) is also kept for future inspection.

h_2 oracle: When $\mathcal{A}$ submits a fresh h_2 oracle on (R, σ, Z), $\mathcal{B}$ responds with a vale $v_2 \in_R \{0, 1\}^k$. The record (R, σ, Z, v_2) is also kept for future inspection.

h_3 oracle: When $\mathcal{A}$ submits a fresh h_3 oracle on $v_3 \in \boldsymbol{G}_2$, $\mathcal{B}$ responds with a vale $V_3 \in_R \boldsymbol{G}_1$. The record (v_3, V_3) is also kept for future inspection.

Keygen oracle: When $\mathcal{A}$ submits a fresh Keygen oracle on the index $i \in (b, c)$, $\mathcal{B}$ directly returns either $(yP, Cert_b)$ for $i = b$ or $(zP, Cert_c)$ for $i = c$. Otherwise, $\mathcal{B}$ submits a Keygen(i) oracle to get $(x_i, Y_i, Cert_i)$ and then responds with $(Y_i, Cert_i)$.

AEncrypt oracle: When $\mathcal{A}$ submits a fresh AEncrypt oracle on (m, Y_i, Y_j, Y_k) where $i \notin (b, c)$, $\mathcal{B}$ responds with $\delta \leftarrow AEncrypt(m, Y_i, Y_j, Y_k)$. Otherwise, $\mathcal{B}$ aborts.

ADecrypt oracle: When $\mathcal{A}$ submits a fresh ADecrypt oracle on $\{\delta = (R, \sigma, r), Y_i, Y_j, Y_k\}$ where $(j, k) \neq (b, c)$, $\mathcal{B}$ responds with $ADecrypt(\delta, Y_i, Y_j, Y_k)$. In case that $(j, k) = (b, c)$, $\mathcal{B}$ inspects all h_2 oracle records containing the parameter (R, σ). If the value v_2 of any matched record fulfills that $R = \sigma P + h_1(r \oplus v_2, R)Y_i$, $\mathcal{B}$ responds with $\{m = r \oplus v_2, \Omega = (R, \sigma)\}$; else, an error symbol is returned.

Challenge: The adversary $\mathcal{A}$ sends $\mathcal{B}$ two messages, m_0 and m_1, of the same length. Next, the challenger $\mathcal{B}$ flips an internal coin $\lambda \leftarrow \{0, 1\}$ to decide m_λ, chooses $v_1, \sigma^* \in_R Z_q$, $v_2 \in_R \{0, 1\}^k$ and generates an authenticated ciphertext $\delta^* = (R^*, \sigma^*, r^*)$ where $R^* = xP$ and $r^* = m_\lambda \oplus v_2$. For consistency, two records of (m_λ, R^*, v_1) and $(R^*, \sigma^*, \text{null}, v_2)$ are also separately added into the lists of h_1 and h_2 oracles. Finally, the ciphertext δ^* is returned to $\mathcal{A}$ as a target challenge.

Phase 2: The adversary $\mathcal{A}$ can issue new oracles as those stated in Phase 1. Yet, any ADecrypt oracle containing the target ciphertext δ^* is prohibited.

Analysis of the game: According to previous simulation of this game, it can be seen that the public keys Y_b and Y_c are set as yP and zP, respectively, and the ciphertext parameter R^* is set as xP. When the adversary $\mathcal{A}$ queries an h_3 oracle on (R^*, σ^*, Z^*) where $Z^* = h_3(e(Y_c, x_bR^*)) = h_3(e(P, P)^{xyz})$ in phase 2, $\mathcal{B}$ would have a non-negligible advantage $\frac{1}{q_{h_3}}$ to solve the BDHP instance. Such an event is referred to as H_3O^*. However, $\mathcal{B}$ might respond with an error symbol for an ADecrypt oracle on some valid ciphertext if $\mathcal{A}$ had never submitted the corresponding h_2 oracle. We denote the event as ADecrypt_ERR and $\Pr[\text{ADecrypt\_ERR}] \leq \frac{q_{ADecrypt}}{2^k}$ for the entire simulation game. When the game is perfectly simulated, represented as the event PS, the adversary $\mathcal{A}$ has no overwhelming probability in outputting λ, i.e., $\Pr[\lambda' = \lambda \mid \text{PS}] = 1/2$. Based on conditional probability and further derivations, we know that $\mid \Pr[\lambda' = \lambda] - 1/2 \mid \leq (1/2)\Pr[\neg\text{PS}]$. Since our initial assumption gives the adversary $\mathcal{A}$ the probability ε to break the proposed DAE scheme, we have

$$\begin{aligned}
&\varepsilon = \mid \Pr[\lambda' = \lambda] - 1/2 \mid \\
&\leq (1/2)\Pr[\neg\text{PS}] \\
&= (1/2)(\Pr[\text{H}_3\text{O}* \vee \text{ADecrypt_ERR}]) \\
&\leq (1/2)(\Pr[\text{H}_3\text{O}*] + \Pr[\text{ADecrypt_ERR}]) \\
&= (1/2)(\Pr[\text{H}_3\text{O}*] + \tfrac{q_{ADecrypt}}{2^k})
\end{aligned}$$

which means that

$$\Pr[\text{H}_3\text{O}*] \geq 2\varepsilon - \frac{q_{ADecrypt}}{2^k}.$$

Then, the success probability of the algorithm $\mathcal{B}$ can be represented as $\varepsilon' \geq (\frac{1}{q_{h_3}})(2\varepsilon - \frac{q_{ADecrypt}}{2^k})$ and the running time is $t' \approx t + t_\lambda$. As we know that BDHP is polynomial-time intractable, the simulation result of this game is clearly a contradiction, which indicates that our initial assumption is wrong. Therefore, we conclude that the proposed DAE scheme is secure in the IND-CCA2 security notion.

Q.E.D.

Theorem 2. (Proof of Unforgeability) *In the EF-CMA security notion, the proposed DAE scheme is said to be (t, ε)-secure if no probabilistic polynomial-time bounded adversary having a non-negligible advantage $\varepsilon \geq 10(q_{AEncrypt} + 1)(q_{AEncrypt} + q_{h1})/2^k$ breaks ECDLP within the time $t' \leq 120686q_{h_1}t/\varepsilon$.*

Proof: Let $\mathcal{A}$ be a probabilistic polynomial-time adversary who can asks oracles as those stated in Definition 2 and h_i oracles (for i = 1, 2 and 3). Let q_O be the maximum times that $\mathcal{A}$ is allowed to query for each oracle O. It is assumed that in the security notion of EF-CMA, the adversary $\mathcal{A}$ has a non-negligible advantage ε to break the proposed DAE scheme within the time t. By using the techniques of oracle replay attack and Forking Lemma [36], we will create a (t', ε)-algorithm $\mathcal{B}$ which utilizes the advantage of $\mathcal{A}$ to break an ECDLP instance of (P, xP). The goal of the algorithm $\mathcal{B}$ is to compute x. When $\mathcal{A}$ submits an oracle query, $\mathcal{B}$ also acts as a challenger to make response.

Setup: By initializing the Setup algorithm, the challenger $\mathcal{B}$ returns the system's public parameters $params = \{G_1, G_2, q, P, e\}$ along with a prepared random tape consisting of random bits to the adversary $\mathcal{A}$ who also selects a target sender U_a and two participants U_b and U_c in the simulated three-party communication environment. Then, $\mathcal{B}$ initiates two rounds of the proposed DAE scheme with $\mathcal{A}$ on the same system parameters.

Phase 1: The interactions between the adversary $\mathcal{A}$ and the algorithm $\mathcal{B}$ are described below. For all hash oracles, $\mathcal{B}$ behaves as those in Theorem 1.

Keygen query: When $\mathcal{A}$ submits a fresh Keygen oracle on the index $i = a$, $\mathcal{B}$ directly returns (xP, $Cert_a$). Otherwise, $\mathcal{B}$ submits a Keygen(i) oracle to get (x_i, Y_i, $Cert_i$) and then responds with (Y_i, $Cert_i$).

AEncrypt query: When $\mathcal{A}$ submits a fresh AEncrypt oracle on (m, Y_i, Y_j, Y_k) where $i \notin a$, $\mathcal{B}$ responds with $\delta \leftarrow AEncrypt(m, Y_i, Y_j, Y_k)$. In case that $i = a$, $\mathcal{B}$ first chooses $\sigma, v_1 \in_R Z_q^*$ and then responds with $\delta = (R, \sigma, r)$ where $R = \sigma P + v_1(xP)$ and $r = m \oplus h_2(R, \sigma, h_3(e(x_k R, Y_j)))$. For consistency, a record of (m, R, v_1) is also added into the list of h_1 oracle.

Forgery: At the end of this game, $\mathcal{A}$ outputs a forged ciphertext $\delta = (R, \sigma, r)$ with respect to (m, Y_a, Y_b, Y_c).

Analysis of the game: As mentioned before, the algorithm $\mathcal{B}$ will initiate two rounds of the proposed DAE scheme with the adversary $\mathcal{A}$ on the same parameters and random tape. By utilizing the same random tape in the second round, we can expect that the adversary $\mathcal{A}$ always chooses identical random bits as those used in the first round. However, in the second round, we will replace the oracle response of $h_1(m, R)$ with a new value, say $v_1{}^*$. If the final forgery $\delta^* = (R, \sigma^*, r^*)$ in relation to (m, Y_a, Y_b, Y_c) is also valid and $h_1(m, R) = v_1{}^*$, the algorithm $\mathcal{B}$ can learn two equalities:

$$\sigma = t - xv_1,$$

$$\sigma^* = t - xv_1{}^*.$$

Combining and further deriving the above equalities, we can compute

$$x = \frac{\sigma - \sigma*}{v_1 * - v_1}$$

and solve the ECDLP instance. Therefore, we can express the success probability of the algorithm $\mathcal{B}$ as $\varepsilon \geq 10(q_{AEncrypt} + 1)(q_{AEncrypt} + q_{h1})/2^k$ and the expected running time is $t' \leq 120686 q_{h1} t/\varepsilon$. Since ECDLP is a well-known NP problem, the advantage and running time of the constructed algorithm $\mathcal{B}$ is clearly a contradiction. We thus can conclude that the proposed DAE scheme is secure in the EF-CMA security notion.

Q.E.D.

5. Efficiency

To ensure the practical benefits, we evaluate the efficiency of our DAE scheme in terms of computational efforts in the three-party communication environment. For convenience, some time-consuming computation and their approximate running time experimented by [37] are first defined as Table 1. It is believed that the bilinear pairing operation is the most complicated operation in a pairing-based system. We show detailed evaluation with some related protocols including Lee et al.'s (LCL for short) [38], Hsu and Lin (HL for short) [22], Islam and Biswas (IB for short) [39] and Chen et al.'s (CZXY for short) [40] schemes in Table 2. The comparisons of communication overheads in terms of ciphertext length are also demonstrated in Table 3 utilizing a super singular elliptic curve E/F_p: $y^2 = x^3 + x$ with a 160-bit prime q and a 512-bit prime p. It is obvious to see that the proposed DAE scheme is more efficient from either the computational perspective of sender or that of recipient. However, it should be noted that more than 100 ms total time would be unacceptable for a real-time synchronous voice or video communication. As for the text messaging, we claim that the transmission latency is noticeable, but acceptable with the tradeoff of higher security level. Figure 1 further demonstrates the difference of computational efforts among different quantities of ciphertext.

Table 1. Definition of utilized notations.

Symbol	Description	Approximate Running Time
T_B	the computational time of a bilinear pairing operation	20.01 ms
T_E	the computational time of an exponentiation in G_2	11.20 ms
T_M	the computational time of a pairing-based scalar multiplication	6.38 ms

Table 2. Comparisons of computational costs in three-party communication environments.

Scheme	Computational Costs of Sender	Computational Costs of Each Recipient	Total Computational Costs
LCL	$4T_B + 4T_M$ (≈211.12 ms)	$2T_B + T_M$ (≈46.4 ms)	$8T_B + 6T_M$ (≈198.36 ms)
HL	$2T_B + 8T_M$ (≈91.06 ms)	$3T_B + 3T_M$ (≈79.17 ms)	$8T_B + 14T_M$ (≈249.4 ms)
IB	$6T_B + 6T_M + 2T_E$ (≈198.74 ms)	$T_B + T_M + T_E$ (≈46.59 ms)	$8T_B + 8T_M + 4T_E$ (≈291.92 ms)
CZXY	$2T_B + 6T_M$ (≈78.3 ms)	$T_B + 3T_M$ (≈39.15 ms)	$4T_B + 12T_M$ (≈156.6 ms)
Ours	$T_B + 3T_M$ (≈39.15 ms)	$T_B + 3T_M$ (≈39.15 ms)	$3T_B + 9T_M$ (≈117.45 ms)

Table 3. Comparisons of communication overheads in three-party communication environments.

	LCL	HL	IB	CZXY	Ours
Ciphertext Length (Byte)	256	384	256	296	148

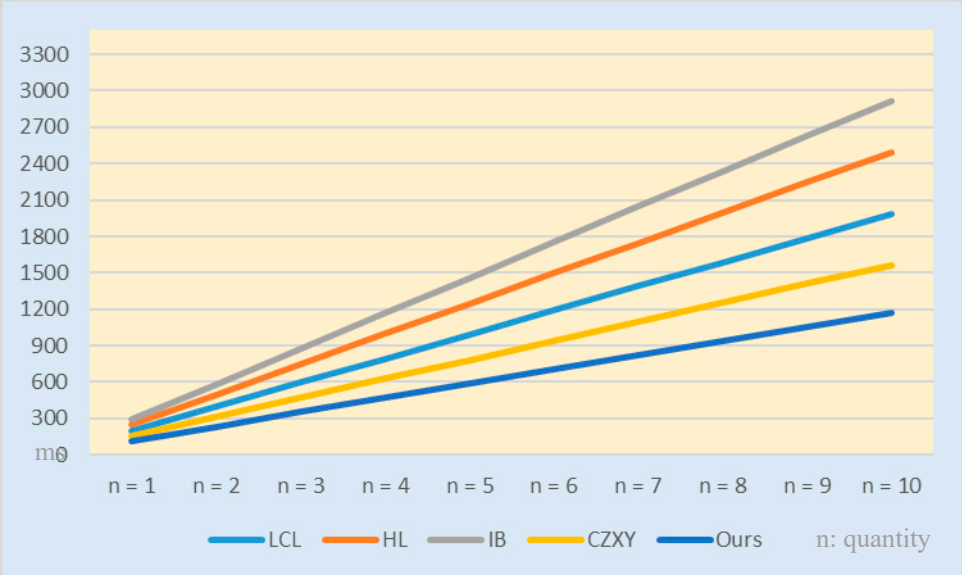

Figure 1. Comparison of computational costs among different quantities of ciphertext in the three-party communication environment.

6. Conclusions

For facilitating the three-party applications of many social networking services, in this paper, the author introduced a novel DAE scheme based on bilinear pairings. In the proposed scheme, a sender engaged in a three-party communication environment is able to generate a single authenticated ciphertext that could be solely decrypted and verified by the other two participants without compromising the confidentiality of their private keys. Unlike attribute-based encryption mechanisms in which a user's attribute is usually associated with the ciphertext or the decryption key, our scheme is implemented in the conventional public key system without managing any attribute. As for the security, we showed that our approach is computationally secure in the notion of IND-CCA2 and that of EF-CMA by utilizing the random oracle proof model. In addition, we compared our scheme with two previous straightforward protocols in terms of computational efforts. The experimental results clearly reveal that the proposed DAE scheme is really a better alternative for three-party communication environments.

Funding: This work was supported in part by the Ministry of Science and Technology of Republic of China under the contract number MOST 107-2221-E-019-017.

Conflicts of Interest: The author declares that he has no conflict of interest.

References

1. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE T. Inform. Theory* **1976**, *IT-22*, 644–654.
2. Hou, F.; Wang, Z.; Tang, Y.; Liu, Z. Protecting Integrity and Confidentiality for Data Communication. In Proceedings of the 9th International Symposium on Computers and Communications (ISCC'04), Alexandria, Egypt, 28 June–1 July 2004; pp. 357–362.
3. Jacob, J. A Uniform Presentation of Confidentiality Properties. *IEEE Trans. Softw. Eng.* **1991**, *17*, 1186–1194. [CrossRef]
4. Stallings, W. *Cryptography and Network Security: Principles and Practices*, 7th ed.; Pearson: London, UK, 2017.
5. Schneider, S. Formal Analysis of a Non-Repudiation Protocol. In Proceedings of the 11th IEEE Computer Security Foundations Workshop, IEEE Press, Rockport, MA, USA, 9–11 June 1998; pp. 54–65.
6. ElGamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trams. Inf. Theory* **1985**, *IT-31*, 469–472. [CrossRef]
7. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
8. Sekhar, M.R. Signatures Scheme with Message Recovery and Its Applications. *Int. J. Comput. Math.* **2004**, *81*, 285–289.
9. Horster, P.; Michel, M.; Peterson, H. Authenticated Encryption Schemes with Low Communication Costs. *Electron. Lett.* **1994**, *30*, 1212–1213. [CrossRef]
10. Zheng, Y. Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption). In Proceedings of the Advances in Cryptology—CRYPTO'97, Santa Barbara, CA, USA, 17–21 August 1997; Springer: Berlin/Heidelberg, Germany, 1997; pp. 165–179.
11. Petersen, H.; Michels, M. Cryptanalysis and Improvement of Signcryption Schemes. *IEE Proc. Comput. Digit. Tech.* **1998**, *145*, 149–151. [CrossRef]
12. Zheng, Y. Signcryption and Its Applications in Efficient Public Key Solutions. In Proceedings of the 1st International Workshop on Information Security (ISW'97), Tatsunokuchi, Japan, 17–19 September 1997; pp. 291–312.
13. Bellare, M.; Jakobsson, M.; Yung, M. Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function. In Proceedings of the Advances in Cryptology—EUROCRYPT'97, Konstanz, Germany, 11–15 May 1997; Springer: Berlin/Heidelberg, Germany, 1997; pp. 280–305.
14. Boyen, X. Multipurpose Identity-Based Signcryption—A Swiss Army Knife for Identity-Based Cryptography. In Proceedings of the Advances in Cryptology—CRYPTO'03, Santa Barbara, CA, USA, 17–21 August 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 383–399.
15. Chaum, D. Zero-Knowledge Undeniable Signatures. In Proceedings of the Advances in Cryptology—EUROCRYPT'90, Aarhus, Denmark, 21–24 May 1990; Springer: Berlin/Heidelberg, Germany, 1990; pp. 458–464.
16. Araki, S.; Uehara, S.; Imamura, K. The Limited Verifier Signature and Its Application. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **1999**, *E82-A*, 63–68.
17. Wu, T.S.; Hsu, C.L. Convertible Authenticated Encryption Scheme. *J. Syst. Softw.* **2002**, *62*, 205–209.
18. Huang, H.F.; Chang, C.C. An Efficient Convertible Authenticated Encryption Scheme and Its Variant. In Proceedings of the 5th International Conference on Information and Communications Security (ICICS 2003), Huhehaote, China, 10–13 October 2003; pp. 382–392.
19. Lv, J.; Wang, X.; Kim, K. Practical Convertible Authenticated Encryption Schemes Using Self-Certified Public Keys. *Appl. Math. Comput.* **2005**, *169*, 1285–1297. [CrossRef]
20. Chien, H.Y. Selectively Convertible Authenticated Encryption in the Random Oracle Model. *Comput. J.* **2008**, *51*, 419–434. [CrossRef]
21. Duan, S.; Cao, Z. Efficient and Provably Secure Multi-Receiver Identity-Based Signcryption. In Proceedings of the Australasian Conference on Information Security and Privacy (ACISP'06), Melbourne, Australia, 3–5 July 2006; pp. 195–206.

22. Hsu, C.L.; Lin, H.Y. Convertible Authenticated Encryption Scheme with Hierarchical Access Control. *Appl. Math. Inf. Sci.* **2014**, *8*, 1239–1246. [CrossRef]
23. Lee, C.C.; Hwang, M.S.; Tzeng, S.F. A New Convertible Authenticated Encryption Scheme Based on the ElGamal Cryptosystem. *Int. J. Found. Comput. Sci.* **2009**, *20*, 351–359. [CrossRef]
24. Lin, H.Y.; Hsu, C.L. A Novel Identity-Based Key-Insulated Convertible Authenticated Encryption Scheme. *Int. J. Found. Comput. Sci.* **2011**, *22*, 739–756. [CrossRef]
25. Lin, H.Y.; Hsu, C.L.; Huang, S.K. Improved Convertible Authenticated Encryption Scheme with Provable Security. *Inf. Process. Lett.* **2011**, *111*, 661–666. [CrossRef]
26. Lin, H.Y.; Wu, T.S.; Huang, S.K. An Efficient Strong Designated Verifier Proxy Signature Scheme for Electronic Commerce. *J. Inf. Sci. Eng.* **2012**, *28*, 771–785.
27. Luo, M.; Wen, Y.; Zhao, H. A Certificate-Based Signcryption Scheme. In Proceedings of the 2008 International Conference on Computer Science and Information Technology, Singapore, 29 August–2 September 2008; pp. 17–23.
28. Wu, T.S.; Chen, Y.S.; Lin, H.Y.; Chang, T.K. Authenticated Encryption Scheme Based on Paillier System with Verifiable Public Keys. *Commun. Comput. Secur.* **2012**, *2*, 1–5. [CrossRef]
29. Wu, T.S.; Lin, H.Y. Efficient Self-Certified Proxy CAE Scheme and Its Variants. *J. Syst. Softw.* **2009**, *82*, 974–980. [CrossRef]
30. Wu, T.S.; Lin, H.Y. Secure Convertible Authenticated Encryption Scheme Based on RSA. *Informatica* **2009**, *33*, 481–486.
31. Wu, T.S.; Lin, H.Y.; Ting, P.Y. A Publicly Verifiable PCAE Scheme for Confidential Applications with Proxy Delegation. *Trans. Emerg. Telecommun. Technol.* **2012**, *23*, 172–185. [CrossRef]
32. Wu, T.S.; Lin, H.Y.; Tsao, S.H.; Ting, P.Y. On the Construction of DL-Based Convertible Authenticated Encryption Scheme with Message Linkages. *Information* **2013**, *16*, 7983–7994.
33. Hsu, C.L.; Lin, H.Y. New Identity-Based Key-Insulated Convertible Multi-Authenticated Encryption Scheme. *J. Netw. Comput. Appl.* **2011**, *34*, 1724–1731. [CrossRef]
34. Lu, C.F.; Hsu, C.L.; Lin, H.Y. Provably Convertible Multi-Authenticated Encryption Scheme for Generalized Group Communications. *Inf. Sci.* **2012**, *199*, 154–166. [CrossRef]
35. Lin, H.Y. Group-Oriented Data Access Structure Using Threshold-CAE Scheme and Its Extension. *Inf. Technol. Control* **2014**, *43*, 252–263. [CrossRef]
36. Pointcheval, D.; Stern, J. Security Arguments for Digital Signatures and Blind Signatures. *J. Cryptol.* **2000**, *13*, 361–369. [CrossRef]
37. Cao, X.; Kou, W.; Du, X. A Pairing-Free Identity-Based Authenticated Key Agreement Protocol with Minimal Message Exchanges. *Inf. Sci.* **2010**, *180*, 2895–2903. [CrossRef]
38. Lee, J.S.; Chang, J.H.; Lee, D.H. Forgery Attacks on Kang et al.'s Identity-Based Strong Designated Verifier Signature Scheme and Its Improvement with Security Proof. *Comput. Electr. Eng.* **2010**, *36*, 948–954. [CrossRef]
39. Islam, S.K.H.; Biswas, G.P. Provably Secure Certificateless Strong Designated Verifier Signature Scheme Based on Elliptic Curve Bilinear Pairings. *J. King Saud Univ.-Comput. Inf. Sci.* **2013**, *25*, 51–61.
40. Chen, Y.; Zhao, Y.; Xiong, H.; Yue, F. A Certificateless Strong Designated Verifier Signature Scheme with Non-delegatability. *Int. J. Netw. Secur.* **2017**, *19*, 573–582.