A Secure Scheme for Authenticated Encryption

Fuw-Yi Yang
Department of Electronic Engineering
Chienkuo Technology University
Changhua City 500, Taiwan, R.O.C.
Email: yangfy@ms7.hinet.net

ABSTRACT

The paper proposes a new scheme of *authenticated encryption* that is either publicly verifiable or not publicly verifiable depending on the quantity of information the recipient released. This property would give recipient much flexibility in many applications. This scheme combines the ElGamal encryption with Schnorr signature. Considering the security goal of signature, the resultant scheme is at least as secure as that of the combined signature scheme. The security goal of encryption is examined under the chosen ciphertext attack, it is proven directly related to the security of signature. Furthermore, this new scheme is also secure against one-more-decryption attack. This novel security goal may be valuable in the applications of private information retrieval.

Keywords

Authenticated encryption, digital signature, encryption, one-more-decryption attack, signcryption.

1. INTRODUCTION

With the quick and ongoing growth of digitalized information, more and more data are being exchanged. Data transferred would be safe from eavesdrop or modification if participants communicate over a secure channel. However, building and maintaining a secure channel for any two prospective participants isn't a good solution to provide secure communication.

Generally, communication parties communicate over an insecure channel (an open channel). This channel could be a telephone line, computer network or Internet, for example. It is not

difficult to have a tapping device tagged on these channels. Therefore, there are eavesdroppers and intruders who can intercept and modify messages transmitted in an open channel.

Let's call the message to be transmitted plaintext m. Plaintext can be text data, executable program or any kind of information. Instead of sending plaintext to a recipient, an encryption scheme $E(.)$ is used to encrypt a plaintext and obtain a ciphertext c. Then the ciphertext is transmitted to the recipient. The recipient can turn the received ciphertext into plaintext by a decryption scheme $D(.)$. Needless to say, there must be some methods so that the processes of enciphering and deciphering work correctly, namely $m = D(c) = D(E(m))$, and no one except the recipient can decrypt the ciphertext to obtain the embedded plaintext. In the public-key cryptography [1-4], each participant has a published public key *pk* and a hidden secret key *sk*. Let pk_r (pk_s) and sk_r (sk_s) denote the recipient's (sender's) public key and secret key. Then the sender using the recipient's public key to construct a ciphertext, $c = E(pk_r, m)$, and sends it to the recipient. Upon receiving ciphertext c, the recipient uses secret key to recover plaintext, $m = D(sk_r, c)$. Theoretically, any eavesdropper should have no idea about the plaintext, since only the recipient knows secret key sk_r. In this way (using encryption scheme), the recipient's *privacy* is protected.

In some applications the recipient may require to make sure of the originator of each message received, *e.g*. key agreement, e-commerce, secure e-mailing. In the public-key setting, the scheme of digital signature can be used to generate a signature on either the plaintext or ciphertext. Then, sender sends recipient the signature together with the ciphertext. This signature confirms that the ciphertext was constructed and sent by the sender. Thus the sender's *authenticity* is protected. Since any modification of the original ciphertext will be detected by the signature, the signature protects the *integrity* of message. Furthermore, the signature also provides the property of *non-repudiation*. That is to say that the sender cannot deny having sent recipient the message.

Traditionally, the schemes of encryption and digital signature are consecutively applied to message to achieve the properties of *privacy*, *authenticity*, *integrity*, and *non-repudiation*. Namely,

enciphering comes after signing on a plaintext (sign-then-encrypt) or signing comes after enciphering a plaintext (encrypt-then-sign). The computational cost is thus the sum of the cost of the two steps. It is possible to integrate enciphering and signing into a single step while still provides the four properties as mentioned above. Indeed, a combination of ElGamal encryption [5] and signature scheme with message recovery [6-7] was presented in [7]. The scheme of *authenticated encryption* in [8] and schemes of *signcryption* in [9] are also integration of digital signature and encryption. The terminologies *signcryption* and *authenticated encryption* denote the same thing, *i.e.* integration of digital signature and encryption. This paper refers to this integration as *authenticated encryption*. Benefiting by the single step operation, the integrated scheme requires less computational cost, narrower communicational bandwidth, and lower expansion rate as compared with the two-step operations of encrypt-then-sign or sign-then-encrypt.

1.1 Related work

Since the germination of *authenticated encryption*, many related schemes have been proposed. Some of these schemes were discussed and arranged in chronological order in [10]. Some researchers further extended the schemes of *authenticated encryption* to the utilization of large message transmission [11-13]. We investigate some of the *authenticated encryption* schemes presented in [7-13]. The signature scheme in [13] signs on ciphertext so that it is difficult to possess the property of *non-repudiation*. Most of these schemes lack rigorous study of security. Namely, there may be potential weakness of leaking partial information. For example, the signature scheme in [11] is always forgeable; the encryption scheme in [12] and many schemes listed in [10] are not secure under the model of chosen ciphertext attack. More precisely, they are distinguishable in polynomial time, using the security definition in [14]. We give some words to explain secure encryption and attack model. Assume that an adversary is given the advantage of choosing two messages m_0 and m_1 (the same length). One of them is encrypted and hands on the ciphertext to the adversary. An encryption scheme is said to be secure if the adversary cannot determine whether the given ciphertext is an encryption of message m_0 or message m_1 in polynomial time. This definition of security comes from [14] and is called *polynomial*

indistinguishability (also known as semantic security [2]). In the attack model of chosen ciphertext, an adversary can access oracles of hash, encryption, and decryption while trying to extract some information about a given ciphertext. For more details about notion of security and attack model please refer to [2, 4, 14-15]. Surely, the adversary is inhibited to ask decryption oracle to decrypt the given ciphertext. Although the original schemes in [9] were formally proven to be secure in [16], they are not easy to fulfill the property of *non-repudiation* since the signature cannot be verified publicly. The worst of it is that to show *non-repudiation* in case of dispute, recipient's *privacy* is lost, as shown in [17].

To conquer the problem found in [9], some authenticated encryption schemes [12, 18-22] are designed so that the signatures are publicly verifiable. Like those schemes mentioned in [7-13], schemes in [18-20] are claimed to be secure without proof. Under the chosen ciphertext attack, the insecurity of schemes in [18-19] is shown in [21]. Scheme in [12, 20] also faces the same problem. Assume that the Gap Diffie-Hellman problem is hard; the authenticated encryption schemes in [21-22] are secure under the chosen ciphertext attack. However the scheme in [21] requires two additional assumptions, *i.e*. a secure symmetric encryption scheme and a secure digital signature scheme.

1.2 Contributions

This paper will propose a new scheme of *authenticated encryption* with publicly verifiable signature. The proposed scheme combines schemes of ElGamal encryption [5] with Schnorr signature [23]. Following the discussion on security of *authenticated encryption* in [24], the security of both signature and encryption are discussed. For signature the new scheme achieves *existentially unforgeable* under the adaptive chosen message attack; for encryption the new scheme achieves indistinguishable under the adaptive chosen ciphertext attack. Again, we give brief description about the security goal and attack model of signature scheme. The terminology *existentially unforgeable* originally defined in [25] is a common security goal of signature. This means that any adversary should have a negligible probability in forging a valid signature on a new message. The attack model is called adaptive chosen message if a signing oracle is available

to adversary while forging a signature. More information can be found in [4, 25-27].

So far the *authenticated encryption* schemes with publicly verifiable [12, 18-22] are unconditionally verifiable. Namely, once a matched plaintext is released from recipient, then everyone can verify whether the plaintext was sent and signed by the sender. It is also called "convertible authenticated encryption scheme" in [28]. In some applications, the recipient may only want to release the plaintext and do not release "publicly verifiable information" till a decisive moment. Our new scheme provides this favor without additional computation, *i.e*. the recipient can choose to release "only the corresponding plaintext" or "all the publicly verifiable information". Without enough information, every one except the recipient cannot recognize that some messages were a signature of the sender.

Furthermore, the proposed *authenticated encryption* is also secure against one-more-decryption attack [29]. Under this attack, an adversary tries to decrypt $(l + 1)$ plaintexts from given l ciphertexts ($l > 1$). In the applications of private information retrieval, a security guarantee against attack of this type would be desirable.

1.3 Organization

Section 2 introduces notation. Section 3 describes the proposed scheme and proves the correctness as well as security. Section 4 discusses the scheme's performance. Finally, Section 5 concludes the paper.

2. NOTATION

Let p and q be two large primes and q divide $(p - 1)$. The notation used in the paper is as follows. Z_q denotes the addition group modulo q; Z_p denotes the addition group modulo p; Z^*_p denotes the multiplicative group modulo p; g is an element of Z^*_p and we write $g \in Z^*_p$; a cyclic group $G \subset Z^*_p$ is generated by g (g is a generator of G), *i.e*. $G = \{g^i \bmod p | \ i = 0, 1, \ldots, (q - 1)\}$; $G' = G \setminus \{ p_1,\ldots, p_i\} = \{x | \ x \in G \text{ and } x \notin \{ p_1,\ldots, p_i\}\}$; use $|G|$ to denote the cardinality of G ($|G| = q$); $a \leftarrow_R G$ denotes that an element a is randomly and uniformly selected from G; $x \leftarrow y$ denotes that value of y is assigned to x. Assume that primes p, q and generator g have been chosen such

that finding the discrete logarithm in G is hard. Namely, given an attacker p, q, g, and an element $y \leftarrow_R G$, it is assumed that finding $x \in Z_q$ such that $y = g^x \bmod p$ is computationally intractable.

Also, $a||b$ denotes a concatenation of strings a and b; $f(.)$ is a one-way permutation function defined as $f(.)$: $G \rightarrow G$; $H(.)$ is a one-way collision-resistant hash function with domain $\{0, 1\}^*$ and range Z_q. Furthermore, we assume that the hash function $H(.)$ and permutation function $f(.)$ have been modeled as a random oracle [30].

3. PROPOSED SCHEME

A recipient randomly selects x_r from Z_q and computes $y_r = g^{x_r} \bmod p$, then publishes y_r as her/his public key and keeps x_r secretly as secret key. Similarly, x_s and $y_s = g^{x_s} \bmod p$ are sender's secret and public keys. A ciphertext of an authenticated encryption on a message $m \in G$ is obtained by computing $(c, e, s) = \textit{Authen-Enc}^{H(), f()}(x_s, m, y_r, y_s)$; the embedded plaintext is recovered and verified by $\{m \in G$, "invalid"$\} = \textit{Authen-Dec}^{H(), f()}(x_r, (c, e, s), y_r, y_s)$, where $H(.)$: $\{0, 1\}^* \rightarrow Z_q$ and $f(.)$:$G \rightarrow G$ as introduced in Section 2. The details of algorithms *Authen-Enc*(.) and *Authen-Dec*(.) are as follows.

Algorithm $\textit{Authen-Enc}^{H(), f()}(x_s, m, y_r, y_s)$

$k \leftarrow_R Z_q$
$Y_r \leftarrow (y_r)^k \bmod p$
$c \leftarrow m / f(Y_r) \bmod p$
$k' \leftarrow Y_r \bmod q$
$e \leftarrow H(c \,||\, m \,||\, y_r \,||\, y_s \,||\, (g^{k + k'} \bmod p))$
$s \leftarrow (k - e \cdot x_s) \bmod q$
Return ciphertext (c, e, s)

Algorithm $\textit{Authen-Dec}^{H(), f()}(x_r, (c, e, s), y_r, y_s)$

$Y'_r \leftarrow (g^s (y_s)^e)^{x_r} \bmod p$
$m' \leftarrow c \cdot f(Y'_r) \bmod p$
$k' \leftarrow Y'_r \bmod q$
$s' \leftarrow s + k' \bmod q$
$e' \leftarrow H(c \,||\, m' \,||\, y_r \,||\, y_s \,||\, (g^{s'} (y_s)^e \bmod p))$
If $e = e'$ then return m' else return 'invalid'

3.1 Correctness

Lemma 1. The algorithm *Authen-Dec*(.) correctly recovers the plaintext embedded in a ciphertext produced by algorithm *Authen-Enc*(.).

Proof. Upon receiving a ciphertext (c, e, s), the recipient runs algorithm *Authen-Dec*$^{H(),\ f()}(x_r, (c, e, s), y_r, y_s)$ to recover plaintext and verify signature. The quantities $(y_r)^k$ and k' are recovered by the computations $Y'_r = (g^s(y_s)^e)^{x_r} \bmod p$ and $k' = Y'_r \bmod q$. Then plaintext is obtained by computing $m' = c \cdot f(Y'_r) \bmod p$.

Now we want to recover the quantity $g^{k+k'}$. Indeed, $g^{s'}(y_s)^e = g^{s+k'}(y_s)^e = g^{k'}g^s(y_s)^e = g^{k'}g^{s+e x_s} = g^{k'+k} \bmod p$. Therefore the signature (e, s) on message ($c \parallel m' \parallel y_r \parallel y_s$) is correctly verified, and a success in verification indicates that the plaintext is correctly recovered. □

3.2 Security of Signature

The security of Schnorr signature scheme has received extensive discussion and has been proven to be *existentially unforgeable* under the adaptive chosen message attack [23, 26-27, 31]. Assume that an adversary $\mathcal{A}$ has maximum advantage $ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(\mathcal{A})$ while trying to forge a Schnorr signature under the attack model of adaptive chosen message. In the following lemma, we will prove that the signature scheme used in algorithm *Authen-Enc*(.) (let's call it *Sig-scheme*) is at least as secure as Schnorr signature scheme, *i.e*. the adversary $\mathcal{A}$ cannot have advantage of forging *Sig-scheme* signature more than $ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(\mathcal{A})$.

A ciphertext (c, e, s) is essential a signature of *Sig-scheme*, *i.e*. a signature on message $c \parallel m \parallel y_r \parallel y_s$, where $m = c \cdot f((g^s(y_s)^e)^{x_r}) \bmod p$, $k' = ((g^s(y_s)^e)^{x_r} \bmod p) \bmod q$, $e = H(c \parallel m \parallel y_r \parallel y_s \parallel (g^{k+k'} \bmod p))$, $s = (k - e \cdot x_s) \bmod q$. Namely, *Sig-scheme* is a variant of Schnorr signature with restricted verifiable information. Nobody except sender and recipient can verify this signature unless the recipient releases plaintext m and k'. Thus the result of the following lemma seems reasonable.

Lemma 2. The signature scheme *Sig-scheme* is at least as secure as Schnorr signature scheme.

Proof. In the following, we will include message in signature at our convenience. With the

knowledge of secret key x_r, recipient transforms a ciphertext (c, e, s) into a Schnorr signature. The details of transformation are as follows. Recipient runs the algorithm *Authen-Dec*(.) and obtains m', k'. Then a Schnorr signature (m'', e, s') is obtained. Namely, message $m'' = c \parallel m' \parallel y_r \parallel y_s$, commitment is $g^{k+k'} \bmod p$, response $s' = s + k'$, and challenge e is a hash value on concatenation of message m'' and commitment, *i.e.* $e = H(c \parallel m' \parallel y_r \parallel y_s \parallel (g^{k+k'} \bmod p))$.

Although a recipient is able to convert a signature of *Sig-scheme*, (c, e, s), into a Schnorr signature; the recipient cannot transform an ordinary Schnorr signature (m, e, s) into a *Sig-scheme* signature, (c', e', s'). An exception is that message $m = c' \parallel m' \parallel y_r \parallel y_s$ and $c' = m' / f((g^s(y_s)^e)^{x_r})$ mod p. Then (c', e, s') is a *Sig-scheme* signature, where $s' = (s - k') \bmod q$ and $k' = ((g^s(y_s)^e)^{x_r} \bmod p) \bmod q$. However, this situation will occur with negligible probability.

Let the quantity $ADV^{\mathrm{uf-cma}}_{\mathrm{Sig-scheme}}(\mathcal{A})$ be $\mathcal{A}$'s advantage of forging a *Sig-scheme* signature under adaptive chosen message attack model. We conclude that

$$ADV^{\mathrm{uf-cma}}_{\mathrm{Sig-scheme}}(\mathcal{A}) \leq ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(\mathcal{A}) \qquad (1)$$

or else the adversary can first forge a *Sig-scheme* signature and then transform it into a Schnorr signature. Therefore a Schnorr signature can be forged with a higher probability than $ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(\mathcal{A})$, this contradicts the assumption that $ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(\mathcal{A})$ is $\mathcal{A}$'s maximum advantage of forging a Schnorr signature. □

The insider security introduced in [24] is a stronger notion for the security of *authenticated encryption*. Assume that an adversary is given recipient's secret key and the adversary still cannot forge a signature with non-negligible probability. Then the signature scheme is secure against insider attack. We see that our *Sig-scheme* is secure against insider attack.

Benefiting by that a ciphertext is also a signature of *Sig-scheme*; the proposed *authenticated encryption* is also secure against one-more-decryption attack. In our scheme, a success in one-more-decryption attack implies that given l ciphertexts (signatures), an adversary can construct another ciphertext different from those l ciphertexts. It would be impossible for an adversary (include recipient) to do that, since the security of *Sig-scheme* is strong enough to resist

this attack, by Lemma 2.

3.3 Security of Encryption

In the following, we will use the technique of sequences games described in [32] to prove the security goal of encryption. Our proof consists of six games, $Game_0$, $Game_1$, …, $Game_5$. $Game_0$ demonstrates the definition of security goal and attack model. Namely, a challenger who honestly runs the algorithm specified in $Game_0$ and an adversary trying to break the algorithm in the sense of definition. $Game_i$ evolves from $Game_{i-1}$ with a small change. Finally, we achieve a final game, $Game_5$. Assume that the differences between games and the success probability of adversary in final game can be calculated efficiently. Then we can compute the adversary's probability of successful experiment in $Game_0$, namely, in the original definition.

During an attack game, we assume that the adversary (denoted by $\mathcal{A}(.)$) called encryption oracle q_e times and decryption oracle q_d times. Let ψ denote ciphertext (c, e, s) and Q_j denote the number of encryption queries made prior to the jth decryption query. It is evident that $0 \le Q_j \le q_e$.

3.3.1 Definition of security goal and attack model

***Game*$_0$:**

$x_s \leftarrow_R Z_q$, $x_r \leftarrow_R Z_q$, $y_s \leftarrow g^{x_s} \bmod p$, $y_r \leftarrow g^{x_r} \bmod p$, $b \leftarrow_R \{0, 1\}$

Upon the ith encryption query:

$(m_{i0}, m_{i1}) \leftarrow \mathcal{A}(y_s, y_r, \psi_1, ..., \psi_{i-1})$ // $m_{i0}, m_{i1} \in G$, ciphertext $\psi = (c, e, s)$

$k_i \leftarrow_R Z_q$, $Y_{ri} \leftarrow (y_r)^{k_i} \bmod p$, $c_i \leftarrow m_{ib} / f(Y_{ri}) \bmod p$, $k'_i \leftarrow Y_{ri} \bmod q$

$e_i \leftarrow H(c_i \| m_{ib} \| y_r \| y_s \| (g^{k_i + k'_i} \bmod p))$, $s_i \leftarrow (k_i - e_i \cdot x_s) \bmod q$, $\psi_i \leftarrow (c_i, e_i, s_i)$

Return ψ_i to $\mathcal{A}(.)$ as the answer

Upon the jth decryption query (ψ'_j denotes the jth ciphertext (c'_j, e'_j, s'_j)):

$Y'_{rj} \leftarrow (g^{s'_j}(y_s)^{e'_j})^{x_r} \bmod p$, $m'_j \leftarrow c'_j \cdot f(Y'_{rj}) \bmod p$, $k'_j \leftarrow Y'_{rj} \bmod q$

$s''_j \leftarrow s'_j + k'_j \bmod q$, $e''_j \leftarrow H(c'_j \| m'_j \| y_r \| y_s \| (g^{s''_j}(y_s)^{e'_j} \bmod p))$

// $\psi'_j \notin \{\psi_a \mid a = 1, \ldots, Q_j\}$

If $e''_j = e'_j$ then return m'_j else return "invalid"

$b' \leftarrow \mathcal{A}(\psi_1, ..., \psi_{q_e}, m'_1, ..., m'_{q_d}) \in \{0, 1\}$

It is clearly that $Game_0$ describes the attack model of adaptive chosen ciphertext (CCA2) [15]. The adversary freely selects two plaintexts (m_{i0}, m_{i1}) and hands on them to challenger. According to the value of a pre-selected random bit b, challenger enciphers either m_{i0} or m_{i1}. Then challenger returns the resultant ciphertext to the adversary and asks him/her what value the random bit b is. While selecting plaintexts, adversary has knowledge of public information and some ciphertexts generated previously, *i.e*, $\psi_1, ..., \psi_{i-1}$. Also, the adversary can query decryption oracle to decrypt some ciphertexts ψ'_j that $\psi'_j \notin \{ \psi_a \mid a = 1, \ldots, Q_j \}$.

Let S_0 define the event that $b = b'$ in $Game_0$. If the adversary simply tosses a fair coin to decide random bit b', then the probability of event S_0 will be $1 / 2$, *i.e*. $\Pr[S_0] = 1 / 2$. Since the adversary has been equipped with some capabilities to guess random bit b', $\Pr[S_0]$ my be higher than $1 / 2$. Thus it is straightforward to define

$$ADV^{CCA2}_{Authen-Enc} = (\Pr[S_0] - 1 / 2); \qquad (2)$$

namely, the advantage that an adversary can have while trying to distinguish between encryption of two plaintexts of his/her choosing.

Now we try to compute the quantity of $ADV^{CCA2}_{Authen-Enc}$ using the following games and differences (transitions) between games.

3.3.2 A change in decryption oracle

***Game$_1$*:**

$x_s \leftarrow_R Z_q$, $x_r \leftarrow_R Z_q$, $y_s \leftarrow g^{x_s} \bmod p$, $y_r \leftarrow g^{x_r} \bmod p$, $b \leftarrow_R \{0, 1\}$

Upon the ith encryption query:

$(m_{i0}, m_{i1}) \leftarrow \mathcal{A}(y_s, y_r, \psi_1, ..., \psi_{i-1})$

$k_i \leftarrow_R Z_q$, $Y_{ri} \leftarrow (y_r)^{k_i} \bmod p$, $c_i \leftarrow m_{ib} / f(Y_{ri}) \bmod p$, $k'_i \leftarrow Y_{ri} \bmod q$

$e_i \leftarrow H(c_i \,||\, m_{ib} \,||\, y_r \,||\, y_s \,||\, (g^{k_i + k'_i} \bmod p))$, $s_i \leftarrow (k_i - e_i \cdot x_s) \bmod q$, $\psi_i \leftarrow (c_i, e_i, s_i)$

Return ψ_i to $\mathcal{A}(.)$ as the answer

Upon the jth decryption query (ψ'_j denotes the jth ciphertext (c'_j, e'_j, s'_j)):

Return "invalid" as the answer // $\psi'_j \notin \{ \psi_a \mid a = 1, \ldots, Q_j \}$

$b' \leftarrow \mathcal{A}(\psi_1, ..., \psi_{q_e}, m'_1, ..., m'_{q_d}) \in \{0, 1\}$

Note that in *Game*$_1$, the decryption oracle always returns "invalid" to the adversary in response to his/her decryption queries. Let S_1 define the event that $b = b'$ in *Game*$_1$. Also F defines the event in *Game*$_1$ that for some $j = 1, \ldots, q_d$, the adversary queried decryption oracle with a ciphertext (c'_j, e'_j, s'_j), and the ciphertext is such that $Y'_{rj} \leftarrow (g^{s'_j}(y_s)^{e'_j})^{x_r} \bmod p$, $m'_j \leftarrow c'_j \cdot f(Y'_{rj}) \bmod p$, $k'_j \leftarrow Y'_{rj} \bmod q$, $s''_j \leftarrow s'_j + k'_j \bmod q$, $e''_j \leftarrow H(c'_j \| m'_j \| y_r \| y_s \| (g^{s''_j}(y_s)^{e'_j} \bmod p))$ and $e'_j = e''_j$. It is clear that *Game*$_0$ and *Game*$_1$ will proceed identically unless event F occurs. Essentially, the event F implies that the adversary has successfully forged a signature of *Sig-scheme*. By Lemma 2 in Section 3.2, event F occurs with probability less than $q_d \cdot ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(.)$, *i.e.*

$$\Pr[F] \le q_d \cdot ADV^{\mathrm{uf-cma}}_{\mathrm{Sig-scheme}}(.) \le q_d \cdot ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(.). \qquad (3)$$

The Difference Lemma in [32] describes the relationship between events S_0, S_1, and F. It states that $|\Pr[S_0] - \Pr[S_1]| \le \Pr[F]$. Therefore the following inequality is obtained.

$$|\Pr[S_0] - \Pr[S_1]| \le q_d \cdot ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(.) \qquad (4)$$

3.3.3 Permutation function f(.) is replaced by a truly random faithful permutation function

***Game*$_2$:**

$x_s \leftarrow_R Z_q$, $x_r \leftarrow_R Z_q$, $y_s \leftarrow g^{x_s} \bmod p$, $y_r \leftarrow g^{x_r} \bmod p$, $b \leftarrow_R \{0, 1\}$

Upon the ith encryption query:

$(m_{i0}, m_{i1}) \leftarrow \mathcal{A}(y_s, y_r, \psi_1, ..., \psi_{i-1})$

$k_i \leftarrow_R Z_q$, $Y_{ri} \leftarrow (y_r)^{k_i} \bmod p$, $k'_i \leftarrow Y_{ri} \bmod q$

$P_i \leftarrow_R G$

If ($P_i \in \{ p_1, \ldots, p_{i-1} \}$) then $P_i \leftarrow_R G \setminus \{ p_1, \ldots, p_{i-1} \}$

$p_i \leftarrow P_i$

$c_i \leftarrow m_{ib} / p_i \bmod p$

$e_i \leftarrow H(c_i \| m_{ib} \| y_r \| y_s \| (g^{k_i + k'_i} \bmod p))$, $s_i \leftarrow (k_i - e_i \cdot x_s) \bmod q$, $\psi_i \leftarrow (c_i, e_i, s_i)$

Return ψ_i to $\mathcal{A}(.)$ as the answer

Upon the jth decryption query:

Return "invalid" as the answer

$b' \leftarrow \mathcal{A}(\psi_1, ..., \psi_{q_e}, m'_1, ..., m'_{q_d}) \in \{0, 1\}$

Note that in *Game*$_2$, the permutation function $f(.)$ is replaced by a truly random faithful permutation function. Then the difference between *Game*$_1$ and *Game*$_2$ is simply the difference between the permutation function $f(.)$ and a truly random faithful permutation function, more information about random permutation and pseudo random permutation functions please refer to [4, 32]. Let $ADV^{\text{prp}}_{f(.)}(.)$ be this difference and S_2 the event that $b = b'$ in *Game*$_2$. Then we have

$$| \Pr[S_1] - \Pr[S_2] | \leq ADV^{\text{prp}}_{f(.)}(.). \qquad (5)$$

3.3.4 The truly random faithful permutation function is replaced by a truly random forgetful permutation function

***Game*$_3$:**

$x_s \leftarrow_R Z_q$, $x_r \leftarrow_R Z_q$, $y_s \leftarrow g^{x_s} \bmod p$, $y_r \leftarrow g^{x_r} \bmod p$, $b \leftarrow_R \{0, 1\}$

Upon the ith encryption query:

$(m_{i0}, m_{i1}) \leftarrow \mathcal{A}(y_s, y_r, \psi_1, ..., \psi_{i-1})$

$k_i \leftarrow_R Z_q$, $Y_{ri} \leftarrow (y_r)^{k_i} \bmod p$, $k'_i \leftarrow Y_{ri} \bmod q$

$P_i \leftarrow_R G$, $p_i \leftarrow P_i$

$c_i \leftarrow m_{ib} / p_i \bmod p$

$e_i \leftarrow H(c_i \| m_{ib} \| y_r \| y_s \| (g^{k_i + k'_i} \bmod p))$, $s_i \leftarrow (k_i - e_i \cdot x_s) \bmod q$, $\psi_i \leftarrow (c_i, e_i, s_i)$

Return ψ_i to $\mathcal{A}(.)$ as the answer

Upon the jth decryption query:

Return "invalid" as the answer

$b' \leftarrow \mathcal{A}(\psi_1, ..., \psi_{q_e}, m'_1, ..., m'_{q_d}) \in \{0, 1\}$

Note that in $Game_3$, the truly random faithful permutation function is replaced by a truly random forgetful permutation function. There will be no difference between $Game_2$ and $Game_3$ except that collision occurs when choosing random numbers P_i. Let $Collision_3$ denote this event and S_3 be the event that $b = b'$. Then

$$\Pr[Collision_3] \leq \frac{1}{|G|} + \frac{2}{|G|} + \ldots + \frac{q_e}{|G|} = \frac{q_e(q_e - 1)}{2|G|} \leq \frac{(q_e)^2}{2|G|}. \quad (6)$$

It is clear that $Game_2$ and $Game_3$ will proceed identically unless event $Collision_3$ occurs. Thus by Difference Lemma, we have

$$|\Pr[S_2] - \Pr[S_3]| \leq \Pr[Collision_3] \leq \frac{(q_e)^2}{2|G|}. \quad (7)$$

3.3.5 Hash function $H(.)$ is replaced by a truly faithfully random function

***Game*$_4$:**

$x_s \leftarrow_R Z_q$, $x_r \leftarrow_R Z_q$, $y_s \leftarrow g^{x_s} \bmod p$, $y_r \leftarrow g^{x_r} \bmod p$, $b \leftarrow_R \{0, 1\}$

Upon the ith encryption query:

$(m_{i0}, m_{i1}) \leftarrow \mathcal{A}(y_s, y_r, \psi_1, ..., \psi_{i-1})$

$k_i \leftarrow_R Z_q$, $Y_{ri} \leftarrow (y_r)^{k_i} \bmod p$, $k'_i \leftarrow Y_{ri} \bmod q$

$P_i \leftarrow_R G$, $p_i \leftarrow P_i$

$c_i \leftarrow m_{ib} / p_i \bmod p$

$e_i \leftarrow_R Z_q$, $s_i \leftarrow_R Z_q$, $Y_i \leftarrow g^{s_i} (y_s)^{e_i} \bmod p$ // now e_i and s_i are random

If $(c_i \| m_{ib} \| y_r \| y_s \| Y_i = c_j \| m_{jb} \| y_r \| y_s \| Y_j)$ for some $j < i$

Then $e_i \leftarrow e_j$, $s_i \leftarrow s_j$, $k'_i \leftarrow k'_j$

Else the hash value of $H(c_i \| m_{ib} \| y_r \| y_s \| Y_i)$ is e_i

$\psi_i \leftarrow (c_i, e_i, (s_i - k'_i) \bmod q)$

Return ψ_i to $\mathcal{A}(.)$ as the answer

Upon the jth decryption query:

Return "invalid" as the answer

$b' \leftarrow \mathcal{A}(\psi_1, ..., \psi_{q_e}, m'_1, ..., m'_{q_d}) \in \{0, 1\}$

Note that in $Game_4$, the hash function $H(.)$ is replaced by a truly faithfully random function. Then the difference between $Game_3$ and $Game_4$ is just the difference between the hash function $H(.)$ and a truly faithfully random function, more information about random and pseudo random functions please refer to [4, 32]. Let $ADV^{prf}_{H(.)}(.)$ be this difference and S_4 the event that $b = b'$ in $Game_4$. Then we have

$$| \Pr[S_3] - \Pr[S_4] | \leq ADV^{prf}_{H(.)}(.). \qquad (8)$$

3.3.6 The truly faithfully random function is replaced by a truly forgetfully random function

***Game*$_5$:**

$x_s \leftarrow_R Z_q$, $x_r \leftarrow_R Z_q$, $y_s \leftarrow g^{x_s} \bmod p$, $y_r \leftarrow g^{x_r} \bmod p$, $b \leftarrow_R \{0, 1\}$

Upon the ith encryption query:

$(m_{i0}, m_{i1}) \leftarrow \mathcal{A}(y_s, y_r, \psi_1, ..., \psi_{i-1})$

$k_i \leftarrow_R Z_q$, $Y_{ri} \leftarrow (y_r)^{k_i} \bmod p$, $k'_i \leftarrow Y_{ri} \bmod q$

$P_i \leftarrow_R G$, $p_i \leftarrow P_i$

$c_i \leftarrow m_{ib} / p_i \bmod p$

$e_i \leftarrow_R Z_q$, $s_i \leftarrow_R Z_q$, $Y_i \leftarrow g^{s_i} (y_s)^{e_i} \bmod p$ // now e_i and s_i are random

Set the hash value of $H(c_i \| m_{ib} \| y_r \| y_s \| Y_i)$ to e_i

$\psi_i \leftarrow (c_i, e_i, (s_i - k'_i) \bmod q)$

Return ψ_i to $\mathcal{A}(.)$ as the answer

Upon the jth decryption query:

Return “invalid” as the answer

$b' \leftarrow \mathcal{A}(\psi_1, ..., \psi_{q_e}, m'_1, ..., m'_{q_d}) \in \{0, 1\}$

Note that in *Game*$_5$, the truly faithfully random function is replaced by a truly forgetfully random function. Let *Collision*$_5$ denote the event that ($c_i \| m_{ib} \| y_r \| y_s \| Y_i = c_j \| m_{jb} \| y_r \| y_s \| Y_j$) for some $j \neq i$. We observe that the adversary may choose m_{ib} from a small subset of group G, *i.e.* $m_{ib} = m_{jb}$ for all $i \neq j$. Thus *Collision*$_5$ is expressed by a simpler equation, ($c_i \| Y_i = c_j \| Y_j$) for some $j \neq i$, namely the sampling space is extended to the Cartesian product of G. The probability of collision is as follows.

$$\Pr[Collision_5] \leq \frac{(q_e)^2}{2|G \times G|} \qquad (9)$$

It is clear that *Game*$_4$ and *Game*$_5$ proceed identically unless *Collision*$_5$ occurs. Let S_5 denote the event that $b = b'$ in *Game*$_5$. Thus we have

$$|\Pr[S_4] - \Pr[S_5]| \leq \Pr[Collision_5] \leq \frac{(q_e)^2}{2|G \times G|}. \qquad (10)$$

Also that $\Pr[S_5] = 1 / 2$. Therefore, combining equations (4), (5), (7), (8), and (10), the proposed scheme’s semantic security is as follows.

$|\Pr[S_0] - 1 / 2|$

$= |\Pr[S_0] - \Pr[S_5]|$

$= |\Pr[S_0] - \Pr[S_1] + \Pr[S_1] - \Pr[S_2] + \Pr[S_2] - \Pr[S_3] + \Pr[S_3] - \Pr[S_4] + \Pr[S_4] - \Pr[S_5]|$

$$\leq q_d \cdot ADV^{\mathrm{uf-cma}}_{\mathrm{Schnorr-sig}}(.) + ADV^{\mathrm{prp}}_{f(.)}(.) + \frac{(q_e)^2}{2|G|} + ADV^{\mathrm{prf}}_{H(.)}(.) + \frac{(q_e)^2}{2|G \times G|} \qquad (11)$$

4. PERFORMANCE

To simplify the estimation of computational cost, we count only the major operation. For example, the computational cost of modular multiplication, hash function, and permutation function is ignored as compared with the expensive cost of modular exponentiation.

The computational cost for encryption is two modular exponentiations. Using the technique of efficient simultaneous multiple exponentiations [2], the computational cost for decryption is *2.34* modular exponentiations.

For a practical cryptosystem, the parameters $|p| = 1024$, $|H(.)| = 160$, and $|q| = 160$ were suggested in [33]. Since a plaintext has bit length *1024* and a ciphertext consists of *1344* ($|p| + |H(.)| + |q|$) bits, therefore the data expansion rate is about *1.3*.

For both the computational cost and data expansion rate, the presented scheme is as efficient as that of those schemes in [18-19, 21].

5. CONCLUSION

This paper has presented a secure authenticated encryption scheme. In the aspect of signature, it is shown at least as secure as the Schnorr signature scheme which we have included in the proposed scheme. It is possible to integrate with other signature scheme, *e.g*. DSA signature scheme. Depending on the amount of information released by recipient, a signature is either publicly verifiable or not.

As for the encryption, it is secure against one-more-decryption attack. Also, the adversary's advantage in guessing random bit *b* is directly related to the advantage of forging a signature as shown in equation (11).

As discussed in Section 3.2, the proposed scheme's signature is secure against insider attack. But encryption is not. If an adversary has the knowledge of sender's secret key, then recipient's *privacy* is lost. It would be a challenge to construct an *authenticated encryption* to prevent both signature and encryption from insider attack.

REFERENCES

1. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, pp. 644-654, 1976.

2. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, New York,

London, Tokyo, CRC Press, 1996.

3. H. Delfs and H. Knebl, *Introduction to Cryptography-Principles and Applications*, New York, Hong Kong, Springer-Verlag, 2002.

4. M. Bellare, *Course note: Introduction to Modern Cryptography*, http://www-cse.ucsd.edu/users/mihir/, Chapter 11, 2004.

5. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, pp. 469-472, 1985.

6. K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," *Proceedings of the 1st ACM Conference on Computer and Communications Security CCS'93*, ACM press, pp. 58-61, 1993.

7. K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Advances in Cryptology- EUROCRYPT'94*, LNCS 950, pp. 182-193, 1994.

8. P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs", *Electronics Letters*, Vol. 30, No. 15, pp. 1212-1213, 1994.

9. Y. Zheng, "Digital signcryption or how to achieve cost (signature and encryption) << cost (signature) + cost (encryption)", *Advances in Cryptology- CRYPTO'97*, LNCS 1294, pp. 165-179, 1997.

10. M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: current status and key issues," *International Journal of Network Security*, Vol. 1, N0. 2, pp. 54-66, 2005. (http://isrc.nchu.edu.tw/ijns/).

11. Y. M. Tseng and J. K. Jan, "An efficient authenticated encryption scheme with message linkages and low communication costs," *Journal of Information Science and Engineering*, Vol. 18, pp. 41-46, 2002.

12. Y. Q. Peng, S. Y. Xie, Y. F. Chen, R. Deng, and L. X. Peng, "A publicly verifiable authenticated encryption scheme with message linkages," *Networking and Mobile Computing:*

3rd International Conference ICCNMC 2005, LNCS 3619, pp. 1271-1276, 2005.

13. E. J. Yoon and K. Y. Yoo, "Robust authenticated encryption scheme with message linkages," *Information and Engineering System KES 2005*, LNAI 3684, pp. 281-288, 2005.

14. S. Goldwasser and S. Micali, "Probabilistic encryption", *Journal of Computer and System Sciences*, Vol. 28, pp. 270-299, 1984.

15. M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, "Relations among notions of security for public-key encryption schemes," *Advances in Cryptology- CRYPTO'98*, LNCS 1462, pp. 26-46, 1998.

16. J. Baek, R. Steinfeld and Y. Zheng, "Formal proofs for the security of signcryption," *Proceedings of Public Key Cryptography 2002*, LNCS 2274, pp. 80-98, 2002.

17. H. Petersen and M. Michels "Cryptanalysis and improvement of signcryption schemes", *IEE Proc-Computers and Digital Techniques*, Vol. 145, (2), pp. 149-151, 1998.

18. F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," *Proceedings of Public Key Cryptography 1998*, LNCS 1431, pp. 55-59, 1998.

19. D. Yum and P. Lee, "New signcryption schemes based on KCDSA," *The 4th International Conference on Information security and Cryptology*, LNCS 2288, pp. 341-354, 2001.

20. G. Wang, F. Bao, C. Ma, and K. Chen, "Efficient authenticated encryption schemes with public verifiability," *IEEE VTC2004 -- Vehicular Technology Conference*, Vol. 5, pp. 3258-3261, 2004.

21. J. B. Shin, K. Lee and K. Shim, "New DSA-Verifiable signcryption schemes," *The 6th International Conference on Information security and Cryptology*, LNCS 2587, pp. 35-47, 2003.

22. B. Libert and J. J. Quisquater, "Efficient signcryption with key privacy from Gap Diffie-Hellman Groups," *Proceedings of Public Key Cryptography 2004*, LNCS 2947, pp. 187-200, 2004.

23. C. P. Schnorr, ”Efficient signature generation by smart cards”, *Journal of Cryptology*, Vol. 4, pp. 161-174, 1991.

24. J. H. An, Y. Dodis and T. Rabin, “On the security joint signature and encryption,” *Advances in Cryptology-EUROCRYPT 2002*, LNCS 2332, pp. 83-107, 2002.

25. S. Goldwasser, S. Micali, and R. Rivest, “A digital signature scheme secure against adaptive chosen-message attacks”, *SIAM J. Computing*, Vol. 17, No. 2, pp. 281-308, 1988.

26. D. Pointcheval and J. Stern, “Security proofs for signature schemes”, *Advances in Cryptology-EUROCRYPT’96*, LNCS 1070, pp. 387-398, 1996.

27. D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures”, *Journal of Cryptology*, Vol. 13, N0. 3, pp. 361-396, 2000.

28. T. S. Wu and S. L. Hsu, “Convertible authenticated encryption scheme,” *The journal of Systems and Software*, Vol. 39, No. 3, pp. 281-282, 2002.

29. C. P. Schnorr and M. Jakobsson, ”Security of signed ElGamal encryption”, *Advances in Cryptology-ASIACRYPT 2000*, LNCS 1976, pp. 73-89, 2000.

30. M. Bellare and P. Rogaway, “Random oracles are practical: a paradigm for designing efficient protocols”, *Proc. of the 1st ACM Conference on Computer and Communications Security CCS’93*, ACM press, pp. 62-73, 1993.

31. K. Ohta and T. Okamoto, “On the concrete security treatment of signatures derived from identification,” *Advances in Cryptology- CRYPTO’98*, LNCS 1462, pp. 354-369, 1998.

32. V. Shoup, “Sequences of games: A tool for taming complexity in security proofs,” http://eprint.iacr.org/2004/332, May 27, 2005.

33. A. Lenstra and E. Verheul, “Selecting cryptographic key sizes”, *The Third International Workshop on Practice and Theory in Public Key Cryptography (PKC2000)*, LNCS 1751, pp. 446-465, 2000.