A Verifiably Encrypted Signature Scheme with Strong Unforgeability

Jianhong Zhang
College of sciences North China University of Technology
Shijingshan District, Beijing, China
State Key Laboratory of Information Security,
Institute of Software of Chinese Academy of Sciences, Beijing, 100039, China
jhzhangs@163.com

ABSTRACT

A verifiably encrypted signature can convince the verifier that a given cipher-text is the encryption of a signature on a given message. It is often used as a building block to construct optimistic fair exchange. In this paper, first we define a stronger unforgeable model, then give a variant of Cha-Cheon's signature [8] and construct a verifiably encrypted signature based on this variant scheme. Finally, the scheme is proven to secure in random oracle model. In comparison with Gu *et.al*'s verifiably encrypted signature scheme, our scheme is more efficient with respect to the size of signature and computation cost of signature.

Categories and Subject Descriptors

E.3 [**DATA ENCRYPTION**]: Public key cryptosystems

General Terms

Security

Keywords

Verifiably encryption, proof, security analysis

1. INTRODUCTION

With Internet rapidly developing, electronic commerce plays an important role in business transactions and is conducting business communications over networks and through computer. It usually involves two distrusted parties exchanging items with each other, for instance a payment via an electronic check for a digital CD over the Internet. When a commercial transaction is conduced in such distributed environments, it is difficult to assess the counter-party's trustworthiness. An urgent problem to be solved is how to realize fair exchange. Fair exchange is the problem of exchanging data in a way that guarantees that either all participants obtain what they want, or none do [9].

Infoscale 2007 June 6-8, 2007, Suzhou, China

A verifiably encrypted signature, which was proposed by N.Asokan [9], provides a way to encrypt a signature under a designated public key and subsequently prove that the resulting ciphertext indeed contains such a signature. Verifiably encrypted signatures are used in application such as online contract signing[9][4]. Suppose Alice wants to show Bob that she has signed a message, but does not want Bob to possess her signature of that message.(Alice will give her signature to Bob only when a certain event has occurred, e.g., Bob has given Alice his signature on the same message.) Alice can achieve his by encrypting her signature using the public key of a trusted third party, and sending this to Bob along with a proof that she has given him a valid encryption of her signature. Bob can verify that Alice has signed the message, but cannot deduce any information of her signature. If Alice is unable or unwilling to reveal her signature, Bob can ask the third party to reveal Alice's signature.

Since the concept of VES was included,J.Camenish [7] and G.Ateniese [4] proposed a verifiable encryption signature based on the discrete logarithm problem, respectively. In 2003, Boheh *et.al* [1] and Zhang *et.al*[3] proposed a verifiably encryption signature with security proofs in random oracle based on bilinear Pairings, respectively. In ICDCIT 2005, M.Choudary Gorantla *et.al*[5] proposed a novel verifiably encrypted signature without random oracle. Recently, by combining ID-based public key cryptography with verifiably encrypted signature, Gu *et.al* [2] proposed a ID-based verifiably encrypted signature scheme based on Hess' signature scheme [6](Gu *et.al* scheme for short), and claimed that their scheme was secure in random oracle model. Unfortunately, Gu et.al scheme is universal forgeable. Namely, any one can forge a verifiably encrypted signature on arbitrary a message. In this work, we propose a novel secure ID-based verifiably encrypted signature scheme, and show the scheme is proven secure in random oracle model. In comparison with Gu *et.al*'s verifiably encrypted signature scheme, our scheme is more efficient with respect to the size of signature and computation cost of signature.

The rest of the paper is organized as follows. In section 2, we review some preliminaries requirement throughout the paper. In section 3, we first give a variant of Cha-Cheon signature scheme, then propose a novel verifiably encrypted scheme based on the variant. In section 4, we analyze the security of our scheme and show that it is secure in random oracle model. Finally, we draw this paper.

2. PRELIMINARIES

In the section, we first briefly describe bilinear Parings and some related mathematical problems, which form the basis of security for our scheme.

Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of order q. Let $e : G_1 \times G_1 \to G_2$ be a map which the following properties[1,2,8,9].

- Bilinear: $\forall P, Q \in G_1$, and $a, b \in Z_q$, $e(aP, bP) = e(P, P)^{ab}$
- Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$,in other words, the map doesn't send all pair in $G_1 \times G_1$ to the identity in G_2.
- Computable: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

Such a bilinear map is called an admissible bilinear pairing. The Weil Parings and Tate Pairings of elliptic curves are able to construct an efficient admissible pairings.

The security of our proposed scheme is related to the computational Diffie-Hellman problem (CDHP), which is given below.

Definition1: (Computational Diffie-Hellman Problem) Let a, b be chosen from Z_q at random and P be chosen from G_1 at random. Given (P, aP, bP), compute $abP \in G_1$.
The success probability of any probabilistic polynomial-time $\mathcal{A}$ in solving CDH problem in G_1 is defined to be

$$Succ^{CDH}_{\mathcal{A},G_1} = Pr[\mathcal{A}(P, aP, bP) = abP : a, b \in Z_p]$$

The CDH assumption states that for every probabilistic polynomial-time algorithm $\mathcal{A}$, $Succ^{CDH}_{\mathcal{A},G_1}$ is negligible.

Definition 2: A verifiably encrypted signature scheme consists of the following algorithms: KeyGen, Sign, Verify, AdjKenGen, VESig Generate, VESig Verify and Adjudicate. The algorithms are described below.

- **Key Generation, Signing, Verification**. As in standard signature schemes.
- **Adjudicator Key**. Generate a public-private key pair (Q_A, s_A) for the adjudicator.
- **VESig Generation**. Give a private key D, a message M, and an adjudicator's Q_A, compute a verifiably encrypted signature δ on M.
- **VESig Verification**. Given a public key Q, a message M, an adjudicator's public key Q_A and a verifiably encrypted signature δ, verify that δ is a valid verifiably encrypted signature on M under public key Q.
- **Adjudication**. Given an adjudicator's key pairs (Q_A, s_A), a public key Q, and a verifiably encrypted signature δ on some message M, extract and output δ_1, an ordinary signature on M under public key Q.

A secure verifiably encrypted signature scheme should satisfy the following properties;

- Strong Unfogeability: It is difficult to forge a valid verifiably encrypted signature in polynomial time.The advantage in existentially forging a verifiably encrypted signature of an algorithm F, given access to a verifiably-encrypted-signature creation oracle S and an adjudication oracle A, along with a hash oracle, is

$$AdVSF_f \stackrel{\text{def}}{=} Pr\left[\begin{array}{c} VESigVerify(PK, APK, M, w) = 1 \\ (PK, SK) \stackrel{\text{R}}{\leftarrow} KeyGen, \\ (APK, ASK) \stackrel{\text{R}}{\leftarrow} AdjKeyGen, \\ (M, w) \stackrel{\text{R}}{\leftarrow} F_{S,A}(PK, APK) \end{array}\right]$$

The probability is taken over the coin tosses of the key-generation algorithms, of the oracles, and of the forger. The forger is additionally limited in where its forgery on (M, w) is not among the message-signature pairs generated during the previous query phase.

Strong unforgeability ensures the adversary cannot even produce a new signature for a previously signed message. In other words, suppose an adversary obtains a message-signature (M, w) along with other message-signature pairs of his choice. The signature system is strongly unforgeable if the adversary cannot produce a new signature $\tilde{w}$ on M.

- Opacity: Given a verifiably encrypted signature, it is difficult to extract the ordinary signature on the same message from the verifiably encrypted signature time without the help of the **Adjudicator**. The advantage in extracting a verifiably encrypted signature of an algorithm ε , given access to a verifiably-encrypted-signature creation oracle S and an adjudication oracle A, along with a hash oracle, is

$$AdvVSF_\varepsilon \stackrel{\text{def}}{=} Pr\left[\begin{array}{c} Verify(PK, M, \sigma) = valid \\ (PK, SK) \stackrel{\text{R}}{\leftarrow} KeyGen, \\ (APK, ASK) \stackrel{\text{R}}{\leftarrow} AdjKeyGen, \\ (M, \sigma) \stackrel{\text{R}}{\leftarrow} \varepsilon_{S,A}(PK, APK) \end{array}\right]$$

The probability is taken over the coin tosses of the key-generation algorithms, of the oracles, and of the forger. The extraction must be nontrivial: the adversary must not have queried the adjudication oracle A at M.

3. OUR PROPOSED SCHEME

In the section, we will propose a novel ID-based verifiably encryption signature scheme. We assume that $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of order q, P be a generator of G_1, $e : G_1 \times G_1 \longrightarrow G_2$ be an admissible bilinear pairing. The detail procedure is as follows:

3.1 Setup

Given (G_1, G_2, q, e, P), randomly choose a number $s \in Z^*_q$ and set $P_{pub} = sP$. The adjudicator randomly chooses a s_A as his private key and compute his public key $Q_A = s_A P$. Then choose two hash functions $H_1 : \{0,1\}^* \longrightarrow G^*_1$ and $H_2 : \{0,1\}^* \longrightarrow Z^*_q$. The system parameters $\Omega = (G_1, G_2, q, e, P, P_{pub}, H_1, H_2)$. The master key is s, the private key of adjudicator is S_A.

3.2 Extract:

Given an identity $ID_X \in \{0,1\}^*$ of a user, compute $Q_X = H_1(ID_X) \in G_1$,$D_X = sQ_X$. PKG uses this algorithm to extract the user's private key D_X, and gives D_X to the user by a secure channel.

3.3 Sign phase (variant of Cha-Cheon signature Scheme)

Given a private key D_X of a user and message m, pick $r, r_2 \in Z_q^*$ at random, and compute

$$\begin{aligned} U &= rQ_{ID_X}, U_2 = r_2 P \\ h &= H_2(m||U_2, U) \\ V &= (r+h)D_X \end{aligned}$$

then, (U, U_2, V) is the signature on the message m, where the above notion $||$ denotes concatenation the messages. Obviously, the signature is a variant of Cha-Cheon's signature which is proven to be secure under random oracle model. In essence, the above signature is a Cha-Cheon signature on the message $m||U_2$. Thus, the our proposed variant of Cha-Cheon signature scheme is equivalent to the Cha-Cheon signature scheme and also secure under the random oracle model.

3.4 Verify phase:

Given a signature (U, U_2, V) of an identity ID_X for a message m, compute $h = H_2(m||U_2, V)$ and accept the signature if and only if

$$e(P, V) = e(P_{Pub}, U + hQ_{ID_X})$$

3.5 VE-Sign

Given a secret key D_X, a message $m \in \{0,1\}^*$ and an adjudicator's public key Q_A. He computes as follows:

- compute $W = V + r_2 Q_A$.
- output the verifiably encrypted signature (U, W, U_2) on the message m.

3.6 VE-Verify

Given a verifiable encrypted signature (W, U, U_2) of a message m, a verifier first computes $h = H_2(m||U_2, U))$, and accepts the signature if and only if

$$e(P, W) = e(P_{Pub}, U + hQ_{ID_X}) e(U_2, Q_A)$$

3.7 Adjudication:

Given a verifiably encrypted signature (W, U, U_2) on a message m, the adjudicator can extract as follows: he computes $V' = W - s_A U_2$. Then (U, V', U_2) is the extracted signature on the message m.

4. ANALYSIS

In this section, we first justify the validity of the scheme and subsequently the security of the scheme.

4.1 Correction

The correctness of our proposed VES(Verifiably Encryption Signature) verification equation is justified as follows:

$$\begin{aligned} e(P, W) &= e(P, V + r_2 Q_A) \\ &= e(P, (r+h)D_X) \cdot e(r_2 P, Q_A) \\ &= e(P_{Pub}, U + hQ_{ID_X}) \cdot e(U_2, Q_A) \end{aligned}$$

The above equality implies the verification of Verifiably Encryption Signature (U_2, r, V) is true. The verification of the signature extracted from the given VES (U_2, r, V) in the adjudication phase holds as shown below.

$$\begin{aligned} h &= H_2(m||U_2, U) \\ e(P, V') &= e(P, W - s_A U_2) \\ &= e(P_{Pub}, U + hQ_{ID_X}) \cdot e(U_2, Q_A) \cdot e(s_A P, -U_2) \\ &= e(P_{Pub}, U + hQ_{ID_X}) \end{aligned}$$

The above equality means that the extracted signature (U_2, U, V') from the verifiably encryption signature (W, U_2, U) by the adjudicator satisfies the verification of **Verifying phase 3.4** . Hence our proposed VES scheme is valid.

4.2 Security Analysis

In the subsection, we will analyze the security of our proposed scheme and show the scheme is secure against existential forgery and extraction in random oracle model.

THEOREM 1. *Let G_1 and G_2 be cyclic groups of prime order p with a computable bilinear map $e : G_1 \times G_1 \longrightarrow G_2$, P be a generator of group G_1. Suppose that the our proposed variant of Cha-Cheon's signature scheme is $(t', q'_H, q'_S, \epsilon')-$ secure against existential forgery. Then the our proposed verifiably encrypted signature scheme is $(t, q_{H_1}, q_{H_2}, q_{H_3}, q_{VS}, q_A, \epsilon)-$ secure against existential forgery, where*

$$t \leq t' - (q_{VS} + q_A + 1)c_{G_1}$$

PROOF. Suppose that there exists a verifiably-encrypted-signature forger algorithm $\mathcal{V}_f$, then we can construct a forger algorithm $\mathcal{F}$ for the proposed variant of Cha-Cheon's signature scheme. (**Note that**: the proposed variant of Cha-Cheon's signature is proven secure in random oracle model).

The proposed variant of Cha-Cheon'signature forger $\mathcal{F}$ is given a public key ID_X, and has access to a signing oracle for ID_X and two hash oracles. It simulates the challenger and runs interacts with $\mathcal{V}_f$ as follows:

- Setup: A challenger $\mathcal{C}$ runs **Setup** of the proposed variant of Cha-Cheon's signature scheme, and gives the corresponding system parameters $(G_1, G_2, q, e, P, P_{pub}, H_1, H_2)$ to $\mathcal{F}$. And algorithm $\mathcal{F}$ chooses a $s_A \in Z_q$ at random and computes $P_A = s_A P$. Let (s_A, P_A) serve as the adjudicator's key pairs. Let $(G_1, G_2, q, e, P, P_{pub}, H_1, H_2, (s_A, P_A))$ be input of $\mathcal{V}_f$.
- $H_1(\cdot), H_2(\cdot), E(\cdot) - Oracle$: When algorithm $\mathcal{V}_f$ requests a $H_1(\cdot)$,(or $H_2(\cdot), E(\cdot)$) query, $\mathcal{F}$ makes a query to its own hash oracle $H_1(\cdot)$,(or $H_2(\cdot), E(\cdot)$), receiving some value, with which it responds to $\mathcal{V}_f$'s query.
- **VESig Oracle**: When algorithm $\mathcal{V}_f$ requests a signature on some string M_i under the user with the identity ID_X and the adjudicator' public P_A, algorithm $\mathcal{F}$ queries its signing oracle with input (ID_i, M_i) and obtains the reply (U_i, U_{2_i}, V_i) . Then $\mathcal{F}$ computes as follows:
  1. compute $W_i = V_i + s_A U_{2_i}$.
  2. output the verifiably encryption signature (W_i, U_i, U_{2_i})

  Finally, the algorithm $\mathcal{F}$ returns (W_i, U_i, U_{2_i}) on the string M_i to $\mathcal{V}_f$.

Table 1: Comparison of our scheme with the Gu et.al's scheme

Scheme	VES	VES-V	size
Our scheme	$1C_P$	$3C_e + 1C_M + 1C_P$	$3p$
Gu scheme	$2C_e + 7C_P$	$3C_e + 1C_P + 2C_M$	$1q + 3p$

- **Adjudication Oracle:** Algorithm $\mathcal{V}_f$ requests adjudication for (U_i, U_{2_i}, W_i), a verifiably encrypted signature on a message M_i under the user with the identity ID_i where $i \neq X$ and adjudicator key P_A. Algorithm $\mathcal{F}$ checks that the verifiably encrypted signature is valid, then computes as follows:

$$V_i' = W_i - s_A U_{2_i} \quad (1)$$

- **Output:** Finally, if $\mathcal{V}_f$ outputs a valid and nontrivial verifiably encrypted signature (U^*, U_2^*, W^*) on a message M^* in non-negligible probability. $\mathcal{F}$ sets $V'^* = W^* - s_A U_2^*$, which is a valid variant of Cha-Cheon's signature on the message M^*.

It remains only to analyze the success probability and running time of $\mathcal{F}$. Algorithm $\mathcal{F}$ succeeds when $\mathcal{V}_f$ does, that is, with probability at least ϵ.

$\mathcal{F}$'s running time is the same as V's running time plus the time it takes to respond to q_{H_1}, q_{H_2} hash queries, q_{VS} verifiably-encrypted signature queries, and q_A adjudication queries, and the time to transform W^*'s final verifiably-encrypted signature forgery into a variant of Cha-Cheon's signature forgery. Hash queries impose no overhead. Each verifiably-encrypted signature query requires $\mathcal{F}$ to only perform one point multiplications in G_1. Each adjudication query requires $\mathcal{F}$ to perform an point multiplication in G_1. The output phase also requires one point multiplication. We assume that the point multiplication in G_1 takes time c_{G_1}. Hence, the total running time is at most $t + (q_{VS} + q_A + 1)c_{G_1}$. □

THEOREM 2. *Let G_1 and G_2 be cyclic groups of prime order p with a computable bilinear map $e : G_1 \times G_1 \longrightarrow G_2$, P be a generator of group G_1. Q_A is the adjudicator's public key. Suppose that the CDH problem isn't solved in a polynomial time, then our verifiably encrypted signature is secure against extraction.*

PROOF. Due to page limitation, the proof is be omitted. Please refer to the full version of the paper for detail. □

4.3 Efficiency

In the following,we compare our verifiably encrypted signature with Gu *et.al*'s scheme from the view point of computation overhead and the size of signature. Let C_e denote the pairing operation, C_P the point scalar multiplication on G_1, C_{Ad} the point addition on G_1, C_M the multiplication on G_2. $|n|$ denotes the length of n. Note that the computation of the pairing and point scalar multiplication are more time-consuming. Comparison our scheme with Gu et.al's scheme, we know that our scheme is much more efficient than Gu et.al's scheme, and the size of our signature is shorter than Gu et.al's signature and consists of three elements of G_1 . where **VES** denotes VESignature, **VES-V** be VESignature Verification and **size** be the signature length.

5. CONCLUSION

Verifiably encrypted signatures are the special extension of general signature primitive, and are often used in online contract signing to provide fair exchange. It plays an important role in the e-commerce. In this works, we first propose a variant of Cha-Cheon signature scheme and give a verifiably encrypted signature scheme based on the variant scheme. Then we prove our proposed scheme to be secure in random oracle model. It is an open problem how to construct a ID-based verifiably encrypted signature without random oracle model.

6. ACKNOWLEDGEMENT

We thanks the anonymous referees for their very valuable comments. This work is supported by China Postdoctoral Science Foundation(NO:20060390007), Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality and Program for New Century Excellent Talents in University (NCET).

7. REFERENCES

[1] L. Boneh.D, Gentry.C and Shacham.H. *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps.* Springer-Verlag, Berlin, Germany, 2003.

[2] C.Gu and Y.Zhu. An identity-based verifiable encrypted signatures scheme based on hess scheme. In *CICC 2005, LNCS 3822*, pages 42–52. Springer -verlag, Nov 2005.

[3] F.Zhang and R.Safavi-Naini. *Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings.* Springer-verlag, New York, 2003.

[4] G.Ateniese. Efficient verifiable encryption (and fair exchange) of digial signatures. In *Proc. of th 6th Conference on CCS*, pages 138–146. ACM Press, Oct 1999.

[5] M. Gorantla and A. Saxena. Verifiably encrypted without random oracle. In *ICDCIT 2005, LNCS 3816*, pages 357–363. Springer -verlag, Nov 2005.

[6] F. Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptology the 9th Annual workshop, SAC 2002, LNCS 2595*, pages 310–324. Springer -verlag, Aug 2003.

[7] J.Camenisch and I.Dagard. Verifiable encryption,group encryption, and their application to separable group sigantures and signature sharing scheme. In *ASIACRYPT2000, LNCS 1976*, pages 331–345. Springer-verlag, March 2000.

[8] J. J.C.Cha. An identity-based signature from gap diffie -hellman groups. In *Proc.of the Public Key Cryptology -PKC 2003, LNCS 2567*, pages 18–30. Springer -verlag, May 2003.

[9] V. N.Asokan and V.Waidner. Optimistic fair exchange of digital signature (extended abstract). In *Cryptology-Eurocrypt'98, LNCS 1403*, pages 591–606. Springer -verlag, May 1998.