Verifiably Encrypted Signature Scheme with Threshold Adjudication

M. Choudary Gorantla and Ashutosh Saxena
Institute for Development and Research in Banking Technology
Road No. 1, Castle Hills, Masab Tank, Hyderabad - 500057
Andhra Pradesh, INDIA.
gmchoudary@gmail.com, asaxena@idrbt.ac.in

Abstract

Verifiably encrypted signature is useful in handling the fair exchange problem especially, online contract signing. In this paper, we propose a verifiably encrypted signature scheme using bilinear pairings. Our scheme facilitates the adjudication to be done in a threshold manner to achieve robustness. We show that the distribution of adjudication capability is robust and unforgeable. Our scheme is secure against extraction and existential forgery in the random oracle model.

Keywords: Fair Exchange, Verifiably Encrypted Signature, Threshold Cryptography, Bilinear Pairings, Random Oracles.

1 Introducion

Fair exchange is the problem of exchanging data in a way that guarantees that either all participants obtain what they want, or none do [1]. Contract signing is a particular form of fair exchange, in which the parties exchange commitments to a contract; typically, containing the terms of the deal. In the case of online contracts [11], a commitment is often identified with the party's digital signature on the contract. The important properties a contract signing protocol should guarantee are *fairness* and *timeliness* [13], [12].

A Verifiably Encrypted Signature (VES) enables optimistic fair exchange (see [1] and [4]) over the Internet. It uses no "time-out" mechanism[3] and neither party can be left hanging or cheated so long as the *Adjudicator*, a trusted party, is available. A VES enables the verifier to test that a given ciphertext is the encryption of a signature on a given message. Alice performs a VES by first signing on the message using her private key and then encrypting the signature using public key of an Adjudicator. The verifier, Bob is convinced that the encrypted signature is indeed of Alice by verifying it with the public keys of Alice and the Adjudicator. Even though Bob does not have the capability of decrypting the VES, the verification can be performed without deducing any information about Alice's signature. At a later stage, on agreed terms, Bob can obtain the original signature from Alice. In case of disputes, Bob approaches the Adjudicator who can retrieve Alice's signature from a valid VES.

It is clear that the property of *fairness* is defied if the adjudicator colludes with any of the participating entities. Distribution of trust, equally among multiple adjudicators, overcomes the problem of collusion of adjudicator with entities to some extent. However, this requires the contribution from all the adjudicators. Another major limitation of the existing VES schemes (see [4], [17] and [9]) is single point of failure of the adjudicator. Since most of the applications of VES are online, it is expected that the adjudication services are always available (*i.e. timeliness*). We address the limitation of the existing schemes w.r.t. *fairness* and *timeliness* by using the concept of threshold cryptosystem [7]. In our scheme, we use threshold adjudication in such a way that the adjudication services can be offered even if t of the adjudicators are corrupted. For this, we employ secure distributed key generation protocol of [8], which produces Shamir's secret-sharing [14] of a secret without trusted dealer. By using this interactive protocol, the adjudication capability can be distributed to n adjudicators out of which any $(t+1)$ can adjudicate a VES.

Boneh *et al.* [4] gave a VES as an application of aggregate signature considering [6] as the base scheme. Later, Zhang *et al.*[17] proposed another VES scheme based on the signature scheme in [16]. Both these schemes are based on bilinear pairings with security proofs in random oracle model. Recently, Hess [9] presented an efficient attack on the VES scheme in [4] by allowing adversaries to access the adjudication oracles for different users but the same adjudicator and proposed an improvement over it.

In this paper, we propose a verifiably encrypted signature scheme with threshold adjudication using the VES scheme given in [9]. We show that the distribution of adjudication capability is robust and unforgeable. Our scheme is secure against extraction and existential forgery in the random oracle model [2].

The rest of the paper is organized as follows: Section 2 gives background concepts. In Section 3, we present our verifiably encrypted signature with threshold adjudication. We analyze the security of our scheme in Section 4 and Section 5 concludes the work.

2 Background Concepts

2.1 The Bilinear Pairings

We use cryptographic bilinear pairing, which is a modified Weil pairing [5] to construct our scheme. The pairing is defined as $e : G \times G \to V$, where G and V both are multiplicative cyclic groups of prime order p with the following properties.

Bilinear: For any $r, s, t \in G$, $e(rs, t) = e(r, t)e(s, t)$ and $e(r, st) = e(r, s)e(r, t)$

Non-degenerate: There exists $r, s \in G$ such that $e(r, s) \neq I_V$ where I_V denotes the identity element of the group V.

Computable: There exists an efficient algorithm to compute $e(r, s)\ \forall\ r, s \in G$.

2.2 Modified Short Signature Scheme

In 2001, Boneh et al. [6] proposed a short signature (BLS) scheme based on Weil pairing. Recently, Tan [15] identified that BLS scheme suffers from key substitution attack [10]. However, we observe that the modified version of BLS (H-BLS) scheme presented by Hess [9] successfully withstands the key substitution attack. We briefly describe the H-BLS scheme here.

Let $M \subseteq \{0, 1\}^*$ be the message space and $H : M \times G \to G$ a full domain hash function.

KeyGen: A signer picks a random $a \in Z_p$ and computes $v \leftarrow g^a$, where g is an arbitrary generator of G. The private key of the signer is a and the corresponding public key is $v \in G$.

Sign: Given a message $m \in M$ and a secret key a, compute $h \leftarrow H(m, v)$ and $\sigma \leftarrow h^a$. The signature is $\sigma \in G$.

Verify: Given a signature σ on a message m and public key v, compute $h \leftarrow H(m, v)$. Accept the signature if $e(g, \sigma) = e(v, h)$, reject otherwise.

3 VES with Threshold Adjudication

A verifiably encrypted signature(VES) scheme consists of three entities: signer, verifier and adjudicator. In our scheme the entity adjudicator is represented by a set of n distinct adjudicators, to whom the adjudication capability is distributed in a threshold manner. The seven phases of the VES scheme are described as below.

KeyGen, Sign, Verify: Same as in the H-BLS scheme given in section 2.2.

AdjKeyGen: In this phase, the shares for all the n adjudicators are generated using the interactive distributed key generation protocol of [8]. Following this protocol, all the n adjudicators communicate among themselves for computing their shares $b_1, \ldots, b_n$ and a common public key $v' = g^b$, where b is the secret key corresponding to v'. The secret key b can be generated by any $(t + 1)$ adjudicators with their shares by Lagrange's interpolation. The n adjudicators also have individual public keys corresponding to their secret shares as $v'_i \leftarrow g^{b_i}$ for $1 \leq i \leq n$.

VES-Creation: The verifiably encrypted signature is generated on a given message $m \in M$ using the user's secret key a and adjudicators' public key v'. The VES $\langle \mu, \omega \rangle \in G \times G$ is computed as

$$
\begin{aligned}
&h \leftarrow H(m, v)\\
&\sigma \leftarrow h^a\\
&s \in_R Z_p\\
&\mu \leftarrow g^s\\
&\omega \leftarrow \sigma v'^s
\end{aligned}
$$

The VES on the message m is $\langle \mu, \omega \rangle$.

VES-Verification: A given VES $\langle \mu, \omega \rangle$ on a message m is verified using the adjudicators' public key v' and signer's public key v. It is accepted if and only if the equation $e(g, \omega) = e(v, h)e(v', \mu)$ holds, setting $h \leftarrow H(m, v)$.

Adjudication: If the signer is unable or unwilling to cooperate with the verifier, the verifier sends the the VES $\langle \mu, \omega \rangle$ to all the n adjudicators. Then each adjudicator computes the share $\sigma_i \leftarrow \omega/\mu^{b_i}$ for $1 \le i \le n$ and sends it to the verifier in a secure channel. The verifier validates the correctness of each of the received σ_i by checking the below equation using the individual public key v'_i of i^{th} adjudicator,

$$e(\sigma_i, g) = e(\omega, g)e(1/\mu, v'_i)$$

The share to the signature σ_i is rejected if it does not satisfy the above equation. The original signature is reconstructed from all the valid signature shares σ_i, by the following equation

$$\sigma \leftarrow \omega \prod_i \left(\frac{\sigma_i}{\omega}\right)^{L_i}$$

Here, i represents the index for honest adjudicator and L_i is the corresponding Lagrange's coefficient available publicly.
Note that using the interactive protocol of [8], the original signature σ can be reconstructed only if at least $(t+1)$ honest adjudicators contribute in the adjudication process.
Validity: The correctness of the VES verification equation is justified as below:

$$
\begin{aligned}
&e(g, \omega)\\
&\quad = e(g, \sigma v'^s)\\
&\quad = e(g, \sigma)e(g, v'^s)\\
&\quad = e(g, h^a)e(g, g^{bs})\\
&\quad = e(g^a, h)e(g^b, g^s)\\
&\quad = e(v, h)e(v', \mu)
\end{aligned}
$$

The above equations mean VES-Verification(m, VES-Creation) is true.
And also the verification of the signature extracted from the given $\langle \mu, \omega \rangle$ in the adjudication phase holds good as shown below.

$$
\begin{aligned}
&e\left(g, \omega \prod_i \left(\tfrac{\sigma_i}{\omega}\right)^{L_i}\right)\\
&\qquad = e\left(g, \omega \prod_i \left(\frac{1}{\mu^{b_i}}\right)^{L_i}\right)\\
&\qquad = e\left(g, \frac{\omega}{\mu^{\sum_i L_i b_i}}\right)\\
&\qquad = e\left(g, \frac{\omega}{\mu^b}\right)\\
&\qquad = e(g, h^a)\\
&\qquad = e(g^a, h)\\
&\qquad = e(v, h).
\end{aligned}
$$

which means Verify(m, Adjudication(VES-Creation(m))) is true.

Hence, the *Validity* of our verifiably encrypted signature scheme holds.

4 Security Analysis

In this section we first show that the protocol executed by the adjudicators is robust and unforgeable. Subsequently, we give the proof of security against extraction and unforgeability for our scheme using the result of [9].

Theorem I. *The protocol executed by the adjudicators is secure against an adversary which can corrupt t adjudicators, for any $t < n/2$ in the random oracle model.*
Proof. We first prove that the protocol is robust and then show that it is unforgeable.
Robustness. In the presence of an adversary that corrupts $t < n/2$ adjudicators, all subsets of $(t+1)$ shares generate the same unique b that correspond to the unique public key $v' = g^b$. Note that b is uniformly distributed in Z_p and thus v' is also uniformly distributed in G and hence the AdjKeyGen completes successfully even in the presence of a corruptive adversary. It may also be noted that only valid signature shares of the adjudicators can pass the verification step performed by the verifier in the Adjudication phase since each valid signature share σ_i is generated by a valid secret share b_i corresponding to the individual public key v'_i. The fact that the original signature σ can be constructed from any $(t+1)$ valid signature shares σ_i using Lagrange's interpolation implies that threshold adjudication is complete.
Unforgeability. The threshold adjudication is unforgeable if no signature share can be forged without the knowledge of corresponding secret share. To analyze this, we assume that there exists a probabilistic polynomial-time simulator (SIM) for every probabilistic polynomial-time adversary $\mathcal{A}$ that corrupts up to t adjudicators. Given the public key v', the VES $\langle \mu, \omega \rangle$ and signature σ on a message m the SIM can simulate the view for $\mathcal{A}$. But, this view is polynomially indistinguishable from $\mathcal{A}$'s view of the runs of the AdjKeyGen and Adjudication that output v' and σ respectively.

Without loss of generality assume that the adversary corrupts the adjudicators with indices $1, \ldots, t'$ where $t' \le t$. Due to [8], the SIM knows all the shares b_i except one (with out loss of generality assumed to be b_n) of the honest adjudicators. The values corresponding to the last share can be computed using the fixed v' and the rest of the shares. The SIM can verify the validity of the shares σ_i that are output by the corrupted adjudicators, who are honest during the run of AdjKeyGen, using the knowledge of their shares. Now, it needs to simulate the signature shares of the uncorrupted adjudicators. Since SIM has all the shares $b_{t'+1}, \ldots, b_{n-1}$, it can generate the signature shares σ_i as $\sigma_i \leftarrow \omega/\mu^{b_i}$ for $i = t'+1, \ldots, n-1$. SIM creates the signature share corresponding to the honest adjudicator as $\sigma_n = \sigma \left(\omega \prod_i \left(\frac{\sigma_i}{\omega}\right)^{-1} \right)$. Since all the shares b_i used by SIM have the right distribution, all the signature shares computed by SIM also have the right distribution. This is because all signature shares except σ_n explicitly use known corresponding secret shares and by construction σ_n corresponds to the share b_n which is implicitly used by SIM. Thus no signature share can be forged without the knowledge of corresponding secret share and hence the adjudication is unforgeable.

Theorem II. *Our verifiably encrypted signature scheme is secure against extraction.*
Proof. An extracting adversary is successful in its attempts if it can retrieve the original signature from the the VES.A forging adversary to the H-BLS scheme is trivially an extracting adversary against our scheme. The security of our scheme is derived from the fact that H-BLS scheme is secure against existential forgery and directly follows from Theorem 1 of [9].

Theorem III. *Our verifiably encrypted signature scheme is secure against existentially forgery.*
Proof. A forging adversary is successful in its attempts if it can
(i) construct a valid signature by corrupting t adjudicators for $t < n/2$. or
(ii) perform an existential forgery on the original signature.
The adversary becoming successful in (i) is a contradiction to the unforgeability property given in Theorem I. The proof for (ii) directly follows from Theorem 2 of [9].

5 Conclusions

Verifiably encrypted signatures find applications in online fair exchange, especially in online contract signing protocols. In this work, we proposed a verifiably encrypted signature scheme with threshold adjudication by distributing the adjudication capability in such a way that the service can be provided if at least $(t+1)$ honest adjudicators contribute to the adjudication. We showed that the distribution is robust and unforgeable. Our scheme is secure against extraction and existential forgery in the random oracle model.

References

[1] Asokan, N., Shoup, V., Waidner, M.: Optimistic Fair Exchange of Digital Signatures. In Advances in Cryptology-Eurocrypt 98, LNCS **1403**. Springer-Verlag. (1998) 591-606

[2] Bellare, M., Rogaway, P.: Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. In 1st ACM Confernece on Computer and Communications Security. ACM Press. (1993) 62-73

[3] Ben-Or, M., Goldreich, O., Micali, S., Rivest, R.: A fair protocol for signing contracts. IEEE Transactions on Information Theory, **36(1)**. (1990) 4046

[4] Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In Advances in Cryptology-Eurocrypt 2003. LNCS **2656**. Springer-Verlag. (2003) 272-293

[5] Boneh, D., Franklin, M.: Identity-based Encryption from the Weil pairing. In Advances in Cryptology-Crypto 2001. LNCS **2139**. Springer-Verlag, (2001) 213-229

[6] Boneh, D., Lynn, B., Shacham, H.: Short Signatures from the Weil Pairing. In Advances in Cryptology-Asiacrypt 2001. LNCS **2248**. Springer-Verlag. (2001) 514-532

[7] Gemmel, P.: An introduction to threshold cryptography. RSA CryptoBytes. **2(3)**. (1997) 712

[8] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Secure distributed key generation for discrete-log based cryptosystems. In Advances in Cryptology-Eurocrypt'99. **LNCS** 1592. Springer-Verlag. (1999) 295-310

[9] Hess, F.: On the Security of the verifiably-encrypted signature scheme of Boneh, Gentry, Lynn and Shacham. Information Processing Letters. **89**. (2004) 111-114.

[10] Menezes, A., Smart, N.: Security of Signature Schemes in a multi-user setting. Designs, Codes and Cryptography, **33(3)**. (2004) 261-274

[11] Molnar, D.: Signing electronic contracts. Crossroads. **7(1)**. ACM Press. (2000) 6ff

[12] Norman, G., Shmatikov, V.: Analysis of Probabilistic Contract Signing. In Proceeding of FASec 2002. LNCS **2629**. Springer. (2003) 81-96

[13] Ray, I., Ray, I.: Fair Exchange in E-commerce, ACM SIGecom Exchange, **3(2)**. ACM Press. (2002) 9-17

[14] Shamir, A.: How to share a secret. Communications of the ACM. **22(11)**. ACM Press. (1979) 612-613

[15] Tan, C.-H.: Key Substitution Attacks on Provable secure Short Signature Scheme. IEICE Trans. Fundamentals. **E88-A** (2005) 611-612

[16] Zhang, F., Safavi-Naini, R., Susilo, W.: An efficient signature scheme from bilinear pairings and its applications. In Public Key Cryptography 2004. LNCS **2947**. Springer-Verlag. (2004) 277-290

[17] Zhang, F., Safavi-Naini, R., Susilo, W.: Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. In Progress in Cryptology-Indocrypt 2003. LNCS 2904, Springer-Verlag. (2003) 191-204