ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.4, April 2009, pp.1069−1076
doi: 10.3724/SP.J.1001.2009.00555
© by *Institute of Software, the Chinese Academy of Sciences*. All rights reserved.

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种无随机预言机的高效可验证加密签名方案*

杨浩淼+, 孙世新, 徐继友

(电子科技大学 计算机学院,四川 成都 610054)

Efficient Verifiably Encrypted Signature Scheme without Random Oracles

YANG Hao-Miao+, SUN Shi-Xin, XU Ji-You

(School of Computer, University of Electronic Science and Technology of China, Chengdu 610054, China)

+ Corresponding author: E-mail: haomyang@uestc.edu.cn

Yang HM, Sun SX, Xu JY. Efficient verifiably encrypted signature scheme without random oracles. *Journal of Software*, 2009,20(4):1069−1076. http://www.jos.org.cn/1000-9825/555.htm

Abstract: This paper proposes an efficient verifiably encrypted signature scheme without random oracles. The scheme is constructed from the recent Gentry signature and can be rigorously proven to be secure in the standard model. The scheme has several advantages over previous systems such as, shorter public keys, lower computation overhead, and a tighter security reduction, therefore, it is a truly practical verifiably encrypted signature without random oracles, which can be used in online contract signing protocols. Additionally, the proof of our scheme, which depends on the Strong Diffie-Hellman assumption, may be of independent interest.

Key words: digital signature; verifiably encrypted signature; provable security; random oracle model

摘 要: 提出了一种高效的无随机预言机的可验证加密签名方案.该方案使用近来出现的 Gentry 签名进行构造,并在标准模型下严格证明其安全性.与同类方案相比,该方案构造简单,有较短的公钥尺寸、较低的计算代价以及较紧的安全归约.它是一个真正实践的无随机预言机的可验证加密签名方案,可以用于实际的在线合同签署协议.此外,方案的证明依赖于强 Diffie-Hellman 假设,也有其独立的价值.

关键词: 数字签名;可验证加密签名;可证明安全;随机预言机模型

中图法分类号: TP309 **文献标识码**: A

1 Introduction

A verifiably encrypted signature (VES) scheme involves three parties, the user or signer, the verifier, and a trusted third party, the adjudicator. The basic idea is that the user Alice creates an encryption of her signature on some message using the public key of the adjudicator. The verifier Bob can verify that this encrypted signature is indeed the encryption of the Alice's signature on the message, but Bob cannot deduce any information about Alice's signature. At a later stage, if Alice is unable or unwilling to reveal her signature, Bob can ask the adjudicator to reveal Alice's signature. Verifiably encrypted signatures may be used in contract signing protocols to provide

* Supported by the National Natural Science Foundation of China under Grant No.60673075 (国家自然科学基金); the Doctoral Program Foundation of Chinese Ministry of Education under Grant No.20050614018 (国家教育部高等学校博士学科点专项科研基金)

Received 2007-11-13; Accepted 2008-02-04

optimistic fair exchange[1,2].

Previous constructions of verifiably encrypted signatures require zero knowledge proofs to verify an encrypted signature[1]. In 2003, Boneh, *et al*.[3] gave a verifiably encrypted signature scheme as an application of their aggregate signature. There is no need for zero knowledge proofs, so the scheme is short and can be validated efficiently. In Ref.[4], Zhang, *et al*. also proposed a verifiably encrypted signature scheme based on their short signature from bilinear pairings, which does not need zero knowledge proofs and is more efficient than previous schemes. However, both schemes are provably secure only in the random oracle model and thus there is only a heuristic argument for their security.

It is natural to ask whether secure verifiably encrypted signatures exist in the standard model. This question is especially relevant in light of several recent uninstantiable random oracle cryptosystems[5], which are secure in the random oracle model, but are provably insecure under any actual instantiation of the oracle.

In ICDCIT 2005, based on the short signature without random oracles proposed by Boneh and Boyen[6], Gorantla, *et al*.[7] firstly proposed a verifiably encrypted signature without random oracles. Using the same short signature, Li, *et al*.[8] also proposed a similar verifiably encrypted signature with rigorous security proofs in the stand model. In EUROCRYPT 2006, Lu, *et al*.[9] presented a novel verifiably encrypted signature without random oracles, which was based on the Waters signature. However, their scheme is not quite efficient. For example, a user's public key will be quite large. If a 160-bit collision resistant hash function is used, keys will be approximately 160 group elements and take around 10KB to store. Additionally, based on Wei's signature, Ming and Wang[10] presented a verifiably encrypted signature scheme without random oracles, which is more efficient than existing schemes in the literature and has a tight security reduction.

In this paper, we propose a efficient verifiably encrypted signature that is fully secure without random oracles. Our construction is based on the signature of Gentry[11], which is derived from his practical Identity-Based Encryption (IBE). As a result, our scheme is simple and efficient. For example, signature and verification require only a small constant number of group operations, while user public keys are compact (three group elements).

2 Preliminaries

In this section we first review the definitions of bilinear maps and bilinear groups. Next, we discuss the complexity assumption on which the security of our system is based. Then, we briefly recall the definition and security notions of the verifiably encrypted signature. Finally, we derive the signature of Gentry from his IBE.

2.1 Bilinear maps and bilinear groups

We briefly review bilinear maps and bilinear groups, following the notation in Ref.[6]. For simplicity we set $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$. Consider the following setting:

(1) $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative cyclic groups of prime order p;

(2) g is a generator of $\mathbb{G}$.

(3) e: $\mathbb{G}\times\mathbb{G} \rightarrow \mathbb{G}_T$ is a bilinear map.

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups as above. A bilinear map is a map e: $\mathbb{G}\times\mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

(1) Bilinear: for all $u,v \in \mathbb{G}$ and $a,b \in \mathbb{Z}$, $e(u^a,v^b) = e(u,v)^{ab}$.

(2) Non-degenerate: $e(g,g) \neq 1$.

We say that $\mathbb{G}$ is a bilinear group if the group action in $\mathbb{G}$ can be computed efficiently and there exists a group $\mathbb{G}_T$ and an efficiently computable bilinear map e: $\mathbb{G}\times\mathbb{G} \rightarrow \mathbb{G}_T$ as above.

2.2 Complexity assumption

Let $\mathbb{G}$ be a cyclic group of prime order p, and let g be a generator of $\mathbb{G}$.

*q-Strong Diffie-Hellman Problem***.** The q-SDH problem in $\mathbb{G}$ is defined as follows: given a (q+1)-tuple $\left(g, g^{x}, g^{x^2}, \ldots, g^{x^q}\right)$ as input, output a pair $\left(c, g^{1/(x+c)}\right)$ where $c \in \mathbb{Z}_p^{\ *}$. An algorithm $\mathcal{A}$ has advantage ε in solving q-SDH in $\mathbb{G}$ if

$$\Pr\left[\mathcal{A}\left(g, g^{x}, g^{x^2}, \ldots, g^{x^q}\right) = \left(c, g^{1/(x+c)}\right)\right] \geq \varepsilon ,$$

where the probability is over the random choice of x in $\mathbb{Z}_p^{\ *}$ and the random bits consumed by $\mathcal{A}$.

Definition 1. We say that the (q, t, ε)-SDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the q-SDH problem in $\mathbb{G}$.

Occasionally we drop the t and ε and refer to the q-SDH assumptions in $\mathbb{G}$.

2.3 Verifiably encrypted signatures

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

Key Generation, Signing, Verification. As in standard signature schemes.

Adjudicator Key. Generate a public-private key pair (*apk*,*ask*) for the adjudicator.

VESig Creation. Given a secret key *sk*, a message *m*, and an adjudicator's public key *apk*, compute (probabilistically) a verifiably encrypted signature *v* on *m*.

VESig Verification. Given a public key *pk*, a message *m*, an adjudicator's public key *apk*, and a verifiably encrypted signature *v*, verify that *v* is a valid verifiably encrypted signature on *m* under key *pk*.

Adjudication. Given an adjudicator's key pair (*apk*,*ask*), a certified public key *pk*, and a verifiably encrypted signature *v* on some message *m*, extract and output σ, an ordinary signature on *m* under *pk*.

Besides the ordinary notions of signature security in the signature component, a verifiably encrypted signature scheme should satisfy the following properties.

Validity. It requires that verifiably encrypted signatures verify, and that adjudicated verifiably encrypted signatures verify as ordinary signatures, i.e., that *VESigVerify*(*m*,*VESigCreate*(*m*)) and *Verify*(*m,Adjudicate* (*VESigCreate*(*m*)) hold for all *m* and for all properly-generated key pairs and adjudicator key pairs.

Unforgeability. It requires that it be difficult to forge a valid verifiably encrypted signature. The advantage in existentially forging a verifiably encrypted signature of an algorithm $\mathcal{F}$, given access to a verifiably-encrypted-signature creation oracle S and an adjudication oracle A is

$$\mathrm{Adv}_{\mathcal{F}}^{\mathrm{VSigF}} = \Pr\left[\begin{array}{r} \mathit{VESigVerify}(pk, apk, m, v) \ = \ \text{valid}: \\ (pk, sk) \leftarrow \mathit{KeyGen}, \\ (apk, ask) \leftarrow \mathit{AdjKeyGen}, \\ (m, v) \leftarrow \mathcal{F}^{S,A}(pk, apk) \end{array}\right].$$

The probability is taken over the coin tosses of the key-generation algorithms, of the oracles, and of the forger. The forger is additionally constrained in that its forgery on *m* must be nontrivial: It must not previously have queried either oracle at *m*.

Definition 3. An algorithm $\mathcal{F}$ (t, q_S, q_A, ε)-forges a verifiably encrypted signature if: $\mathcal{F}$ runs in time at most t, makes at most q_S queries to the verifiably-encrypted-signature creation oracle S, at most q_A queries to the adjudication oracle A, and $\mathrm{Adv}_{\mathcal{F}}^{\mathrm{VSigF}}$ is at least ε. A verifiably encrypted signature scheme is (t, q_S, q_A, ε)-secure against existential forgery if no forger (t, q_S, q_A, ε)-breaks it.

Opacity. It requires that it be difficult, given a verifiably encrypted signature, to extract an ordinary signature on the same message. 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 is

$$\mathrm{Adv}_{\mathcal{E}}^{\mathrm{VSigE}}=\Pr\begin{bmatrix} Verify(pk,m,\sigma)\ =\ \text{valid}: \\ (pk,sk)\leftarrow KeyGen, \\ (apk,ask)\leftarrow AdjKeyGen, \\ (m,\sigma)\leftarrow \mathcal{E}^{S,A}(pk,apk) \end{bmatrix}.$$

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. Verifiably encrypted signature extraction is thus no more difficult than forgery in the underlying signature scheme.

Definition 4. An algorithm ε $(t, q_S, q_A, \varepsilon)$-extracts a verifiably encrypted signature if: ε runs in time at most t, makes at most q_S queries to the verifiably-encrypted-signature creation oracle S, at most q_A queries to the adjudication oracle A, and $\mathrm{Adv}_{\mathcal{E}}^{\mathrm{VSigE}}$ is at least ϵ. A verifiably encrypted signature scheme is $(t, q_S, q_A, \varepsilon)$-secure against extraction if no algorithm $(t, q_S, q_A, \varepsilon)$-extracts it.

2.4 The gentry signature scheme

We describe the signature scheme of Gentry obtained from his IBE, although the signature scheme is not explicitly given in Ref.[11]. As noted by Moni Naor (see Section 5 of Ref.[12]), every IBE system secure against an adaptive-ID attack can be converted a public key signature scheme secure against existential forgery under a chosen-message attack. Note that from the generic transformation, the verification algorithm is randomized. However, we can use the bilinear map to deterministically verify a signature.

In our description, the message m to be signed is an element of $\mathbb{Z}_p^*$. However, in practice one could apply a collision-resistant hash function H: $\{0,1\}^* \to \mathbb{Z}_p^*$ to sign messages of arbitrary length. Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p, and let e: $\mathbb{G}\times\mathbb{G} \to \mathbb{G}_T$ be the bilinear map. The Gentry signature scheme is a three-tuple of algorithms $\mathcal{G}$ = (Kg, Sig, Vf). The signature works as follows.

G.**Kg**. Pick random generators g, $h \in \mathbb{G}$ and a random $\alpha\in \mathbb{Z}_p^*$. Set $g_1 = g^{\alpha}\in \mathbb{G}$. The public key pk is (g,g_1,h) and the private key sk is α.

G.**Sig**(sk, m). Given a private key sk and a message $m \in \mathbb{Z}_p^*$, parse sk as $\alpha\in \mathbb{Z}_p^*$. Pick a random $r \in \mathbb{Z}_p^*$, and compute $S = (hg^{-r})^{1/(\alpha-m)}$. The signature is $\sigma = (r,S)$.

G.**Vf**(pk, m, σ). Given a public key pk, a message $m \in \mathbb{Z}_p^*$ and a signature σ, parse pk as $(g,g_1,h) \in \mathbb{G}^3$ and σ as $(r,S) \in \mathbb{Z}_p^*\times\mathbb{G}$. Verify that $e(g_1g^{-m},S)\, e(g,g)^r = e(g,h)$ holds; if so, output valid; if not, output invalid.

3 A New Verifiably Encrypted Signature Scheme without Random Oracles

In this section, we propose a new verifiably encrypted signature scheme without random oracles. This new scheme uses the above Gentry signature and is a seven-tuple of algorithms $\mathcal{GVES}$ = (Kg, Sig, Vf, AKg, ESig, EVf, Adj) that behave as follows.

GVES.**Kg**, **GVES**.**Sig**, **GVES**.**Vf**. These are the same as G.Kg, G.Sig, and G.Vf, respectively.

GVES.**AKg**. Pick a random $\beta\in \mathbb{Z}_p^*$, and set $g_2 = g^{\beta}$ and $h_2 = h^{\beta}$. The adjudicator's public key apk is (g_2,h_2) and the adjudicator's private key ask is β.

GVES.**ESig**(sk, apk, m). Given the user's private key sk, the adjudicator's public key apk and a message $m \in$

$\mathbb{Z}_p^*$, parse *sk* as $\alpha \in \mathbb{Z}_p^*$ and *apk* as $(g_2,h_2) \in \mathbb{G}^2$. Pick a random $r \in \mathbb{Z}_p^*$, and compute $K = (h_2 g_2^{-r})^{1/(\alpha-m)}$. The verifiably encrypted signature is $v = (r,K)$.

GVES.**EVf**(*pk*, *apk*, *m*, *v*). Given the user's public key *pk*, the adjudicator's public key *apk*, a message $m \in \mathbb{Z}_p^*$, and a verifiably encrypted signature *v*, parse *pk* as $(g,g_1,h) \in \mathbb{G}^3$, *apk* as $(g_2,h_2) \in \mathbb{G}^2$, and *v* as $(r,K) \in \mathbb{Z}_p^* \times \mathbb{G}$. Accept if the following equation holds: $e(g_1 g^{-m},K)\, e(g,g_2)^r = e(g,h_2)$.

GVES.**Adj**(*ask*, *pk*, *apk*, *m*, *v*). Given the adjudicator's private key *ask*, the user's public key *pk*, the adjudicator's public key *apk*, a message $m \in \mathbb{Z}_p^*$, and a verifiably encrypted signature *v*, parse *ask* as $\beta \in \mathbb{Z}_p^*$, *pk* as $(g,g_1,h) \in \mathbb{G}^3$, *apk* as $(g_2,h_2) \in \mathbb{G}^2$, and *v* as $(r,K) \in \mathbb{Z}_p^* \times \mathbb{G}$. Verify (using EVf) that the verifiably encrypted signature *v* is valid, and compute $S = K^{1/\beta}$. The extracted ordinary signature is $\sigma = (r,S)$.

4 Security Analysis

In this section, we show that the proposed scheme satisfies the three security properties of verifiably encrypted signatures: validity, unforgeability, and opacity.

4.1 Validity

Given a verifiably encrypted signature (*r*, *K*) for a message *m*, we have

$$\begin{aligned} e(g_1 g^{-m},K)e(g,g_2)^r &= e\left(g^{\alpha-m},(h_2 g_2^{-r})^{1/(\alpha-m)}\right)e(g,g_2)^r = e(g,h_2 g_2^{-r})e(g,g_2)^r \\ &= e(g,h_2)e(g,g_2)^{-r}e(g,g_2)^r = e(g,h_2). \end{aligned}$$

This implies that the verifiably encrypted signatures verify. On the other hand, given the signature (*r*,*S*) extracted from the verifiably encrypted signature (*r*, *K*) in the adjudication phase, we have

$$\begin{aligned} e(g_1 g^{-m},S)e(g,g)^r &= e(g^{\alpha-m},K^{1/\beta})e(g,g)^r = e(g^{\alpha-m},K)^{1/\beta}e(g,g)^r = \left(e(g,h_2)e(g,g_2)^{-r}\right)^{1/\beta}e(g,g)^r \\ &= e(g,h_2)^{1/\beta}\left(e(g,g_2)^{-r}\right)^{1/\beta}e(g,g)^r = e(g,h)e(g,g)^{-r}e(g,g)^r = e(g,h). \end{aligned}$$

This means that the adjudicated verifiably encrypted signatures verify as ordinary signatures. Hence, the validity of our verifiably encrypted signature scheme holds.

4.2 Unforgeability

Theorem 1. The verifiably encrypted signature scheme $\mathcal{GVES}$ is $(t, q_S, q_A, \varepsilon)$-unforgeable if the Gentry signature scheme is (q', t', ε')-unforgeable, where

$$t' = t + O(q_S + q_A) \text{ and } q' = q_S \text{ and } \varepsilon' = \varepsilon.$$

Proof: We will show how to turn a verifiably-encrypted signature forger $\mathcal{A}$ into a forger $\mathcal{B}$ for the underlying Gentry signature scheme.

Setup. Algorithm $\mathcal{B}$ is given a Gentry signature public key (g, g_1, h). It picks a random $\beta \in \mathbb{Z}_p^*$ and sets $g_2 = g^\beta$ and $h_2 = h^\beta$, and provides the adversary $\mathcal{A}$ with (g, g_1, h) and (g_2, h_2).

Verifiably Encrypted Signing Queries. When $\mathcal{A}$ requests a verifiably encrypted signature on some message *m*, the challenger $\mathcal{B}$ requests a signature on *m* from its own signing oracle, obtaining a Gentry signature (*r*,*S*). It then computes $K = S^\beta$. The tuple of (*r*,*K*) is a valid verifiably encrypted signature on *m*. Algorithm $\mathcal{B}$ provides $\mathcal{A}$ with it.

Adjudication Queries. When algorithm $\mathcal{A}$ requests adjudication of a verifiably encrypted signature (*r*,*K*) on some message *m* under the challenge key (g, g_1, h), $\mathcal{B}$ responds with GVES.Adj(β, (g,g_1,h), (g_2,h_2), *m*, (*r*,*K*)). Note that $\mathcal{B}$ knows the adjudicator's private key β.

Output. Finally, $\mathcal{A}$ outputs a forged verifiably-encrypted signature (r^*, K^*) on some message m^*. Algorithm $\mathcal{A}$ must never have made a verifiably encrypted signing query at m^*. The challenger $\mathcal{B}$ computes $S^* = K^{*1/\beta}$. Then (r^*,

S^*) is a valid Gentry signature on the message m^*.

Because $\mathcal{A}$ did not make a verifiably encrypted signing query at m^*, neither did $\mathcal{B}$ make a signing query at m^*, and the forgery is thus nontrivial. The challenger $\mathcal{B}$ outputs (r^*, S^*) and halts.

Algorithm $\mathcal{B}$ thus succeeds whenever $\mathcal{A}$ does. $\mathcal{B}$'s running time is roughly the same as $\mathcal{A}$'s running time plus the time taken to respond to each of $\mathcal{A}$'s verifiably encrypted signing and adjudication queries.

4.3 Opacity

Theorem 2. The verifiably encrypted signature scheme $\mathcal{GVES}$ is (t, q_S, q_A, ϵ)-opaque if (q, t', ε')-SDH assumption holds in $\mathbb{G}$, where

$$t' = t + O(q_S + q_A) + O(q^2) \text{ and } q_S < q \text{ and } \varepsilon' = \frac{p-1}{p}\varepsilon \approx \varepsilon .$$

Proof: Given an algorithm $\mathcal{A}$ that breaks the opacity of the scheme, we show how to construct an algorithm $\mathcal{B}$ that breaks the Strong Diffie-Hellman Assumption. The challenger $\mathcal{B}$ is given $\{g^{\alpha^i} : i \in [0,q]\}$; its goal is to compute a pair (c, $g^{1/(\alpha-c)}$).

Given $\{g^{\alpha^i}\}$, $\mathcal{B}$ sets $g_1 = g^{\alpha}$, and computes h by generating a random q-degree polynomial $f(x) \in \mathbb{Z}_p[x]$ and setting $h = g^{f(\alpha)}$. $\mathcal{B}$ picks a random $\beta \in \mathbb{Z}_p^*$ and sets $g_2 = g^{\beta}$ and $h_2 = h^{\beta}$. It then interacts with $\mathcal{A}$ as follows.

Setup. Algorithm $\mathcal{B}$ gives to $\mathcal{A}$ the signer's public key (g, g_1, h), and the adjudicator's public key (g_2, h_2). Note that the (unknown) private signing key is α.

Verifiably Encrypted Signing Queries. $\mathcal{A}$ requests a verifiably-encrypted signature on $m \in \mathbb{Z}_p^*$ under the challenge key (g, g_1, h) and adjudicator key (g_2, h_2). If the signature for m is requested more than once, the same value of r_m is used each time.

To generate a Gentry signature for m ($m \neq \alpha$; if $m = \alpha$, $\mathcal{B}$ can use α to solve q-SDH immediately), $\mathcal{B}$ sets $r_m = f(m)$ and $S_m = (hg^{-r_m})^{1/(\alpha-m)} = g^{(f(\alpha)-f(m))/(\alpha-m)}$; $\mathcal{B}$ can compute the latter from $\{g^{\alpha^i}\}$, since $(f(\alpha)-f(m))/(\alpha-m)$ is a $(q-1)$-degree polynomial in α. The values of r_{m_i} in the simulation for $i \in [1, q_S]$ appear uniformly random, since $f(x)$ is a random polynomial of degree q. The tuple of (r_m, S_m) is a valid Gentry signature.

$\mathcal{B}$ then computes $K_m = (S_m)^{\beta}$ and returns the verifiably encrypted signature (r_m, K_m) to $\mathcal{A}$.

Adjudication Queries. Suppose $\mathcal{A}$ requests adjudication on (r_m, K_m) for message $m \in \mathbb{Z}_p^*$. $\mathcal{B}$ computes $S_m = K_m^{1/\beta}$ and returns the extracted signature (r_m, S_m) to $\mathcal{A}$.

Note that $\mathcal{A}$ must previously have made a verifiably encrypted signing query at m, since otherwise we could use it to break the unforgeability of $\mathcal{GVES}$.

Output. Finally, algorithm $\mathcal{A}$ outputs a valid Gentry signature (r^*,S^*) on a message m^*; it must not have queried its adjudication oracle at m^*.

Since S^* satisfies $e(g_1 g^{-m*}, S^*)e(g,g)^{r*} = e(g, h)$, and by the bilinearity of e, we have $e(g,S^*) = e(g,(hg^{-r*})^{1/(\alpha-m*)})$. By the non-degeneracy, we have $S^* = (hg^{-r*})^{1/(\alpha-m*)}$.

Since $h = g^{f(\alpha)}$, we have $S^* = g^{(f(\alpha)-r*)/(\alpha-m*)}$. Using long division, the rational fraction $(f(\alpha)-r^*)/(\alpha-m^*)$ can be written as

$$(f(\alpha)-r^*)/(\alpha-m^*) = \frac{b_{-1}}{(\alpha-m^*)} + \sum_{i=0}^{q-1} b_i \alpha^i .$$

Since $f(x) \in \mathbb{Z}_p[x]$ is a random polynomial of degree q, the values of b_{-1} appear uniformly random between 0 and $p-1$, and therefore the probability that $b_{-1} = 0$ is $1/p$.

If $b_{-1} = 0$, $\mathcal{B}$ declares failure and exits. Otherwise, $(\alpha-m^*)$ does not divide $(f(\alpha)-r^*)$ and $\mathcal{B}$ computes

$$g^{1/(\alpha-m^*)} = \left(S^* \cdot \prod_{i=0}^{q-1} \left(g^{\alpha^i}\right)^{-b_i}\right)^{1/b_{-1}}.$$

The tuple $(m^*, g^{1/(\alpha-m^*)})$ is the solution to the strong Diffie-Hellman challenge; $\mathcal{B}$ outputs it and halts.

$\mathcal{B}$ thus succeeds with probability $\frac{p-1}{p}\varepsilon$ when $\mathcal{A}$ does with probability ε. Its running time overhead is $O(1)$ for each of $\mathcal{A}$'s verifiably encrypted signing and adjudication queries, and for computing the final output.

5 Efficiency

We compare our verifiably encrypted signature scheme only to these schemes which are proven secure without random oracles. Considering security in the "real world", the verifiably encrypted signature schemes proposed by Boneh, *et al*.[3] and Zhang, *et al*.[4] are not involved here, because both schemes are provably secure only in the random oracles model.

We present the comparisons in Table 1 (optimized by precomputing). For the comparison, we instantiate pairing-based schemes using Barreto-Naehrig curves[13] with 160-bit point representation. The "PK Size" column gives the size of the public keys (the number of Group elements). The "SigSize" column gives verifiably encrypted signature length at the 1024-bit security level. The "VESigGen", "VESigVerify" and "Adjudication" columns give the computational costs of those operations. We denote *Pa* the pairing operation, *E* the exponentiation in $\mathbb{G}$ or $\mathbb{G}_T$, and *k* is the output length of a collision-resistant hash function. We ignore other operations.

Table 1 Comparison of verifiably encrypted signatures without random oracles

Scheme	PKSize	SigSize	VESigGen	VESigVerify	Adjudication
Ref.[7]	3	320 bits	2*E*	2*Pa* + 3*E*	1*E*
Ref.[8]	3	320 bits	3*E*	2*Pa* + 3*E*	1*E*
Ref.[9]	*k* +3	480 bits	4*E*	3*Pa*	1*E*
Ref.[10]	4	320 bits	1*E*	1*Pa* + 3*E*	1*E*
Ours	3	320 bits	2*E*	1*Pa* + 2*E*	1*E*

We note that the computation of the pairing is the most time-consuming. In our scheme, $e(g,g_2)$ and $\mathrm{e}(g,h_2)$ only need to be computed at initialization time and cached, therefore, there is only one pairing operation in VESigVerify phase, which is the same as the one of Ref.[10], while there are two or three pairing operations in other three schemes.

As shown in Table 1, in five existing VES schemes without random oracles, our scheme and the one of Ref.[10] are the best from the view point of the efficiency. However, our scheme has two advantages over the one of Ref.[10]: (1) The one of Ref.[10] is proven secure under joint assumptions that the hardness of *q*-SDH problem and the existence of collision resistant hash functions, but our scheme depends only on *q*-SDH assumption. (2) Our scheme obtains tighter reduction, which allows us to choose a smaller security parameter, adding to the efficiency advantages of our scheme.

6 Conclusions

In this paper, we propose a new verifiably encrypted signature that is fully secure without random oracles. Our construction is based on the Gentry signature and is remarkably simple. Our scheme has several advantages over previous such schemes – namely, shorter public keys, lower computation overhead, and a tighter security reduction, which can be used in practical online contract signing better.

Acknowledgement The authors would like to thank anonymous reviewers for their valuable comments.

References:

[1] Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures. IEEE Journal of Selected Areas in Communication, 2000,18(4):593−610.

[2] Zhou YB, Zhang ZF, Qing SH, Ji QG. A fair exchange protocol based on RSA signature scheme. Journal of Software, 2004,15(7):1049−1055 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1049.htm

[3] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. EUROCRYPT 2003. LNCS 2656, Berlin: Springer-Verlag, 2003. 416−432.

[4] Zhang FG, Safavi R, Susilo W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings. In: Johansson T, Maitra S, eds. Proc. of the Indocrypt 2003. LNCS 2904, Berlin: Springer-Verlag, 2003. 191−204.

[5] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited. Journal of the ACM, 2004,51(4):557−594.

[6] Boneh D, Boyen X. Short signatures without random oracles. In: Cachin C, Camenisch J, eds. EUROCRYPT 2004. LNCS 3027, Berlin: Springer-Verlag, 2004. 56−73.

[7] Gorantla MC, Saxena A. Verifiably encrypted signature scheme without random oracles. In: Chakraborty G, ed. Proc. of the ICDCIT 2005. LNCS 3816, Berlin: Springer-Verlag, 2005. 357−363.

[8] Li XX, Chen KF, Liu SL, Li SQ. Verifiably encrypted signatures without random oracles. Journal of Shanghai Jiaotong University (Science), 2006,E-11(2):230−235.

[9] Lu S, Ostrovsky R, Sahai A, Shacham H, Waters B. Sequential aggregate signatures and multisignatures without random oracles. In: Vaudenay S, ed. Proc. of the EUROCRYPT 2006. LNCS 4004, Berlin: Springer-Verlag, 2006. 465−485.

[10] Ming Y, Wang YM. An efficient verifiably encrypted signature scheme without random oracles. 2006, http://ijns.nchu.edu.tw/paper_upload/IJNS-2006-10-09-1-r.pdf

[11] Gentry C. Practical identity-based encryption without random oracles. In: Vaudenay S, ed. Proc. of the EUROCRYPT 2006. LNCS 4004, Berlin: Springer-Verlag, 2006. 445−464.

[12] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Proc. of the CRYPTO 2001. LNCS 2139, Berlin: Springer-Verlag, 2001. 213−229.

[13] Barreto PSLM, Naehrig M. Pairing-Friendly elliptic curves of prime order. Cryptology ePrint Archive, 2005/133. 2005, http://eprint.iacr.org/

附中文参考文献:

[2] 周永彬,张振峰,卿斯汉,季庆光.基于 RSA 签名的优化公平交换协议.软件学报,2004,15(7):1049−1055.http://www.jos.org.cn/1000-9825/15/1049.htm

YANG Hao-Miao was born in 1974. He is a Ph.D. candidate at the University of Electronic Science and Technology of China. His current research areas are cryptographic algorithms and information security.

XU Ji-You was born in 1971. He is a Ph.D. candidate at the University of Electronic Science and Technology of China. His current research areas are cryptographic algorithms and information security.

SUN Shi-Xin was born in 1940. He is a professor and Ph.D. supervisor at the University of Electronic Science and Technology of China. His research areas are combination algorithms, grid computing and cryptographic algorithms.