# Cryptanalysis and Fixed of Short Signature Scheme without Random Oracle from Bilinear Parings

Mingwu Zhang[1,2,3], Bo Yang[1], Yusheng Zhong[1], Pengcheng Li[1], Tsuyoshi Takagi[3]
*(Corresponding author: Mingwu Zhang)*

College of Informatics, South China Agricultural University[1]
No.383, Wushan Rd., Tianhe District, Guangzhou 510642, China

National Laboratory for Modern Communications, Chengdu 610041, China[2]
Graduate School of Mathematics, Kyushu University[3]
744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan

*(Received Nov. 1, 2009; revised and accepted Apr. 13, 2010)*

## Abstract

We first analyze the security of a short signature scheme without random oracles called ZCSM scheme and point out that it cannot support unforgeable under the chosen message and public key attacks. We also propose a new signature scheme without random oracle using bilinear pairing that is existentially unforgeable under a chosen message attack. The security of the proposed scheme depends on a complexity assumption called the $k$+1 square roots inverse assumption. The proposed scheme has the same signature length with the previous short signature scheme where it fixes the ZCSM scheme's deficiency.

*Keywords: Bilinear pairing, signature, standard model, unforgeability*

## 1 Introduction

Recently, many signature schemes using the bilinear pairings without random oracles have been proposed that are efficient and at the same provable security in the standard model [2, 8, 13, 15, 17, 18]. Short digital signatures [3, 4, 12, 16] are always desirable that can deploy in some situation where people need to enter the signature manually, such as using a PDA that is not equipped with a keyboard and RFID that has poor computing capability. Additionally, short digital signatures are essential to ensure the authenticity of messages in low-bandwidth communication channels such as Wireless Sensor Network (WSN) and Ad hocs that support low bandwith transmissions and dynamic communications [6, 10, 11]. In general, short digital signatures are used to reduce the communication complexity of any transmission. Boneh, Lynn and Shacham [4] used a totally new approach to design short digital signatures, referred to as the BLS scheme, is based on the Computational Diffie-Hellman (CDH) assumption on elliptic curves with low embedding degree. The BLS scheme is provable security in the random oracles model. Although the model is efficient and useful, it has received a lot of criticism that the proofs in the random oracle model are not proofs at all. In BLS signature scheme, with a signature length $l$ = 160 bits which is approximately half the size of DSS signatures and only 16.6% size of the RSA signature with the same security level, it provides a security level of approximately $O(280)$ in the random oracle model. In Table 1, it lists several signatures size comparison with the same security levels such as BLS, DSS and RSA etc.

Table 1: Signature size under the same security level

| Schemes | BLS | DSS | RSA |
|---|---|---|---|
| Size | 160 bits | 320 bits | 1024 bits |

Camenisch and Lysyanskaya [5] and Fischlin [7] constructed two provably secure signature schemes under the strong RSA assumption in the standard model, repectively. Boneh and Boyen [1] proposed a short signature scheme without using random oracles from bilinear groups which is fully secure with the support of existentially unforgeable under a chosen message attack where its security reduces to $q$-strong Diffie-Hellman (q-SDH) assumption that is a stronger assumption compared with the standard computational Diffie-Hellman (CDH) assumption. Furthermore, their construction is too inefficient to be of practical use. In [14], Tan pointed that it cannot resist on the strong-key substitution attacks in [1]. Li et al. [9] constructed a short signature in the standard model with a shorter signature size than previous schemes [1, 3], but it needs to introduce two Hashing functions to support random value to another uniformly field element. In [19], Zhang et al. proposed a new signature scheme without random oracle called ZCSM scheme. The security of the ZCSM scheme depends on a new complexity assumption called the $k+1$ square roots assumption. Moreover, the $k+1$ square roots assumption can be used to construct shorter signatures under the random oracle model.

In this paper, we analyze the security of the ZCSM scheme [19] that is an efficient short signature scheme in the standard model from bilinear pairings. We give the forgeable attack to provide that the ZCSM scheme is not secure in unforgeability under the chosen message and public key attacks. We also propose a new signature scheme with bilinear pairing that is existentially unforgeable under a chosen message attack without random oracle. The security of the proposed scheme depends on a new complexity assumption called the k+1 square roots inverse assumption that derived from SDH assumption [1]. The proposed scheme has the same signature length with the ZCSM scheme where it improves and fixes the security requirements.

# 2 Preliminaries and Mathematics Backgrounds

## 2.1 Bilinear Groups and Maps

**Definition 1.** ***(Bilinear maps)*** *A map $\hat{e}: G\times G \to G_T$. $G_T$ is called a bilinear pairing if it satisfies the following properties:*

*1) $G$ and $G_T$ are two multiplicative finite cyclic groups of order $q$.*

*2) $g$ is a generator of $G$, and $\hat{e}(g,g)$ is generator of $G_T$.*

*3) $\hat{e}$ is a bilinear map $\hat{e}: G\times G \to G_T$. In other words, for all $u,v \in G$ and $a,b \in Z_q$, it has $\hat{e}(u^a,v^b) = \hat{e}(u,v)^{ab}$.*

*The bilinear map $\hat{e}$ is commutative such that $\hat{e}(u^a,v^b) = \hat{e}(u^b,v^a) = \hat{e}(v,u)^{ab}$. We say that $G$ is a bilinear group if the group action in $G$ can be computed efficiently and there exists both a group $G_T$ and an efficiently computable bilinear map $\hat{e}: G\times G \to G_T$ as above.*

## 2.2 Constructing Bilinear Groups of a Given Order $q$

Let $q > 3$ be a given square-free integer that is not divisible by 3. We construct a bilinear group $G$ of order $q$ as follows:

1) Find the smallest positive integer $l \in Z$ such that $p = lq - 1$ is prime and $p = 2 \ mod \ 3$ holds.

2) Consider the group of points on the super-singular elliptic curve $y^2 = x^3 + 1$ defined over $\mathcal{F}_p$. Since $p = 2 \ mod \ 3$, the curve has $p + 1 = lq$ points in $\mathcal{F}_p$. Moreover, the group of points on the curve has a subgroup of order $q$ which we denote by $G$.

3) Let $G_T$ be the subgroup of $\mathcal{F}_{p^2}$ of order $q$. The modified Weil pairing on the curve gives a bilinear map $\hat{e}: G \times \mathbb{G} \to G_T$ with the required properties.

For a bilinear maps $\hat{e}: G\times G \to G_T$. We assume we work over a 160-bit elliptic curve group for the discrete-logarithm based scheme. For example, $k = 80$, $|G| = |q| = 160$.

## 2.3 The Hard Problem Assumptions and Security

**Definition 2.** ***(k+1 Square Roots Assumption, k+1-SRP)*** *[19] Given as input an integer $k$, $x \in Z_q$, $g \in G$ and (2k+1)-tuples: $\{\alpha = g^x, h_1, \cdots, h_k \in Z_q, g^{\{x+h_1\}^{1/2}}, \cdots, g^{\{x+h_k\}^{1/2}}\}$, to compute $g^{\{x+h\}^{1/2}} \in G$ for some $h \in \{h_1,\cdots,h_k\}$.*

**Definition 3.** ***(SDH Assumption)*** *[3] Given as input a (q+1)-tuple of elements: $(g, g^x, g^{x^2}, \cdots, g^{x^q}) \in G^{q+1}$, to compute a pair $(c, g^{1/(x+c)}) \in z_q \times G$ for a free chosen value $c \in Z_q \backslash \{-x\}$.*

**Definition 4.** ***(k+1 Square Roots Inverse Assumption, k+1-SRIP)*** *For an integer k, and $x \in Z_q$, $g \in G$, given*

$$\{g, \alpha = g^x, h_1, \cdots, h_k \in Z_q, g^{\overline{\frac{1}{(x+h_1)^{1/2}}}}, \cdots, g^{\overline{\frac{1}{(x+h_k)^{1/2}}}}\},$$

*to compute $g^{\overline{\frac{1}{(x+h)^{1/2}}}}$ for some $h \in \{h_1,\cdots,h_k\}$.*

Let $\Omega$ be a $k$+1-SRIP parameter generator. We say that an algorithm $\mathcal{B}$ has the advantage $Adv_{\Omega,\mathcal{B}}(k)$ in solving the $k+1$-SRIP problem for $\Omega$ in time $t(k)$ if for sufficiently large parameter $k$. We have

$$\begin{aligned} Adv_{\Omega,B}^{k+1-SRIP}(k) &= Pr[\mathcal{B}(g, \alpha = g^x, h_1, \cdots, \\ &\quad h_k \in Z_q, g^{\overline{\frac{1}{(x+h_1)^{1/2}}}}, \cdots, \\ &\quad g^{\overline{\frac{1}{(x+h_k)^{1/2}}}} | x \in_R Z_q, g \in G, \\ &\quad h_1, \cdots, h_k \in Z_q) = g^{\overline{\frac{1}{(x+h)^{1/2}}}}, \\ &\quad h \in \{h_1, \cdots, h_k\}] < \epsilon, \end{aligned}$$

where $\epsilon$ is negligible.

**Definition 5.** ***Unforgeability.*** *A forger $\mathcal{A}$ is said to $(t, q_S, \epsilon)$-break a signature scheme if $\mathcal{A}$ runs in time at most $t$, makes at most $q_S$ signature queries, and $Sign_{Adv}(\mathcal{A})$ is at least $\epsilon$. A signature scheme is $(t, q_S, \epsilon)$-strongly existentially unforgeable under an adaptive chosen message attack if there exists no forger that $(t, q_S, \epsilon)$-breaks it.*

We note that the definition above captures a stronger version of existential unforgeability than the standard one, as it requires that the adversary cannot even generate a new signature on a previously signed message.

# 3 Construction of ZCSM Signature without Random Oracles

The ZCSM scheme [19] is described as follows.

**Setup.** Picks out a bilinear group and map tuples $(G, G_T, \hat{e}, g, q)$ with generator $g$. It assumes that $q \equiv 3 \bmod 4$ which statisfies $-1$ is a non-quadratic residue modulo $q$. The message space $\mathcal{M} = \{1, \cdots, (q-1)/2\}$. For any message $m \in \mathcal{M}$, if $m$ is not a quadratic residue modulo $q$, then $q - m$ or $-m$ will be a quadratic residue modulo $q$. The system parameters are $(G, G_T, \hat{e}, q, g)$.

**Key Generation.** Randomly picks $x, y \in_R Z_q$, computes $u = g^x$, $v = g^y$. The secret key is $(x, y)$ and the public key is $(u, v)$.

**Sign.** Given a message $m \in \mathcal{M}$, a user with secret key $(x, y)$ generates a signature as follows:
First, randomly picks $r \in_R Z_q$;
If $m$ is a quadratic residue modulo $q$, computes

$$\sigma = g^{(x+my+r)^{1/2} \bmod q}.$$

Otherwise, if $m$ is a non-quadratic residue modulo $q$, then computes

$$\sigma = g^{(x+(-m)y+r)^{1/2} \bmod q}.$$

The signature is $(\sigma, r)$.

**Verify**. Given a public parameters $(G, G_T, q, g)$, public key $(u, v)$, a message $m \in \mathcal{M}$, and a signature $(\sigma, r)$, anyone can verify the validation of the signature $(\sigma, r)$ by the following equation:

$$\hat{e}(\sigma, \sigma) = \hat{e}(uv^m g^r, g)$$

or

$$\hat{e}(\sigma, \sigma) = \hat{e}(uv^{-m} g^r, g).$$

# 4 Forgery Attacks

In this section, we describe the two attack models on the ZCSM scheme to point out that the ZCSM scheme cannot against unforgeability by signature forgery attack. One is signature forgeability attack, and the other is strong key replacement attack.

## 4.1 Signature Forgery

When obtained a valid signature $(\sigma, r)$, it easy to forge a new signature by setting signature $(\sigma', r')$ as

$$(\sigma', r') = (\sigma^2, 2r).$$

Anyone can verify the valid of the signature $(\sigma', r')$ for the forged public key $(u', v') = (u^2, v^2) = (g^{2x}, g^{2y})$ by the verify algorithm:

$$\begin{aligned} \hat{e}(\sigma', \sigma') &= \hat{e}(g^{x+my+r}, g^{x+my+r}) \\ &= \hat{e}(g^{2x} g^{2my} g^{2r}, g) \\ &= \hat{e}(u' v'^m g^{r'}, g). \end{aligned}$$

## 4.2 Strong Key Replacement Attack

After given a message $m$'s signature $(\sigma, r)$ signed by Alice, attacker $\mathcal{A}$ forges a valid public key by

- Randomly picks $v' \in_R G$;
- Computes $u' = u(v/v')^m$.

It easy sees that $(u', v')$ is a valid public key. The signature $(\sigma, r)$ can be verified as valid for public key $(u', v')$ as

$$\begin{aligned} \hat{e}(u' v'^m g^r, g) &= \hat{e}(u(v/v')^m \cdot v'^m g^r, g) \\ &= \hat{e}(uv^m g^r, g) \\ &= \hat{e}(\sigma, \sigma). \end{aligned}$$

Attacker $\mathcal{A}$ can replace Alice's public key with $(u', v')$, which may be the public key of Bob's. So, the signature $(\sigma, r)$ can be considered for Bob's signature by strong key replacement attack.

# 5 Fixed and Improved Scheme

We now improve and fix a security short signature scheme in the standard model using the (k+1)-SRIP assumption that derived from SDH assumption. We also assume that the message $m$ to be signed are elements in $Z_q$, the domain can be extended to all $\{0,1\}^*$ by using collision resistant hash function.

**Setup.** Let $G$ and $G_T$ be two cyclic groups of prime order $q$, $g$ be a generator of $G$ and $\hat{e}$ be an efficiently computable bilinear map from $G \times G$ into $G_T$. It assumes that $q \equiv 3 \bmod 4$ which satisfies $-1$ is a non-quadratic residue modulo $q$. The message space $\mathcal{M} = \{1, \cdots, (q-1)/2\}$. For any message $m \in \mathcal{M}$, if $m$ is not a quadratic residue modulo $q$, then $q - m$ or $-m$ will be a quadratic residue modulo $q$. Let $z = \hat{e}(g, g)$. The system parameters are $(G, G_T, g, \hat{e}, q, z)$, together with the message space $\mathcal{M}$ and the signature space $\mathcal{C}$.

**KeyGen.** Randomly selects $x, y \in_R Z_q$, computes $u = g^x \in G$ and $v = g^y \in G$. The the secret key is $(x, y)$ and the public key is $(u, v)$.

**Sign.** Given a message $m \in \mathcal{M}$, a user with secret key $(x, y)$ produces a signature as follows:

- First, randomly picks a $r \in_R Z_q$;

- If $m$ is a quadratic residue modulo $q$, compute

$$\sigma = g^{\frac{1}{\sqrt{x+my+r}}} \bmod q.$$

- Otherwise, if $m$ is a non-quadratic residue modulo $q$, then compute:

$$\sigma = g^{\frac{1}{\sqrt{x+(-m)y+r}}} \bmod q$$

The signature is $(\sigma, r)$.

**Verify.** Upon receipt of public parameters ($G$, $G_T$, $g$, $q$, $z$), public key $(u, v)$, a message $m \in \mathcal{M}$, and a signature $(\sigma, r)$, anyone can verify the validation of the signature by the following equations:

$$\hat{e}(\sigma^2, ug^m v^r) = z \qquad (1)$$

or

$$\hat{e}(\sigma^2, ug^{-m} v^r) = z. \qquad (2)$$

If either equation Equation (1) or Equation (2) holds, it outputs valid. Otherwise, it outputs invalid.

It's obvious that the signature size is the same as the ZCSM's, but the computation cost in Verify algorithm is more efficient for that it needs only one pairing computation.

A signature pair generated by the signing procedure verifies as valid under the corresponding public key. Indeed, it has

$$\begin{aligned}
\hat{e}(\sigma^2, ug^{\pm m} v^r) &= \hat{e}(g^{\frac{1}{x \pm my + r}}, ug^{\pm m} v^r) \\
&= \hat{e}(g^{\frac{1}{x \pm my + r}}, g^x g^{\pm my} g^r) \\
&= \hat{e}(g, g) \\
&= z.
\end{aligned}$$

# 6 Security and Performance Analysis

## 6.1 Signature Size

Let $(G, G_T)$ be bilinear group where $|G| = |G_T| = q$ for some prime $p$. A signature $(\sigma, r)$ which each element of signature approximately $log_2 q$-bits when embedded degree $k = 6$ and the modified Weil pairing or Tate pairing, therefore the total signature length is approximately $2log_2 q$. If it instantiates the pairing using elliptic curves, the signature length is approximately the same as DSA signature with the same security where the proposed scheme is provable security under the standard model.

We can select the parameter such that the elements in G are 171-bit strings. A possible choice of these parameters can be from Boneh et al.'s BLS short signature scheme. Therefore, at the current security requirement, we can obtain a signature whose length is approximately the same as a DSA signature with the same level of security, but which is provably secure and existentially unforgeable under a chosen message attack without the random oracle model. It keeps the same signature length with ZCSM scheme, where it improves security to reinforces the forgeability attack under chosen message attacks and chosen public key attacks, and reduce the Verify algorithm time.

## 6.2 Computation Cost

The improved signature scheme requires one computation of square root in $Z_q$ and one exponentiation in $G$ for Sign algorithm. For the verification, it requires only one paring and three exponentiations in $G$, which has more computational efficient than ZCSM scheme that needs two pairings computations and two exponentiations in Verify algorithm for that $z$ can be greatly accelerated with a moderate amount of reusable pre-computation in our scheme.

Key generation times are comparable to the BLS scheme [4]. Signature times are much faster than BLS, by up to an order of magnitude, because our signing algorithm only makes one exponentiation to the fixed base $g$, and this can be greatly accelerated with a moderate amount of reusable pre-computation. Verification times are also faster than BLS since verification requires only one pairing and two multi-exponentiation, instead of two pairing computations in BLS. Since exponentiation tends to be faster than pairing, signature verification is faster than in the BLS system. Compared with the BB04 scheme [1], this is the second short signature scheme without random oracles. In Table 2, it lists the comparison of the security and performance about related signature schemes.

## 6.3 Security

**Theorem 1.** *Suppose the $(q, t', \epsilon')$-(k+1)SRIP assumption holds in $(G, G_T)$, then the signature scheme above is $(t, q_s, \epsilon)$-secure against strong existential forgery under an adaptive chosen message attack such that*

$$q_s < q, \epsilon \approx 2\epsilon'.$$

*Proof.* Assume a forger $\mathcal{F}$ with $(t, q_s, \epsilon)$ advantage breaks the signature scheme. We construct an algorithm $\mathcal{A}$ to solve the SRIP problem by interacting with $\mathcal{F}$.

Before describing the algorithm $\mathcal{B}$, we distinguish between two types of forgers that $\mathcal{A}$ can emulate. Let $(G, G_T, q, g, \hat{e}, u, v, z)$ be the public key given to $\mathcal{A}$, where $u = g^x$ and $v = g^y$. Let $h_i = m_i y + r_i$ be the k+1-SRIP input, and let $(m^*, r^*, \sigma^*)$ be the forgery produced by $\mathcal{A}$. There are two types of forgers $\mathcal{A}$ as:

- Type-I forger: (1) He makes a signature query for the message $m = -x$, or (2) He outputs a forgery where $m^* + yr^* \notin \{h_1, \cdots, h_{q_s}\}$;

Table 2: Comparison of security, signature sizes and computing costs

| Schemes | Security Model | Unforgeability | Signature Size | Sign Cost | Verify Cost |
|---|---|---|---|---|---|
| Ours | Standard | Yes | $\|G\| + \|Z_q\|$ | 1Exp+1Sr | 1Pr+3Mp |
| [4] | ROM | Yes | $\|G\|$ | 1Sr | 2Pr |
| [19] | Standard | No | $\|G\| + \|Z_q\|$ | 1Exp+1Sr | 2Pr+2Mp |
| [1] | Standard | Yes | $\|G\| + \|Z_q\|$ | 1Exp | 1Pr+3Mp |
| [17] | Standard | Yes | $2\|G\|$ | 2Exp+1Sr | 3Pr+1Mp |

Exp: exponentiation in G; Sr: square root in $Z_q$;
Mp: multiple in G; Pr: pairing computation of $\hat{e}$.

- Type-II forger: (1) He never makes a signature query for the message $m = -x$, and (2) He outputs a forgery where $m^* + yr^* = h_i$ for some $i \in \{1, \cdots, q_s\}$.

**Setup.** Algorithm $\mathcal{B}$ first selects a list of $q_s$ random messages $h_1, \cdots, h_{q_s} \in Z_q$ and sets $s_i = g^{(x+h_i)^{-1/2}} \in G$, and sends them to the challenger. The challenger responds with a valid public key $(g, u, v, z)$ and a list of $q_s$ signatures $\sigma_1, \cdots, \sigma_{q_s}$ on these messages. If some $\sigma_i = 1 \in G$, then $\mathcal{B}$ just learned the challenger's private key, $x = -m_i$, which it can then use to produce a valid forgery. Otherwise, we know that all $m_i$ are uniform in $Z_q \backslash \{-x\}$ and that $e(\sigma_i^2, ug^{m_i}v^{r_i}) = \hat{e}(g, g) = z$ for $i = 1, \cdots, q_s$. To proceed, $\mathcal{B}$ first sets $\alpha = g^x$, and then picks a random $y \in Z_q$ and gives to $\mathcal{A}$ the public key $PK_1 = (g, u, v, z) = (g, \alpha, g^y, z)$ for Mode I. Otherwise, he gives the public key $PK_2 = (g, u, v, z) = (g, g^y, \alpha, z)$ to $\mathcal{A}$ under Mode II. It easy sees that $PK_1$ and $PK_2$ are valid public keys for forger $\mathcal{F}$.

**Queries.** The forger $\mathcal{A}$ issues $q_s$ signature queries in an adaptive fashion. In order to respond, $\mathcal{B}$ maintains a query counter $\ell$ which is initially set to empty.

- For Mode I, upon receiving a signature query for $m \in Z_p$, the simulator $\mathcal{B}$ increments $\ell$ by one, sets $r_\ell = (h_\ell - my) \in Z_q$, and gives $\mathcal{A}$ the signature $(\sigma_\ell, r_\ell)$. We claim that $(\sigma_\ell, r_\ell)$ is a valid signature on $m$ under $PK_1$. First, $r_\ell$ is uniform in $Z_q \backslash \{-(x + my)\}$ for that $r_\ell$ is uniform in $Z_q \backslash \{-x\}$.

  $$\hat{e}(\sigma_\ell^2, ug^m v^{r_\ell}) = \hat{e}(g, g) = z$$

  as required. The reason this works is that $\mathcal{B}$ chooses an $r_\ell$ such that $m_\ell + yr_\ell = h_\ell$, and we also set $m_\ell = m$.

- For Mode II, $\mathcal{B}$ sets $r_\ell = mh_\ell - y$ and return tuples $(r_\ell, \sigma_\ell = s_\ell^{m^{-1/2}})$ if $m$ is a quadratic residue modulo $q$ (If $m$ is a non-quadratic residue modulo $q$, the tuples are $(r_\ell, \sigma_\ell = s_\ell^{(-m)^{-1/2}})$). This is a valid signature on $m$ for $PK_2$ because $r_\ell$ is uniform in $Z_q$ and

  $$\begin{aligned} \hat{e}(\sigma_\ell^2, ug^m v^{r_\ell}) &= \hat{e}((g^{(x+h_i)^{1/2} m^{-1/2}})^2, ug^m v^{r_\ell}) \\ &= \hat{e}(g^{(x+h_i)} g^{1/m}, ug^m v^{mh_i - y}) \\ &= \hat{e}(g^{(x+h_i)}, uv^{mh_i - y}) \\ &= z. \end{aligned}$$

  A forger may issue a signature query for $m \in Z_q$ where $m = -x$. If this ever happens then $\mathcal{B}$ can obtain the private key for the public key $(g, u, v, z)$ it was given. This allows $\mathcal{B}$ to forge the signature on any message of its choice without further interaction with $\mathcal{A}$. It terminates the simulation and wins the game.

**Output.** Eventually, suppose $\mathcal{A}$ returns a forgery $(m^*, \sigma^*, r^*)$, where $(\sigma^*, r^*)$ is a valid forgery distinct from any previously given signature on message $m^*$.

Let $m_\ell = m^* + yr^*$. It shows that $(m^*, \sigma^*)$ is a valid message/signature pair in the basic signature scheme. Furthermore, the pair is a valid existential forgery for a forger that it has $m^* \in \{m_1, \cdots, m_{q_s}\}$.

If $u = g^{m^*}$, then $\mathcal{B}$ has already recovered the secret key of its of its challenger, $\mathcal{B}$ can forge a signature on any message of his choice. We assume that $\mathcal{A}$ produced a type-I forgery $(m^*, r^*, \sigma^*)$. Let $h = m^*y + r^*$, the forgery $(m^*, r^*, \sigma^*)$ solves the $q_s$-SRIP problem.

Otherwise, since $v = \alpha = g^x$, then we know that there exists a pair $v^{m_\ell} g^{r_\ell} = v^{m^*} g^{r^*}$, $\mathcal{B}$ can compute $x = (r_\ell - r^*)/(m^* - m_\ell)$ to recover the challenger's private key and forge a signature for any chosen message.

It is easy to see that, if the forger $\mathcal{A}$ outputs a valid forgery with probability $\epsilon$ in time $t$, then the reduction $\mathcal{B}$ succeeds in time $t' \approx t$ with the same probability $\epsilon$.

□

## 7 Conclusion

We analyzed the security of a short signature scheme called ZCSM scheme in the standard model and pointed out that it cannot resist on the unforgeable attack. Furthermore, we improved and fixed the ZCSM scheme to provide existentially unforgeable under a chosen message attack without using random oracles. The proposed scheme has the same signature length to the ZCSM scheme where it is more efficient than previous schemes.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant 60773175 and 60973134, the Foundation of National Laboratory for Modern Communications under Grant 9140c1108020906, the Natural Science Foundation of Guangdong Province under Grants 10151064201000028 and 10351806001000000, the Foundation for Distinguished Young Talents in Higher Education of Guangdong(wym09066), and the Support of JSPS Postdoctoral Fellowship, Japan.

## References

[1] D. Boneh and X. Boyen, "Short signatures without random oracles", *Advances in Cryptology (Eurocrypt 2004)*, LNCS 3027, pp. 56-73, Springer-Verlag, 2004.

[2] D. Boneh, X. Boyen, H. Shacham, "Short group signatures", *Advances in Cryptology (CRYPTO 2004)*, LNCS 3152, pp. 41-55, Springer-Verlag, 2004.

[3] D. Boneh, X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups", *Journal of Cryptology*, vol. 21, pp. 149-177, 2008.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing", *Advances in Cryptology (Asiacrypt 2001)*, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[5] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps", *Advances in Cryptology (Crypto 2004)*, LNCS 3152, pp. 56-72, Springer-Verlag, 2004.

[6] F. Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," *International Journal of Network Security*, vol. 7, no. 1, pp. 61-68, 2008.

[7] M. Fischlin, "The cramer-shoup strong - RSA signature scheme revisited", *PKC 2003*, LNCS 2567, pp. 116-129, Springer-Verlag, 2003.

[8] F. Guo, Y. Mu, Z. Chen, "Efficient batch verification of short signatures for a single-signer setting without random oracles", *Advances in Information and Computer Security*, LNCS 5312, pp. 49-63, 2008.

[9] L. Kang, X. Tang, X. Lu, et al., "A short signature scheme in the standard model", *Cryptology ePrint Archive*, Report 2007/398, 2007.

[10] T. Landstra, S. Jagannathan, and M. Zawodniok, "Energy-efficient hybrid key management protocol for wireless sensor networks," *International Journal of Network Security*, vol. 9, no. 2, pp. 121-134, 2009.

[11] A. Mohaisen, D. Nyang, and K. Lee, "Hierarchical grid-based pairwise key pre-distribution in wireless sensor networks," *International Journal of Network Security*, vol. 8, no. 3, pp. 282-292, 2009.

[12] A. N. Moldovyan, "Short signatures from difficulty of factorization problem", *International Journal of Network Security*, vol. 8, no. 1, pp. 90-95, Jan. 2009.

[13] H. Shacham, B. Waters, "Efficient ring signatures without random oracles", *PKC 2007*, LNCS 4450, pp. 166-180, 2007.

[14] C. H. Tan, "Key substitution attacks on provably secure short signature schemes", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88-A, no. 2, pp. 611-612, 2005.

[15] C. H. Tan, "A new signature scheme without random oracles", *International Journal of Security and Networks*, vol. 1, no. 3-4, pp. 237-242, 2006.

[16] R. Tso, T. Okamoto, E. Okamoto, "Efficient short signatures from pairing," *2009 Sixth International Conference on Information Technology: New Generations (ITNG' 09)*, pp. 417-422, 2009.

[17] B. Waters, "Efficient identity-based encryption without random oracles", *EuroCrypt2005*, LNCS 3494, pp.114-127, 2005.

[18] F. Zhang, X. Chen, Y. Mu, and W. Susilo, "A new and efficient signature on commitment values", *International Journal of Network Security*, vol. 7, no. 1, pp. 100-105, July 2008.

[19] F. Zhang, X. Chen, W. Susilo, and Y. Mu, "A new signature scheme without random oracles from bilinear pairings", *VietCrypt 2006*, LNCS 4341, pp. 67-80, 2006.

**Mingwu Zhang** is an associate professor at South China Agricultural University, and current a Postdoctoral fellow at Kyushu University in Japan supported by JSPS. He received his M.S. in computer science and engineering from Hubei Polytechnic University in 2000, and the Ph.D degree in South China Agricultural University in 2009, respectively. He is a senior member of Chinese Computer Federation (CCF), a senior member of Chinese Association for Cryptologic Research(CACR), and a member of IEEE Computer Society. He now serves for the organization committee chair for JWIS2010. His research interests include network and information security, trusted and secure computing (E-mail: csmwzhang@gmail.com).

**Bo Yang** received his B. S. degree from Peking University in 1986, and the M. S. and Ph. D. degrees from Xidian University in 1993 and 1999, respectively. From July 1986 to July 2005 he had been at Xidian University, from 2002, he had been a professor of National Key Lab. of ISN in Xidian University, supervisor of Ph.D. He had served as a Program Chair for the CCICS2005, and ChinaCrypt2009. He severed the co-Chair of JWIS2010. He is currently a professor and supervisor of Ph.D. at College of Information, South China Agricultural

University. He is a senior member of Chinese Institute of Electronics (CIE), a member of specialist group on information security in Ministry of Information Industry of China and a member of specialist group on computer network and information security in Shanxi Province. His research interests include information theory and cryptography (E-mail: byang@scau.edu.cn)

**Yusheng Zhong** is now a doctoral student in South China Agricultural University. His research interests include distributed network, information security, and trusted computing (E-mail: zhongyusheng3000@163.com).

**Pengcheng Li** pursues his M. Sc. in South China Agricultural University. His research interests include distributed network, information security, and trusted computing (E-mail: lipengcheng7@yahoo.com.cn).

**Tsuyoshi Takagi** received his B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He had engaged in the research on network security at NTT Laboratories from 1995 to 2001. He received the Dr.rer.nat degree from Technische University Darmstadt in 2001. He was an Assistant Professor in the Department of Computer Science at Technische University Darmstadt until 2005, and a Professor at the School of Systems Information Science in Future University-Hakodate, Japan until 2009. He is currently a Professor in Graduate School of Mathematics, Kyushu University. His current research interests are information security and cryptography. Dr. Takagi is a memeber of International Association for Cryptologic Research (IACR).