Efficient and Forward-Secure Identity-Based Signcryption

Noel McCullagh[1*] and Paulo S. L. M. Barreto[2]

[1] School of Computer Applications
Dublin City University
Ballymun, Dublin 9, Ireland.
`noel.mccullagh@computing.dcu.ie`

[2] Escola Politécnica, Universidade de São Paulo.
Av. Prof. Luciano Gualberto, tr. 3, 158.
BR 05508-900, São Paulo(SP), Brazil.
`pbarreto@larc.usp.br`

Abstract. Several signcryption schemes proposed in the literature are known to lack semantic security, and semantically secure signcryption schemes tend to be more computationally expensive. In fact, devising an efficient signcryption scheme providing both public verifiability and forward security was until now an open problem. In this paper, we show how a particular kind of signcryption scheme may become completely insecure when implemented with certain efficient instantiations of the Tate or Weil pairing. We also address the drawbacks of the secure schemes by proposing efficient, semantically and forward-secure signcryption schemes, in both transferable and non-transferable form, that can be realised on top of any pairing instantiation. As a bonus, we also derive from them a new, efficient identity-based signature scheme.

1 Introduction

The two fundamental services of public key cryptography (PKC) are encryption and signing. Encryption provides confidentiality as only the intended recipient can recover the plaintext from the ciphertext. Digital signatures provide authentication and non-repudiation. Often when we use one of these services we would like to use also the other, combining the properties of these schemes.

In 1997, Zheng [15] proposed a novel cryptographic primitive which he called signcryption. The idea behind signcryption is to encrypt and sign data in a single operation which has a computational cost less than that of doing both operations sequentially. Proper signcryption schemes provide confidentiality, authentication, and non-repudiation. Non-transferable signcryption (sometimes called authenticryption) schemes provide confidentiality and authentication, although it is often possible to extend such systems to attain non-repudiation with the

* This author wishes to thank Enterprise Ireland for their support with this research under grant IF/2002/0312/N.

recipient's cooperation, at the cost of revealing the plaintext. Like conventional encryption, it must be computationally infeasible to recover the plaintext from the signcrypted message without the recipient's private key; like conventional digital signatures, it must be computationally infeasible to forge signcryption signatures without the sender's private key.

Identity-based signcryption schemes have been proposed as well. Identity-based cryptography is an idea originally proposed in 1984 by Shamir [13]. The idea behind identity-based cryptography is that the senders and receivers in the system use their online identifiers (combined with certain system-wide information) as their public keys. This greatly reduces the problems with key management that have hampered the mass uptake of public key cryptography on a per individual basis.

Identity-based signcryption algorithms include the schemes proposed by Boyen [3], Libert and Quisquater [9], Malone-Lee [10], Nalla and Reddy [11], Sakai and Kasahara [12], Chen and Malone-Lee [5]. Unfortunately, we show that the Sakai-Kasahara scheme, though being among the fastest of these, is not semantically secure, leaking information about the signcrypted message (formally, this means that it does not satisfy the indistinguishability against adaptive chosen ciphertext attacks property). Furthermore, we show that it becomes completely insecure when implemented on top of many popular settings of the Tate or Weil pairing, particularly those settings where the pairings are most efficiently computable. Specifically, we show that under those circumstances the recipient of a signcrypted message can afterward impersonate the sender, and a third party can do the same if the plaintext of any signcrypted message is compromised. This weakness is inherent to an algorithmic detail of the Sakai-Kasahara scheme that could be employed in other schemes, making them equally insecure.

To a lesser extent, semantic insecurity also plagues the Malone-Lee scheme, and the Libert-Quisquater methods have been proposed to remedy this situation. Unfortunately, the properties of public verifiability and forward security are mutually exclusive in the Libert-Quisquater scheme; in fact, Libert and Quisquater [9] leave it as an open problem the task of devising an efficient signcryption scheme providing both public verifiability and forward security.

Our contributions in this paper are the following. First, we define the concept of projection attacks, which imposes constraints on the family of groups on top of which certain pairing-based schemes can be securely defined. Second, we propose new, efficient, semantically and forward secure signcryption schemes, in transferable and non-transferable form, that do not impose any *a priori* restriction on the pairing settings. The transferable scheme directly addresses — and closes — the open problem posed by Libert and Quisquater. And third, we derive from our signcryption algorithms a new, efficient identity-based signature scheme.

This paper is organised as follows. In section 2 we give the security definition for signcryption schemes. We review the Sakai-Kasahara scheme in section 3, and assess its security deficiencies in section 4. We then describe our new schemes in section 5, both in non-transferable (authenticryption) and transferable forms.

We propose a new identity-based signature scheme in section 6, compare the efficiency of the various schemes in section 7, and draw our conclusions in section 8. We also discuss a curious security properties of the Nalla-Reddy scheme in the appendix.

2 Security Definitions for Signcryption Schemes

We use as our security model the now *de facto* standard for identity-based systems, as defined by Malone-Lee [10]. This is a two-part definition in which he looks at the encryption and unforgeability properties of the signcryption scheme separately. This security model for encryption is called indistinguishability of identity-based signcryptions under chosen ciphertext attack (IND-IDSC-CCA) and is a natural adaptation of the *de facto* standard for public key encryption schemes: indistinguishability of encryptions under chosen ciphertext attack [10].

Definition 1. *We say that an identity-based signcryption scheme (IDSC) has the indistinguishability against adaptive chosen ciphertext attacks property (IND-IDSC-CCA) if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the following game.*

- The challenger $\mathcal{C}$ runs the **Setup** algorithm with a security parameter k and sends the system parameters to the adversary $\mathcal{A}$.
- **Phase 1:** $\mathcal{A}$ performs a polynomially bounded number of the following queries ($\mathcal{A}$ can present its requests adaptively – every request may depend on the answer to the previous ones):
  - **Signcryption query:** $\mathcal{A}$ produces two identities A (sender) and B (receiver), and a plaintext m. $\mathcal{C}$ computes $P_a = \mathbf{Keygen}(A)$ and then $\mathbf{Signcrypt}(m, P_a, B)$ and sends the resulting ciphertext to $\mathcal{A}$.
  - **Unsigncryption query:** $\mathcal{A}$ produces two identities A (sender) and B (receiver), and a ciphertext σ. $\mathcal{C}$ generates the private key $P_b = \mathbf{Keygen}(B)$ and sends the result of $\mathbf{Unsigncrypt}(\sigma, P_b, A)$ to $\mathcal{A}$ (this result can be the $\perp$ symbol if σ is an invalid ciphertext).
  - **Key Extraction query:** $\mathcal{A}$ produces an identity A and receives the extracted private key $P_a = \mathbf{Keygen}(A)$.
- $\mathcal{A}$ chooses two plaintexts m_0 and m_1, and two identities A and B on which he wishes to be challenged. He cannot have asked the private key *(Key Extraction query)* corresponding to A or B in the first stage.
- $\mathcal{C}$ takes a random bit b, computes $\sigma^* = \mathbf{Signcrypt}(m_b, P_a, B)$, and sends σ^* to $\mathcal{A}$.
- **Phase 2:** $\mathcal{A}$ can again perform a polynomially bounded number of queries as in phase 1. This time, $\mathcal{A}$ cannot make a key extraction query on A nor B, nor ask the query $\mathbf{Unsigncrypt}(A, B, \sigma^*)$.
- Finally, $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.

The adversary's advantage is defined to be $Adv(\mathcal{A}) = |\text{Prob}(b' = b) - 1/2|$.

Definition 2. *An identity-based signcryption scheme (IDSC) is said to be secure against an existential forgery for adaptive chosen messages attacks (EF-IDSC-ACMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

- The challenger $\mathcal{C}$ runs the **Setup** algorithm with a security parameter k and gives the system parameters to the adversary $\mathcal{A}$.
- The adversary performs a polynomially bounded number of requests as in the definition above — Key Extraction queries, Signcryption queries and Unsigncryption queries.
- Finally, $\mathcal{A}$ produces a new triple (σ, A, B) (i.e. a triple that was not produced by the signcryption oracle), and the private key of A was not asked. $\mathcal{A}$ wins the game if the result of **Unsigncrypt**(σ, P_a, B) is not the symbol $\perp$. This is the definition of *success* in the above game.

In this definition, the adversary is allowed to ask for the private key corresponding to the identity B for which the ciphertext he produces must be valid. This condition is necessary to obtain the non-repudiation property and to prevent a dishonest recipient from sending a ciphertext to himself on Alice's behalf and trying to convince a third party that Alice was the sender.

The adversary's advantage is $Adv(\mathcal{A}) = |\text{Prob}(success)|$.

3 The Sakai-Kasahara scheme

As a general setting, we use co-gap notation with the conventional Tate pairing $e : \langle P\rangle \times \langle Q\rangle \to \mu_r$, where $\langle P\rangle \subseteq E(F_q)[r]$, $\langle Q\rangle \subseteq E(F_{q^k})$, $\mu_r \subseteq \mathbb{F}_{q^k}^*$ is the set of r-th roots of unity in $\mathbb{F}_{q^k}$, $\gcd(k, r) = 1$, and P and Q are linearly independent. As a consequence, in this notation each user has two key pairs, corresponding to the two groups $\langle P\rangle$ and $\langle Q\rangle$. If a distortion map $\psi : \langle P\rangle \to \langle Q\rangle$ is available, as is the case for supersingular curves and certain classes of ordinary curves [7], one might consider collapsing the groups $\langle P\rangle$ and $\langle Q\rangle$ by using the modified Tate pairing $\hat{e} : \langle P\rangle \times \langle P\rangle \to \mu_r$ given by $\hat{e}(U, V) = e(U, \psi(V))$. However, contrary to other methods the Sakai-Kasahara algorithm depends essentially on the availability of a pairing $e : \mathbb{G} \times \mathbb{G} \to \mu_r$ where $\mathbb{G}$ contains two distinct subgroups $\langle P\rangle$ and $\langle Q\rangle$.

In the following we use an assortment of publicly known random oracles:

- $\mathcal{H}_P : \{0,1\}^* \to \langle P\rangle$,
- $\mathcal{H}_Q : \{0,1\}^* \to \langle Q\rangle$,
- $\mathcal{H}_0 : \{0,1\}^* \to \mathbb{Z}_r^*$,
- $\mathcal{H}_1 : \mu_r \to \{0,1\}^*$,
- $\mathcal{H}_2 : \mu_r \times \{0,1\}^* \to \mathbb{Z}_r^*$,
- $\mathcal{H}'_2 : \langle P\rangle \times \{0,1\}^* \to \mathbb{Z}_r^*$,
- $\mathcal{H}_3 : \langle P\rangle \times \mu_r \times \{0,1\}^* \to \mathbb{Z}_r^*$.
- $\mathcal{H}'_3 : \langle P\rangle \times \langle P\rangle \times \{0,1\}^* \to \mathbb{Z}_r^*$,

Furthermore, all existing identity-based signcryption schemes depend on the existence of a Key Generation Centre (KGC) responsible for issuing private keys corresponding to public identities. Assuming that a KGC is available, the Saka-Kasahara scheme works as follows.

– **Setup:** The KGC generates a random secret polynomial $s(x) = \sum_{i=0}^{d} s_i x^i \in \mathbb{Z}_r[x]$ which acts as its private master key. The simplest choice is $d = 1$, $s_1 = 1$, so the secret key reduces to the single $\mathbb{Z}_r^*$ value s_0. The KGC publishes the points P, Q, $g = e(P, Q)$, and $s_i Q$ for $i = 0, \ldots, d$.
– **Keygen:** A user identity is a public element $u \in \mathbb{Z}_r^*$. The KGC computes a user's private key as $P_u = s(u)^{-1}P$, where the inverse is computed modulo r. The corresponding public key can be (publicly) computed from u and the points $s_i Q$ as $Q_u = \sum_{i=0}^{d} u^i(s_i Q) = s(u)Q$. Let Alice's identity be a and Bob's identity be b.
– **Signcrypt:** To signcrypt a message m to Bob, Alice generates a random integer $x \in \mathbb{Z}_r^*$ and computes:

$$\begin{aligned} R &\leftarrow g^x \\ h &\leftarrow \mathcal{H}_0(m) \\ c &\leftarrow \mathcal{H}_1(R^{1+h}) \oplus m \\ S &\leftarrow x(hP_{sa} + Q_b) \end{aligned}$$

The signcrypted message is (c, S).
– **Unsigncrypt:** Upon reception of the above pair, Bob computes:

$$\begin{aligned} R &\leftarrow e(P_b, S) \\ W &\leftarrow e(S, Q_{sa}) \\ m &\leftarrow \mathcal{H}_1(RW) \oplus c \\ h &\leftarrow \mathcal{H}_0(m) \end{aligned}$$

Bob then verifies that $W = R^h$.

Other identity-based signcryption and authenticryption schemes have been proposed in the literature. We include a summary of the associated computational costs in section 7, covering the above scheme plus those of Boyen [3], Libert-Quisquater [9], Malone-Lee [10], Nalla-Reddy [11], and Chen-Malone-Lee [5].

4 Security problems in the Sakai-Kasahara scheme

4.1 Information leak

The Sakai-Kasahara scheme makes it possible to distinguish between a number of possible plaintexts given only the ciphertext, the public identity of the sender, and the KGC's public key. This also happens in Malone-Lee's scheme, as pointed out by Libert and Quisquater [9].

The attack we now describe against Sakai-Kasahara is a modification of the Libert-Quisquater attack against Malone-Lee's scheme and proceeds as follows. The ciphertext is (c, S). We assume that Carol knows that the plaintext Alice sent to Bob is one of the messages in a set $\{m_i \mid i = 1, \ldots, n\}$. Carol computes $W \leftarrow e(S, Q_a)$ and then, for each $i = 1, \ldots, n$:

$$h_i \leftarrow \mathcal{H}_0(m_i)$$
$$R_i \leftarrow W^{h_i^{-1} \bmod r}$$

until one value of i is found that makes $\mathcal{H}_1(R_i W) \oplus m_i = c$ actually hold. Therefore, the Sakai-Kasahara does not satisfy the IND-IDSC-CCA property.

4.2 Projection attacks

The original description of the Sakai-Kasahara scheme does not impose any restriction upon the groups over which it is defined, assuming only the existence of a bilinear, non-degenerate, efficiently computable pairing on those groups.

As it turns out, the group choice seriously affects the security of the Sakai-Kasahara scheme, in the sense that the scheme structure implicitly uses the relationship between $\langle P \rangle$ and $\langle Q \rangle$ for the security purpose of concealing the signer's private key. In particular, when implemented on a large class of groups where the Tate or Weil pairing is especially efficient, it allows the recipient of a signcrypted message to obtain sufficient information to impersonate the sender, as we show next.

Definition 3. *The* Frobenius endomorphism *is the mapping* $\Phi : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$, $(X, Y) \mapsto (X^q, Y^q)$.

Definition 4. *The* trace map *is the mapping* $\mathrm{tr} : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$ *defined as* $\mathrm{tr}(P) = P + \Phi(P) + \Phi^2(P) + \cdots + \Phi^{k-1}(P)$.

We see that $\mathrm{tr}(\Phi(P)) = \Phi(\mathrm{tr}(P)) = \mathrm{tr}(P)$ for any $P \in E(\mathbb{F}_{q^k})$; this shows that the range of the trace map is indeed $E(\mathbb{F}_q)$.

Definition 5. *The* trace-zero subgroup *or* trace kernel *is the subgroup* $\mathcal{T} = \{Q \in E(\mathbb{F}_{q^k}) \mid \mathrm{tr}(Q) = O\}$.

The following maps:

$$\pi_0 : E(\mathbb{F}_{q^k}) \to \mathcal{T},\ \pi_0(Q) = Q - k^{-1}\,\mathrm{tr}(Q),$$
$$\pi_1 : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q),\ \pi_1(P) = k^{-1}\,\mathrm{tr}(P),$$

where k^{-1} is computed modulo r, satisfy $\pi_0(Q) = Q$ for any $Q \in \mathcal{T}$ and $\pi_1(P) = P$ for any $P \in E(\mathbb{F}_q)[r]$. Notice that any point $R \in E(\mathbb{F}_{q^k})[r]$ can be written $R = \pi_0(R) + \pi_1(R)$.

With these tools, we can mount a forgery attack against the Sakai-Kasahara scheme. The crucial assumption is that the KGC chooses a point $Q \in \mathcal{T}$. This is the case if the implementation is based on certain supersingular curves as described in [1, 6, 7] (such as curves of form $y^2 = x^3 + ax$ over $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$), or curves of form $y^2 = x^3 + ax + b$ over $\mathbb{F}_{3^m}$), or ordinary curves as suggested in [2]. These are popular choices, as they favour efficient implementation of the Tate or Weil pairing as well as other arithmetic operations.

The basic attack allows the legitimate receiver of a signcrypted message to fake other signcryptions from the same sender. This attack proceeds as follows. Bob unsigncrypts the received message (c, S), obtaining R and h. Let m' be the message he wants to pretend was sent by Alice. He computes:

$$\begin{aligned}
U &\leftarrow h^{-1}\,\pi_1(S) \;\; [= xP_a] \\
V &\leftarrow \pi_0(S) \;\; [= xQ_b] \\
h' &\leftarrow \mathcal{H}_0(m') \\
c' &\leftarrow \mathcal{H}_1(R^{1+h'}) \oplus m' \\
S' &\leftarrow h'U + V
\end{aligned}$$

Now Bob can use the pair (c', S') as evidence that Alice sent him m' rather than m. He can even further disguise his ruse by using a different x, say $x' = \alpha x$. All he has to do is to set $R' \leftarrow R^\alpha$, $U' \leftarrow \alpha U$, and $V' \leftarrow \alpha V$ and use these values instead.

This attack is especially annoying because, if the plaintext of any signcrypted message m from Alice to Bob is compromised, then a third party, Carol, can impersonate Alice and forge new signcrypted messages to Bob. Carol simply computes $h \leftarrow \mathcal{H}_0(m)$, $R = e(h^{-1}S, Q_a)$, and proceeds as above. We see that, in fact, Carol needs only h, not m itself.

5 The proposed schemes

The security of our schemes is based on the intractability of not only the Bilinear Diffie-Hellman Problem (BDHP) and the Computational Diffie-Hellman Problem (CDHP), but also the Inverse Computational Diffie-Hellman Problem (Inv-CDHP), namely, given P and $a^{-1}P$, compute a. However, the Inv-CDHP is polynomial-time equivalent to the CDHP [14].

5.1 A forward-secure authenticryption scheme

This scheme is based on Sakai-Kasahara, with additional techniques suggested in [14]. It is non-transferable, in the sense that Alice's signature can only be publicly verified with Bob's cooperation, at the cost of implicitly revealing the plaintext.

- **Setup:** The KGC generates a random secret polynomial $s(x) = \sum_{i=0}^{d} s_i x^i \in \mathbb{Z}_r[x]$ which acts as its private master key. The simplest choice is $d = 1$, $s_1 = 1$, so the secret key reduces to the single $\mathbb{Z}_r^*$ value s_0. The KGC publishes the points P, Q, $g = e(P, Q)$, s_iP, and s_iQ for $i = 0, \ldots, d$.

- **Keygen:** A users identity is hashed using a random oracle to a public element $u \in \mathbb{Z}_r^*$. The KGC computes this user's private keys as $P_{su} = s(u)^{-1}P$ and $Q_{su} = s(u)^{-1}Q$, where the inverse is computed modulo r. The corresponding public keys can be (publicly) computed from u and the points s_iP, s_iQ as $P_u = \sum_{i=0}^{d} u^i(s_iP) = s(u)P$ and $Q_u = \sum_{i=0}^{d} u^i(s_iQ) = s(u)Q$, respectively. Let Alice's identity be a and Bob's identity be b.
- **Signcrypt:** To signcrypt a message $m \in \{0,1\}^*$ to Bob, Alice generates a random integer $x \in \mathbb{Z}_r^*$ and computes:

$$\begin{aligned} R &\leftarrow g^x \\ c &\leftarrow \mathcal{H}_1(R) \oplus m \\ h &\leftarrow \mathcal{H}_2(R, c) \\ S &\leftarrow (x+h)P_{sa} \\ T &\leftarrow xP_b \end{aligned}$$

  The signcrypted message that Alice sends to Bob is (c, S, T).
- **Unsigncrypt:** Upon reception of the above triple, Bob computes:

$$\begin{aligned} R &\leftarrow e(T, Q_{sb}) \\ h &\leftarrow \mathcal{H}_2(R, c) \\ m &\leftarrow \mathcal{H}_1(R) \oplus c \\ V &\leftarrow e(S, Q_a) \end{aligned}$$

  Bob then verifies that $V = Rg^h$.

This scheme works by the following reasoning. If the triple is correct, then $e(T, Q_{sb}) = e(xs(b)P, s(b)^{-1}Q) = R$. Besides, $e(S, Q_a) = e((x + h)s(a)^{-1}P, s(a)Q) = e(P, Q)^{x+h} = Rg^h$ as expected.

Contrary to the Sakai-Kasahara scheme, the relationship between $\langle P \rangle$ and $\langle Q \rangle$ is not used here for security purposes beyond the fact that the pairing must be non-degenerate on these groups, thus making the projection attack not applicable.

5.2 A forward-secure transferable signcryption scheme

The previous scheme is not publicly verifiable because the signature tag computation depends on R, which can only be recovered by the legitimate receiver. Libert and Quisquater [9] propose as an open problem the task of devising an efficient signcryption scheme providing both public verifiability and forward security. We now describe such a scheme, thereby closing that gap.

Usually one conceives a signcryption scheme as an algorithm more efficient than the encrypt-then-sign paradigm; it turns out as a surprise that our scheme, which ranks among the latter type, becomes faster than any of the previously known signcryption methods in certain settings (see table 1).

- **Setup:** The KGC generates a random secret polynomial $s(x) = \sum_{i=0}^{d} s_i x^i \in \mathbb{Z}_r[x]$ which acts as its private master key. The simplest choice is $d = 1$, $s_1 = 1$, so the secret key reduces to the single $\mathbb{Z}_r^*$ value s_0. The KGC publishes the points P, Q, $g = e(P, Q)$, and $s_i P$ for $i = 0, \ldots, d$.
- **Keygen:** A users identity is hashed using a random oracle to a public element $u \in \mathbb{Z}_r^*$. The KGC computes a user's private key as $Q_{su} = s(u)^{-1}Q$, where the inverse is computed modulo r. The corresponding public key can be (publicly) computed from u and the points $s_i P$ as $P_u = \sum_{i=0}^{d} u^i(s_i P) = s(u)P$. Let Alice's identity be a and Bob's identity be b.
- **Signcrypt:** To signcrypt a message $m \in \{0,1\}^*$ to Bob, Alice generates a random integer $x \in \mathbb{Z}_r^*$ and computes:

$$\begin{aligned} N &\leftarrow g^{x^{-1}} \\ R &\leftarrow xP_a \\ S &\leftarrow x^{-1}P_b \\ c &\leftarrow \mathcal{H}_1(N) \oplus m \\ h &\leftarrow \mathcal{H}'_3(R, S, c) \\ T &\leftarrow (x+h)^{-1}Q_{sa} \end{aligned}$$

The signcrypted message that Alice sends to Bob is (c, R, S, T).
- **Unsigncrypt:** Upon reception of the above quadruple, Bob computes:

$$\begin{aligned} h &\leftarrow \mathcal{H}'_3(R, S, c) \\ V &\leftarrow e(R + hP_a, T) \\ N &\leftarrow e(S, Q_{sb}) \\ m &\leftarrow \mathcal{H}_1(N) \oplus c \end{aligned}$$

Bob then verifies that $V = g$.

This scheme works by the following reasoning. If the quadruple is correct, then h is correct and $e(R + hP_a) = e(xs(a)P + hs(a)P, (x+h)^{-1}s(a)^{-1}Q) = e(P, Q) = g$. Besides, $e(S, Q_b) = e(x^{-1}s(b)P, s(b)^{-1}Q) = e(P, Q)^{x^{-1}}$, which is the original N as expected.

The signcryption is transferable (publicly verifiable) because V does not depend on any private information. It is also forward-secure, in the sense that only Bob (and the KGC) can recover m: knowledge of Alice's private keys P_a and Q_a alone is insufficient to compute N (or, equivalently, $x^{-1}P$, $x^{-1}Q$, or x^{-1} itself). Notice that one could generalise the scheme by substituting $\mathcal{H}(x)$ for x^{-1}, where $\mathcal{H}$ is a suitable random oracle.

6 A new identity-based signature scheme

We can derive an efficient identity-based signature scheme from the non-transferable signcryption scheme in section 5.2. Actually this scheme is the identity-based analogue of the signature scheme proposed by Zhang, Safavi-Naini and Susilo [14]. Existing identity-based signature methods include the Heß scheme [8] and the Cha-Cheon [4] scheme; we compare their relative efficiency in section 7.

- **Setup:** The KGC generates a random secret polynomial $s(x) = \sum_{i=0}^{d} s_i x^i \in \mathbb{Z}_r[x]$ which acts as its private master key. The simplest choice is $d = 1$, $s_1 = 1$, so the secret key reduces to the single $\mathbb{Z}_r^*$ value s_0. The KGC publishes the points P, Q, $g = e(P, Q)$, and $s_i P$ for $i = 0, \ldots, d$.
- **Keygen:** A users identity is hashed using a random oracle to a public element $u \in \mathbb{Z}_r^*$. The KGC computes this user's private key as $Q_{su} = s(u)^{-1}Q$, where the inverse is computed modulo r. The corresponding public key can be (publicly) computed from u and the points $s_i P$ as $P_u = \sum_{i=0}^{d} u^i(s_i P) = s(u)P$. Let Alice's identity be a.
- **Signing:** To sign a message $m \in \{0, 1\}^*$, Alice generates a random integer $x \in \mathbb{Z}_r^*$ and computes:

$$\begin{aligned} R &\leftarrow xP_a \\ h &\leftarrow \mathcal{H}'_2(R, m) \\ S &\leftarrow (x + h)^{-1}Q_{sa} \end{aligned}$$

  The signature attached to m is the pair (R, S).
- **Verification:** Upon reception of the above pair, Bob computes $h \leftarrow \mathcal{H}'_2(R, m)$ and checks that $e(R + hP_a, S) = g$.

7 Computational cost comparison

We now briefly assess the comparative efficiency of several identity-based signcryption schemes, implemented according to their original descriptions.

Table 1 compares the processing times of our schemes with other identity-based signcryption and signature schemes, for the underlying base finite field $\mathbb{F}_{3^{97}}$ and a supersingular curve of embedding degree $k = 6$. Table 2 does the same for an underlying finite field $\mathbb{F}_q$ with $\lg q = 512$ bits and an ordinary curve with $k = 2$. All implementations were written in C++ and run on an Athlon XP 1.6 GHz.

We see from these results that our proposed algorithms rank among the fastest schemes.

8 Conclusion

We have pointed out semantic security problems in existing signcryption schemes, and showed that the choice of the bilinear pairing may impair schemes otherwise arguably secure.

We have also proposed efficient signcryption schemes that are semantically and forward secure, in both transferable and non-transferable form. Our schemes

Table 1. Efficiency comparison, $k = 6$

non-transferable scheme	signcryption (ms)	unsigncryption (ms)
Malone-Lee	18.2	40.6
Boyen	25.5	55.2
Chen-Malone-Lee	18.2	40.6
Libert-Quisquater	18.2	27.6
Nalla-Reddy	24.0	46.8
Sakai-Kasahara	19.3	33.8
ours	10.9	33.8
transferable scheme	signcryption (ms)	unsigncryption (ms)
Libert-Quisquater	29.7	53.7
ours	13.0	27.6
signature scheme	signing (ms)	verification (ms)
Heß	11.4	33.8
Cha-Cheon	3.7	27.6
ours	3.7	14.6

Table 2. Efficiency comparison, $k = 2$

non-transferable scheme	signcryption (ms)	unsigncryption (ms)
Malone-Lee	106.8	70.8
Boyen	44.8	99.5
Chen-Malone-Lee	42.7	70.8
Libert-Quisquater	42.7	49.5
Nalla-Reddy	37.5	66.1
Sakai-Kasahara	18.8	44.8
ours	16.1	44.8
transferable scheme	signcryption (ms)	unsigncryption (ms)
Libert-Quisquater	56.8	89.6
ours	23.4	49.5
signature scheme	signing (ms)	verification (ms)
Heß	16.2	44.8
Cha-Cheon	14.1	49.5
ours	14.1	28.7

can be implemented with any secure pairing instantiation, including those that use the trace-zero group. Our transferable scheme answers an open problem posed by Libert and Quisquater in [9], and also gives rise to a new, efficient identity-based signature scheme.

References

1. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *Advances in Cryptology – Crypto'2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–368. Springer-Verlag, 2002.
2. P. S. L. M. Barreto, B. Lynn, and M. Scott. On the selection of pairing-friendly groups. In *Selected Areas in Cryptography – SAC'2003*, 2003. to appear.
3. X. Boyen. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In *Advances in Cryptology – Crypto'2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 383–399. Springer-Verlag, 2003.
4. J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. In *Practice and Theory in Public Key Cryptography – PKC'2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 18–30, Miami, USA, 2003. Springer-Verlag.
5. L. Chen and J. Malone-Lee. Improved identity-based signcryption. Cryptology ePrint Archive, Report 2004/114, 2004. `http://eprint.iacr.org/2003/114`.
6. S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. In *Algorithm Number Theory Symposium – ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer-Verlag, 2002.
7. S. Galbraith and V. Rotger. Easy decision-diffie-hellman groups. Cryptology ePrint Archive, Report 2004/070, 2004. `http://eprint.iacr.org/2004/070`.
8. F. Heß. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography – SAC'2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 310–324. Springer-Verlag, 2003.
9. B. Libert and J.-J. Quisquater. New identity based signcryption schemes based on pairings. In *IEEE Information Theory Workshop*, Paris, France, 2003.
10. J. Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002. `http://eprint.iacr.org/2002/098`.
11. D. Nalla and K. C. Reddy. Signcryption scheme for identity-based cryptosystems. Cryptology ePrint Archive, Report 2003/066, 2002. `http://eprint.iacr.org/2003/066`.
12. R. Sakai and M. Kasahara. Id based cryptosystems with pairing on elliptic curve. In *2003 Symposium on Cryptography and Information Security – SCIS'2003*, Hamamatsu, Japan, 2003. See also `http://eprint.iacr.org/2003/054`.
13. A. Shamir. Identity based cryptosystems and signature schemes. In *Advances in Cryptology – Crypto'84*, volume 0196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1984.
14. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *International Workshop on Practice and Theory in Public Key Cryptography – PKC'2004*, Lecture Notes in Computer Science. Springer-Verlag, 2004. to appear.
15. Y. Zheng. Signcryption and its applications in efficient public key solutions. In *ISW'97*, pages 291–312, 1998.

A Strict non-transferability of the Nalla-Reddy scheme

The Nalla-Reddy scheme was proposed in [11]. We now show that, contrary to all other identity-based signcryption schemes we are aware of, it is inherently non-transferable, in the sense that a recipient cannot under any circumstance use the signcrypted message to convince a third party about the identity of the sender. In other words, if Alice signcrypts and sends a message to Bob, he can thereafter easily forge other messages to himself as if they had been signcrypted by Alice; as a consequence, Bob cannot convince anyone that a message has really been sent by Alice.

Interestingly, deciding if this is a weakness or rather a useful property depends on the application where the scheme is to be employed.

Setup: The KGC generates a random master secret $s \in \mathbb{Z}_r^*$ and publishes P, Q, $P_s \equiv sP$, and $Q_s \equiv sQ$. One can (and should) verify that this set is consistent by checking that $e(P, Q_s) = e(P_s, Q)$.

Keygen: A user identity is an element $u \in \{0,1\}^*$, to which there correspond public points $P_u = \mathcal{H}_P(u)$ and $Q_u = \mathcal{H}_Q(u)$. The KGC calculates this user's private keys as $P_{su} = sP_u$ and $Q_{su} = sQ_u$. Let Alice's identity be a and Bob's identity be b.

Signcrypt: To signcrypt a message $m \in \{0,1\}^*$ to Bob, Alice generates a number integer $x \in \mathbb{Z}_r^*$ and computes:

$$\begin{aligned} R &\leftarrow xP_{sa} \\ Y &\leftarrow e(P_{sa}, Q_b) \\ h &\leftarrow \mathcal{H}_3(R, Y, m) \\ S &\leftarrow xhP_a \\ N &\leftarrow Y^{xh} \\ c &\leftarrow \mathcal{H}_1(N) \oplus m \end{aligned}$$

The signcrypted message that Alice sends to Bob is (c, R, S).

Unsigncrypt: Upon receiving the above triple, Bob computes:

$$\begin{aligned} N &\leftarrow e(S, Q_{sb}) \\ m &\leftarrow \mathcal{H}_1(N) \oplus c \\ Y &\leftarrow e(P_a, Q_{sb}) \\ h &\leftarrow \mathcal{H}_3(R, Y, m) \end{aligned}$$

Bob then verifies that $N = e(R, Q_b)^h$.

The Nalla-Reddy protocol is non-transferable and so does not allow the digital signature service of non-repudiation. Bob can manipulate a valid ciphertext and claim to a third party that Alice signcrypted a different message to him. Say Bob received from Alice the valid triple (c, R, S) and he wishes to replace

m by the forged message m'. He computes:

$$
\begin{aligned}
h' &\leftarrow \mathcal{H}_3(R, e(P_a, Q_{sb}), m') \\
S' &\leftarrow h^{-1}h'S \\
N' &\leftarrow N^{h^{-1}h'} \\
c' &\leftarrow \mathcal{H}_1(N') \oplus m'
\end{aligned}
$$

The forged ciphertext on m' is (c', R, S'). Therefore, the Nalla-Reddy scheme is inherently non-transferable.