A Formal Proof of Security of Zhang and Kim's ID-Based Ring Signature Scheme *

Javier Herranz

Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3, Mòdul C3, Campus Nord, 08034-Barcelona, Spain

Abstract. In this work we provide a formal analysis of the security of an identity-based ring signature scheme proposed by Zhang and Kim in [10]. We first define the security requirements that this kind of schemes must satisfy; or in other words, the capabilities and goals of the most powerful attacks these schemes must remain secure against. Then we prove, in the random oracle model, that the above-mentioned scheme is secure against the defined attacks, assuming that the Computational Diffie-Hellman problem is hard to solve.

1 Introduction

In a *ring signature scheme*, a user computes a signature on behalf of a set (or ring) of users which contains himself. The goal is that any verifier must be convinced that the signature has been computed by some member of this ring, but he has no better way than at random to guess which member is the actual author of the signature.

In practice, if the communications system is authenticated with the use of a Public Key Infrastructure (PKI) based on certificates, the signer must first verify that the public keys of the ring correspond (via a certificate) to the identities of the users that he wants to include on the ring. Later, the verification process of a ring signature obviously employs the public keys of the members of the ring. Therefore, the verifier must first check that these public keys are actually certificated as the ones of the members of the ring.

This means that the cost of both processes of generating and verifying a ring signature substantially increases because of the necessary management of digital certificates. Any possible alternative which avoids the necessity of a PKI is very welcome if we want to design efficient public key cryptosystems, in particular ring signature schemes where the number of certificates that must be checked in each operation can be reasonably high.

Identity-based (from now on, ID-based) cryptography, introduced by Shamir in 1984 [9], is a solution to this problem. The idea is that the public key of a

* This work was partially supported by Spanish *Ministerio de Ciencia y Tecnología* under project TIC 2003-00866.

Herranz J. (2004).
A Formal Proof of Security of Zhang and Kim's ID-Based Ring Signature Scheme.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 63-72
DOI: 10.5220/0002661000630072

user can be easily (and publicly) computed from his identity (for example, from a complete name, an e-mail or an IP address). Then, the secret key is derived from the public key. In this way, certificates which link identities and public keys are not needed any more, because anyone can easily verify that some public key PK_U corresponds in fact to user U. The process that generates secret keys from public keys must be executed by an external entity, known as the *master*.

In this work we analyze the security of an ID-based ring signature scheme, based on bilinear pairings. Let us do a brief overview of some works related to ring signatures.

In [8], Rivest, Shamir and Tauman formalize the concept of ring signature schemes, and propose a scheme which they prove existentially unforgeable under adaptive chosen-message attacks, in the ideal cipher model, assuming the hardness of the RSA problem. This scheme also uses a symmetric encryption scheme and the notion of combining functions.

Bresson, Stern and Szydlo show in [3] that the scheme of [8] can be modified in such a way that the new scheme is proved to achieve the same level of security, but under the strictly weaker assumption of the random oracle model.

In [1], Abe, Ohkubo and Suzuki give general constructions of ring signature schemes for a variety of scenarios, including those where signature schemes are based on one-way functions, and those where signature schemes are of the three-move type (for example, Schnorr's signature scheme).

Some security results for generic ring signature schemes, as well as a new specific scheme based on Schnorr's signature scheme, are given by Herranz and Sáez in [5].

Finally, the only ID-based ring signature scheme proposed until now (as far as we know) is the one by Zhang and Kim [10], which is based on pairings. However, they do not provide a formal proof of the existential unforgeability of the proposed scheme.

We provide such a formal proof of security for this ID-based ring signature scheme, assuming that the Computational Diffie-Hellman problem is hard to solve. The proof uses standard techniques in the random oracle model [2], like replaying attacks (formalized in the forking lemmas by Pointcheval and Stern in [7]), which have been already employed to prove the security of other ring signature schemes, for example [1, 5].

2 Zhang and Kim's ID-Based Ring Signature Scheme

In this section we review the ID-based ring signature scheme proposed by Zhang and Kim in [10]. We first explain some basics on bilinear parings and on ring signature schemes.

2.1 A Note on Pairings

Let $\mathbb{G}_1$ be an additive group of prime order q, generated by some element P. Let $\mathbb{G}_2$ be a multiplicative group with the same order q. We consider a *pairing* as a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following three properties:

1. It is bilinear, which means that given elements $T_1, T_2, T_3 \in \mathbb{G}_1$, we have that $e(T_1+T_2, T_3) = e(T_1, T_3) \cdot e(T_2, T_3)$ and $e(T_1, T_2+T_3) = e(T_1, T_2) \cdot e(T_1, T_3)$. In particular, for all $a, b \in \mathbb{Z}_q$, we have $e(aP, bP) = e(P, P)^{ab} = e(P, abP) = e(abP, P)$.
2. The map e can be efficiently computed for any possible input pair.
3. The map e is non-degenerate: there exist elements $T_1, T_2 \in \mathbb{G}_1$ such that $e(T_1, T_2) \neq 1_{\mathbb{G}_2}$.

Combining properties 1 and 3, it is easy to see that $e(P, P) \neq 1_{\mathbb{G}_2}$ and that the equality $e(T_1, P) = e(T_2, P)$ implies that $T_1 = T_2$.

The typical way of obtaining such pairings is by deriving them from the Weil or the Tate pairing on an elliptic curve over a finite field. The interested reader is referred to [11] for a complete bibliography of cryptographic works based on pairings.

2.2 Ring Signatures

The idea of a ring signature is the following: a user wants to compute a signature on a message, on behalf of a set (or ring) of users which includes himself. He wants the verifier of the signature to be convinced that the signer of the message is in effect some of the members of this ring. But he wants to remain completely anonymous. That is, nobody will know which member of the ring is the actual author of the signature.

These two informal requirements are ensured, if the scheme satisfies the following properties:

1. **Anonymity:** any verifier should not have probability greater than $1/n$ to guess the identity of the real signer who has computed a ring signature on behalf of a ring of n members. If the verifier is a member of the ring distinct from the actual signer, then his probability to guess the identity of the real signer should not be greater than $1/(n-1)$.
2. **Unforgeability:** among all the proposed definitions of unforgeability (see [4]), we consider the strongest one: any attacker must have negligible probability of success in forging a valid ring signature for some message m on behalf of a ring that does not contain himself, even if he knows valid ring signatures for messages, different from m, that he can adaptively choose.

Ring signatures are a useful tool to provide anonymity in some scenarios. For example, if a member of a group wants to leak to the media a secret information about the group, he can sign this information using a ring scheme. Everybody will be convinced that the information comes from the group itself, but anybody could accuse him of leaking the secret.

A different application is the following: if the signer A of a message wants that the authorship of the signature could be entirely verified only by some specific user B, he can sign the message with respect of the ring $\{A, B\}$. The rest of users could not know who between A and B is the author of the signature, but B will be convinced that the author is A.

2.3 The Scheme

Zhang and Kim proposed in [10] the first ID-based ring signature scheme, following the idea behind the ring signature schemes proposed by Abe, Ohkubo and Suzuki in [1]. We review Zhang and Kim's scheme in this section.

Setup: let $\mathbb{G}_1$ be an additive group of prime order q, generated by some element P. Let $\mathbb{G}_2$ be a multiplicative group with the same order q. We need $q \geq 2^k$, where k is the security parameter of the scheme. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a pairing as defined in Section 2.1. Let $H_1 : \{0,1\}^* \to \mathbb{G}_1 - \{0\}$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_q$ be two hash functions (in the proof of security, we will assume that they behave as random oracles [2]).

The master entity chooses at random his secret key $x \in \mathbb{Z}_q^*$ and publishes the value $Y = xP \in \mathbb{G}_1$.

Secret key extraction: a user U, with identity $ID_U \in \{0,1\}^*$, has public key $PK_U = H_1(ID_U)$. When he requests the master for his matching secret key, he obtains the value $SK_U = xPK_U$.

Ring signature: consider a ring $\mathcal{U} = \{U_1, \ldots, U_n\}$ of users; for simplicity we denote $PK_i = PK_{U_i} = H_1(ID_{U_i})$. If some of these users U_s, where $s \in \{1, \ldots, n\}$, wants to anonymously sign a message m on behalf of the ring $\mathcal{U}$, he acts as follows:

1. Choose a random $T \in \mathbb{G}_1$ and compute $c_{s+1} = H_2(\mathcal{U}, m, e(T, P))$.
2. For $i = s+1, \ldots, s-1$ (where i is considered modulo n), choose T_i at random in $\mathbb{G}_1$. Compute $c_{i+1} = H_2(\mathcal{U}, m, e(T_i, P) \cdot e(c_i PK_i, Y))$.
3. Compute $T_s = T - c_s SK_s \bmod q$.
4. Define the signature of the message m made by the ring $\mathcal{U} = \{U_1, \ldots, U_n\}$ to be $(\mathcal{U}, m, c_0, T_0, T_1, \ldots, T_{n-1})$.

Verification: the validity of the signature is verified by the recipient of the message in the following way:

1. For $i = 0, 1, \ldots, n-1$, compute $c_{i+1} = H_2(\mathcal{U}, m, e(T_i, P) \cdot e(c_i PK_i, Y))$.
2. Accept the signature as valid if $c_n = c_0$, and reject it otherwise.

By using the bilinear property of the pairing e, it is easy to see that the scheme is correct.

3 A Formal Security Analysis

In their paper [10], Zhang and Kim do not provide a formal proof of the security of this scheme. Their arguments are quite heuristic or intuitive. They can be enough for anonymity, but not for unforgeability. For example, they do not define the capabilities of an adversary against an ID-based ring signature scheme. They

assert that the scheme is secure because in the case $n = 1$ the scheme is exactly the ID-based signature scheme proposed by Hess in [6], and since this scheme is proved to be secure, then the ring signature scheme is also secure. Clearly, this argument is not enough. We give in this section a formal proof of the security of their scheme, which employs some standard techniques, like replaying attacks [7], already used to prove the security of other ring signature schemes [1, 5].

3.1 The Security Model

We must consider the most powerful attack against an ID-based ring signature scheme, that we call *chosen message and identities attack*. Such an attacker $\mathcal{A}$ is allowed to:

- make Q_1 queries to the random oracle H_1 and Q_2 queries to the random oracle H_2;
- ask for the secret key of Q_e identities of its choice (extracting oracle);
- ask Q_s times for valid ring signatures, on behalf of rings of its choice, of messages of its choice (signing oracle).

The total number of queries must be polynomial in the security parameter. The attacker is successful if it outputs, in polynomial time and with non-negligible probability, a valid ring signature for some message m and some ring of users $\mathcal{U} = \{U_1, \ldots, U_n\}$ such that:

- the attacker has not asked for the secret key of any of the members of the ring $\mathcal{U}$;
- the attacker has not asked for a valid ring signature, on behalf of the ring $\mathcal{U}$, of message m.

3.2 The Computational Diffie-Hellman Problem

We consider the following well-known problem in the group $\mathbb{G}_1$ of prime order q, generated by P.

Definition 1. *Given the elements $P, aP, bP \in \mathbb{G}_1$, for some random values $a, b \in \mathbb{Z}_q^*$, the Computational Diffie-Hellman (CDH) problem consists of computing the element abP.*

The Computational Diffie-Hellman Assumption asserts that, if the order of $\mathbb{G}_1$ is $q \geq 2^k$, then any polynomial time algorithm that solves the CDH problem has a success probability p_k which is negligible in the security parameter k. In other words, for all polynomial $f()$, there exists an integer k_0 such that $p_k < \frac{1}{f(k)}$, for all $k \geq k_0$.

3.3 Proving the Unforgeability of the Scheme

We start with a technical lemma which will be necessary for the proof of the main result. Its proof can be found in [7].

Lemma 1. *(The Splitting Lemma) Let $A \subset X \times Y$ such that $\Pr[(x,y) \in A] \geq \delta$. For any $\alpha < \delta$, define*

$$B = \{(x,y) \in X \times Y | \Pr_{y' \in Y}[(x,y') \in A] \geq \delta - \alpha\}.$$

Then the following statements hold:

1. $\Pr[B] \geq \alpha$.
2. *For any $(x,y) \in B$, $\Pr_{y' \in Y}[(x,y') \in A] \geq \delta - \alpha$.*
3. $\Pr[B|A] \geq \alpha/\delta$.

We prove now that the existence of a successful attack against the ID-based ring signature scheme could be used to solve the Computational Diffie-Hellman problem in $\mathbb{G}_1$ (a proof by reduction). Since this problem is assumed to be hard, we conclude that there does not exist such an attack. In this way, the scheme is proved to be existentially unforgeable under chosen message and identities attacks.

In this proof, we assume that the hash functions H_1 and H_2 behave as random oracles [2].

Theorem 1. *Let k be a security parameter, and let the order of $\mathbb{G}_1$ be $q \geq 2^k$. Let $\mathcal{A}$ be a probabilistic polynomial time Turing machine attacking the considered ID-based ring signature scheme. We denote by Q_1, Q_2, Q_e and Q_s the number of queries that $\mathcal{A}$ can ask to the random oracles H_1 and H_2 and to the extracting and signing oracles, respectively. We denote by N the maximum cardinality of the rings for which $\mathcal{A}$ asks for a valid signature.*

Assume that $\mathcal{A}$ produces, within polynomial time t and with non-negligible probability of success ε, a valid ring signature $(\mathcal{U}, m, c_0, T_0, T_1, \ldots, T_{n-1})$, such that $\mathcal{A}$ has not asked for the secret key of any of the members of $\mathcal{U}$, and has not asked for a valid ring signature of m on behalf of the ring $\mathcal{U}$. Assume that $q > \max\{(Q_1 + Q_e)^2, 2N, 2Q_2Q_s\}$ and that $\varepsilon > \frac{64\ Q_2^2}{q}$.

Then the Computational Diffie-Hellman problem in $\mathbb{G}_1$ can be solved with probability $\varepsilon' \geq \frac{9}{100\ Q_1}$ and in time $t' \leq \frac{64 Q_2^2}{\varepsilon} t$.

Proof. Let (P, aP, bP) be an input of the CDH problem in $\mathbb{G}_1$, for some random $a, b \in \mathbb{Z}_q^*$. We design a solver algorithm $\mathcal{B}$ that uses the attacker $\mathcal{A}$ as a subroutine, and finds the solution of the CDH problem.

First, $\mathcal{B}$ runs the setup phase of the ID-based ring signature scheme, defining the public master key as $Y = aP$. Then $\mathcal{B}$ runs the attacker $\mathcal{A}$. The algorithm $\mathcal{B}$ must simulate the environment of the attacker $\mathcal{A}$; that is, it must provide consistent answers to all the queries that $\mathcal{A}$ is allowed to make (random oracles H_1 and H_2, extracting and signing oracles).

Furthermore, $\mathcal{B}$ chooses at random a value $\ell \in \{1, 2, \ldots, Q_1\}$. When the attacker $\mathcal{A}$ makes the ℓ-th query to the random oracle H_1, with some identity ID_ℓ, the algorithm $\mathcal{B}$ sets $PK_\ell = H_1(ID_\ell) = bP$, and sends this value to the attacker. Later, if the attacker $\mathcal{A}$ asks for the secret key of ID_ℓ to the extracting oracle, then the algorithm $\mathcal{B}$ stops and outputs "fail".

For the rest of identities $\{ID_j\}_{1 \leq j \leq Q_e+Q_1}$ that $\mathcal{A}$ queries to the extracting oracle or to the random oracle H_1, $\mathcal{B}$ can provide consistent answers as follows: $\mathcal{B}$ chooses a random element $x_j \in \mathbb{Z}_q^*$ and computes the values $PK_j = x_j P$ and $SK_j = x_j Y$, where Y is the master public key. Then $\mathcal{B}$ sets $H_1(ID_j) = PK_j$, and stores this relation in a random oracle list for H_1. If the query was a random oracle query, $\mathcal{B}$ sends to $\mathcal{A}$ the value PK_j. If the query was an extracting query, $\mathcal{B}$ sends to $\mathcal{A}$ the value SK_j for the secret key, as well.

The only inconsistency problem happens if two different executions (with different identities ID_i and ID_j) of this simulation result in the same value $PK_i = PK_j$. The probability of such a collision is, however, less than $\frac{(Q_1+Q_e)^2}{2} \cdot \frac{1}{q}$.

On the other hand, every time that $\mathcal{A}$ asks for a valid ring signature for a message m and a ring $\mathcal{U}$, the algorithm $\mathcal{B}$ proceeds as follows:

1. Choose at random $c_0 \in \mathbb{Z}_q$.
2. For $i = 0, 1, \ldots, n-1$, choose T_i at random in $\mathbb{G}_1$. If $i \neq n-1$, compute $c_{i+1} = H_2(\mathcal{U}, m, e(T_i, P) \cdot e(c_i PK_i, Y))$. In order to compute this value, the algorithm $\mathcal{B}$ constructs, as before, a random oracle list for H_2. If the input is already in the list, it outputs the matching value. If not, it chooses a random value in $\mathbb{Z}_q$, outputs it and stores the new relation in the list.
3. Define $H_2(\mathcal{U}, m, e(T_{n-1}, P) \cdot e(c_{n-1} PK_{n-1}, Y))$ to be c_0. Store this relation in the list for H_2.
4. Send the tuple $(\mathcal{U}, m, c_0, T_0, T_1, \ldots, T_{n-1})$ to $\mathcal{A}$.

For the queries of $\mathcal{A}$ to the random oracle H_2, the algorithm $\mathcal{B}$ proceeds in the same way: it looks for the input in the list, outputting the matching value if it finds it, or a random value otherwise. Now the risk is that, in step 3 of the above simulation process, the obtained tuple $(\mathcal{U}, m, e(T_{n-1}, P) \cdot e(c_{n-1} PK_{n-1}, Y))$ has been already queried by $\mathcal{A}$ to the random oracle H_2. The probability of such a collision is less than $\frac{Q_2}{q}$ for each execution of the signature simulation, and so less than $\frac{Q_s Q_2}{q}$ for the whole process.

Summing up, the algorithm $\mathcal{B}$ successfully simulates the environment of $\mathcal{A}$ with probability greater than $\epsilon_1 = (1 - \frac{(Q_1+Q_e)^2}{2q})(1 - \frac{Q_s Q_2}{q})$.

We denote by ω the whole set of random tapes that take part in an attack by $\mathcal{A}$, with the environment simulated by $\mathcal{B}$, but excluding the randomness related to the oracle H_2. The success probability of $\mathcal{A}$ in forging a valid ring signature scheme is then taken over the space (ω, H_2). If we denote by $\mathcal{S}$ the set of successful executions of $\mathcal{A}$, we have that $\Pr[(\omega, H_2) \in \mathcal{S}] \geq \varepsilon$.

Now consider a ring signature $(\mathcal{U}, m, c_0, T_0, T_1, \ldots, T_{n-1})$ forged by $\mathcal{A}$. We denote as R_i the value $e(T_i, P) \cdot e(c_i PK_i, Y)$, for all $i = 0, \ldots, n-1$. We use the notation $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_{Q_2}$ for the different queries that $\mathcal{A}$ makes to the random oracle H_2. By the ideal randomness of this oracle, the probability that $\mathcal{A}$ has

not asked for some of the tuples $(\mathcal{U}, m, R_i)$, with $i = 0, \ldots, n-1$ (and so $\mathcal{A}$ must have guessed the corresponding output), is less than $\frac{n}{q} \leq \frac{N}{q}$.

We refer as $\mathcal{S}'$ to the successful executions of $\mathcal{A}$, with $\mathcal{B}$ simulating its environment, where $\mathcal{A}$ has queried all the tuples $(\mathcal{U}, m, R_i)$ in the forged signature to the random oracle H_2. We have that $\epsilon_2 = \Pr[(\omega, H_2) \in \mathcal{S}'] \geq \varepsilon\ \epsilon_1(1 - \frac{N}{q})$. The restriction on the values of q, Q_1, Q_2, Q_e and Q_s in the statement of this theorem implies that $\epsilon_2 > \varepsilon/8$.

Because of the ring structure formed by the queries that $\mathcal{A}$ makes to the random oracle H_2, there exists at least one index $k \in \{1, 2, \ldots, n\}$ such that the query $\mathcal{Q}_u = (\mathcal{U}, m, R_k)$ was made to H_2 before the query $\mathcal{Q}_v = (\mathcal{U}, m, R_{k-1})$ (that is, $u < v$). This pair (u, v) is called then a gap index. If there are two or more gap indexes in a forged signature, we consider only the one with the smallest value u. This allows us to define the subset $\mathcal{S}'_{u,v}$ of $\mathcal{S}'$ as the set of executions in $\mathcal{S}'$ whose gap index is (u, v). This gives us a partition of $\mathcal{S}'$ in exactly $\frac{Q_2(Q_2+1)}{2}$ classes.

If $\mathcal{B}$ invokes $t_1 = 1/\epsilon_2$ times the attacker $\mathcal{A}$ with randomly chosen (ω, H_2), it obtains a successful execution $(\tilde{\omega}, \tilde{H}_2) \in \mathcal{S}'_{u,v}$, for some gap index (u, v), with probability $1 - (1 - \epsilon_2)^{1/\epsilon_2} = 1 - \left[\left(1 + \frac{1}{-1/\epsilon_2}\right)^{-1/\epsilon_2}\right]^{-1} \geq 1 - e^{-1} > 3/5$.

Now we define the set of gap indexes which are more likely to appear as

$$I = \{(u, v) \text{ s.t. } \Pr[(\omega, H_2) \in \mathcal{S}'_{u,v} \mid (\omega, H_2) \in \mathcal{S}'] \geq \frac{1}{Q_2(Q_2+1)}\}.$$

And the corresponding subset of successful executions as $\mathcal{S}'_I = \{(\omega, H_2) \in \mathcal{S}'_{u,v}$ s.t. $(u, v) \in I\}$.

It holds that $\Pr[(\omega, H_2) \in \mathcal{S}'_I \mid (\omega, H_2) \in \mathcal{S}'] \geq 1/2$. In effect, since the sets $\mathcal{S}'_{u,v}$ are disjoint, we have

$$\Pr[(\omega, H_2) \in \mathcal{S}'_I \mid (\omega, H_2) \in \mathcal{S}'] = \sum_{(u,v)\in I} \Pr[(\omega, H_2) \in \mathcal{S}'_{u,v} \mid (\omega, H_2) \in \mathcal{S}'] =$$

$$1 - \sum_{(u,v)\notin I} \Pr[(\omega, H_2) \in \mathcal{S}'_{u,v} \mid (\omega, H_2) \in \mathcal{S}'].$$

Since the complement of I contains at most $\frac{Q_2(Q_2+1)}{2}$ gap indexes, we have that this probability is greater than $1 - \frac{Q_2(Q_2+1)}{2} \cdot \frac{1}{Q_2(Q_2+1)} = 1/2$. Therefore, with probability at least $1/2$, the specific successful execution $(\tilde{\omega}, \tilde{H}_2)$ is in $\mathcal{S}'_I$.

Consider any possible likely gap index $(u, v) \in I$; we have that

$$\Pr[(\omega, H_2) \in \mathcal{S}'_{u,v}] = \Pr[(\omega, H_2) \in \mathcal{S}'] \cdot \Pr[(\omega, H_2) \in \mathcal{S}'_{u,v} \mid (\omega, H_2) \in \mathcal{S}'] \geq$$

$$\geq \epsilon_2 \cdot \frac{1}{Q_2(Q_2+1)}.$$

We split H_2 as (H'_2, c_k), where H'_2 corresponds to the answers of all the queries to H_2 except the query $\mathcal{Q}_v$, whose answer is denoted as c_k. We apply the Splitting

Lemma (lemma 1), taking $X = (\omega, H'_2)$, $Y = c_k$, $A = \mathcal{S}'_{u,v}$, $\delta = \frac{\epsilon_2}{Q_2(Q_2+1)}$ and $\alpha = \frac{\epsilon_2}{2Q_2(Q_2+1)}$. The lemma says that there exists a subset of executions $\Omega_{u,v}$ such that:

$$\Pr[(\omega, H_2) \in \Omega_{u,v} \mid (\omega, H_2) \in \mathcal{S}'_{u,v}] \geq \frac{\alpha}{\delta} = \frac{1}{2}$$

and such that, for any $(\omega, H_2) \in \Omega_{u,v}$:

$$\Pr_{c'_k}[(\omega, H'_2, c'_k) \in \mathcal{S}'_{u,v}] \geq \delta - \alpha = \frac{\epsilon_2}{2Q_2(Q_2+1)}.$$

Assuming that the concrete execution $(\tilde{\omega}, \tilde{H'}_2, \tilde{c}_k)$ is in $\mathcal{S}'_I$, for some concrete gap index $(\tilde{u}, \tilde{v}) \in I$, then with probability greater than $1/2$, the execution is also in $\Omega_{\tilde{u},\tilde{v}}$. In this case, if we now repeat $t_2 = \left(\frac{\epsilon_2}{2Q_2(Q_2+1)} - \frac{1}{q}\right)^{-1}$ times the attack $\mathcal{A}$ with fixed $(\tilde{\omega}, \tilde{H'}_2)$ and randomly chosen $c'_k \in \mathbb{Z}_q$, we obtain with probability again greater than $3/5$ a new c'_k such that $(\tilde{\omega}, \tilde{H'}_2, c'_k) \in \mathcal{S}'_{\tilde{u},\tilde{v}}$ and such that $c'_k \neq \tilde{c}_k$.

Since we have imposed in the stating of the theorem that $\varepsilon > \frac{64Q_2^2}{q}$, we have in particular that $\frac{\epsilon_2}{2Q_2(Q_2+1)} > \frac{2}{q}$, which implies that $t_2 < \frac{4Q_2(Q_2+1)}{\epsilon_2}$.

The total probability is then $\epsilon_3 \geq \frac{3}{5} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{3}{5} = \frac{9}{100}$, and the polynomial number of repetitions of the attack $\mathcal{A}$ is

$$t_1 + t_2 < \frac{1}{\epsilon_2} + \frac{4Q_2(Q_2+1)}{\epsilon_2} < \frac{8}{\varepsilon} + \frac{8 \cdot 4 \cdot Q_2 \cdot 2Q_2}{\varepsilon} = \frac{64Q_2^2 + 8}{\varepsilon}.$$

Now consider the two successful executions of the attack $(\tilde{\omega}, \tilde{H'}_2, \tilde{c}_k)$ and $(\tilde{\omega}, \tilde{H'}_2, c'_k)$ that the algorithm $\mathcal{B}$ has obtained. Since the random tapes and H_1 are identical, and the answers of the random oracle H_2 are the same until the query $\mathcal{Q}_{\tilde{v}} = (\mathcal{U}, m, R_{k-1})$, we have in particular that the query $\mathcal{Q}_{\tilde{u}} = (\mathcal{U}, m, R_k)$, which happens before $\mathcal{Q}_{\tilde{v}}$, is also identical for the two executions. Therefore,

$$R_k = e(T_k, P) \cdot e(\tilde{c}_k PK_k, Y) = e(T'_k, P) \cdot e(c'_k PK_k, Y), \text{ with } c'_k \neq \tilde{c}_k.$$

On the other hand, with probability $1/Q_1$, the choice of the index ℓ made by $\mathcal{B}$ is a correct guess, and the public key PK_ℓ corresponds precisely to this PK_k. In particular, this means that the attacker $\mathcal{A}$ has not asked for the secret key matching with PK_ℓ, and so the CDH-solver $\mathcal{B}$ has not output "fail".

Summing up, with probability $\varepsilon' \geq \frac{9}{100\ Q_1}$ and in time $t' \leq \frac{64Q_2^2+8}{\varepsilon} t$, the algorithm $\mathcal{B}$ obtains values $T_k, T'_k, \tilde{c}_k, c'_k$ such that $e(T_k, P) \cdot e(\tilde{c}_k PK_k, Y) = e(T'_k, P) \cdot e(c'_k PK_k, Y)$, where $PK_k = PK_\ell = bP$ and $Y = aP$.

Since the pairing e is bilinear and non-degenerate, the previous equality implies that $e(T_k + \tilde{c}_k abP, P) = e(T'_k + c'_k abP, P)$ and so $T_k - T'_k = (c'_k - \tilde{c}_k)abP$. Since $c'_k \neq \tilde{c}_k$, one can compute the inverse of $c'_k - \tilde{c}_k$ modulo q, and therefore $\mathcal{B}$ obtains the solution of the CDH problem:

$$abP = \frac{1}{c'_k - \tilde{c}_k}\ (T_k - T'_k)\ \in \mathbb{G}_1.$$

□

Assuming that the Computational Diffie-Hellman problem cannot be solved in polynomial time and with non-negligible probability, this theorem implies that the Zhang and Kim's ID-based ring signature scheme is unforgeable under chosen message and identities attack.

4 Conclusions

In this work we provide a formal model to analyze the unforgeability of ID-based ring signature schemes, by defining the goals and the capabilities of an adversary against such a scheme. Then we prove that the scheme proposed by Zhang and Kim in [10] achieves this level of security, in the random oracle model.

In some way this result completes the work of Zhang and Kim. They designed the scheme and showed that it is unconditionally anonymous, but did not formally prove its unforgeability.

Furthermore, the new formal security model could be used to analyze the security of future proposals of ID-based ring signature schemes.

References

1. M. Abe, M. Ohkubo and K. Suzuki. $1-\text{out}-\text{of}-n$ signatures from a variety of keys. *Advances in Cryptology-Asiacrypt'02*, LNCS **2501**, Springer-Verlag, pp. 415–432 (2002).
2. M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. *First ACM Conference on Computer and Communications Security*, pp. 62–73 (1993).
3. E. Bresson, J. Stern and M. Szydlo. Threshold Ring Signatures for Ad-hoc Groups. *Advances in Cryptology-Crypto'02*, LNCS **2442**, Springer-Verlag, pp. 465–480 (2002).
4. S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptative chosen-message attacks. *SIAM Journal of Computing*, **17 (2)**, pp. 281–308 (1988).
5. J. Herranz and G. Sáez. Forking lemmas for ring signature schemes. *Proceedings of Indocrypt'03*, LNCS **2904**, Springer-Verlag, pp. 266–279 (2003).
6. F. Hess. Efficient identity based signature schemes based on pairings. *Proceedings of SAC'02*, LNCS **2595**, Springer-Verlag, pp. 310–324 (2002).
7. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, Vol. **13** (3), pp. 361–396 (2000).
8. R. Rivest, A. Shamir and Y. Tauman. How to leak a secret. *Advances in Cryptology-Asiacrypt'01*, LNCS **2248**, Springer-Verlag, pp. 552–565 (2001).
9. A. Shamir. Identity-based cryptosystems and signature schemes. *Advances in Cryptology-Crypto'84*, LNCS **196**, pp. 47–53 (1984).
10. F. Zhang and K. Kim. ID-base blind signature and ring signature from pairings. *Advances in Cryptology-Asiacrypt'02*, LNCS **2501**, Springer-Verlag, pp. 533–547 (2002).
11. The Pairing-Based Crypto Lounge. Web page maintained by Paulo Barreto: `http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`