A Signature Scheme with Message Recovery as Secure as Discrete Logarithm

Masayuki Abe and Tatsuaki Okamoto

NTT Laboratories
1-1 Hikari-no-oka, Yokosuka-shi, 239-0847 Japan
{abe,okamoto}@isl.ntt.co.jp

Abstract. This paper, for the first time, presents a *provably secure* signature scheme with *message recovery* based on the (elliptic-curve) *discrete logarithm*. The proposed scheme can be proven to be secure in the strongest sense (i.e., existentially unforgeable against adaptively chosen message attacks) in the random oracle model under the (elliptic-curve) discrete logarithm assumption. We give the concrete analysis of the security reduction. When practical hash functions are used in place of truly random functions, the proposed scheme is almost as efficient as the (elliptic-curve) Schnorr signature scheme and the existing schemes with message recovery such as (elliptic-curve) Nyberg-Rueppel and Miyaji schemes.

1 Introduction

1.1 Background: Digital Signature Schemes with Message Recovery

A digital signature scheme with message recovery is useful for many applications in which small messages (e.g., around 100 bits) should be signed. For example, small messages including time, date and identifiers are signed in certified email services and time stamping services. In addition, as shown in [13,14,15], the benefits of the message recovery are: direct use in other schemes such as identity-based public-key systems or key agreement protocols and natural combination with ElGamal type encryption (which may produce the so-called sign-encryption).

The existing digital signature schemes with message recovery are classified into two types: RSA based schemes (RSA type) and discrete logarithm based schemes (DL type), where an elliptic curve based signature scheme is one of the DL type. PSS-R [2] and ISO/IEC 9796-1,9796-2 are signature schemes with message recovery in the RSA type, and the Nyberg-Rueppel [13,14,15], and Miyaji [11] schemes are in the DL type.

Recently the security flaws of heuristically designed schemes such as PKCS#1 (Ver.1) and the above-mentioned RSA-based signatures with message recovery, CoronISO/IEC 9796-1 and 9796-2, have been found [3,5]. Therefore, the *provable security* even in the random oracle model is most desirable to assure the security of a practical scheme.

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 378–389, 1999.

Among the existing signature schemes with message recovery, only the PSS-R scheme [2] is provably secure (existentially unforgeable against adaptively chosen message attacks) under reasonable assumptions (the RSA assumption and random oracle model). In other words, there exists no *provably secure* signature schemes with *message recovery* in the *DL type* (i.e., no elliptic curve based signature scheme with message recovery) even in the random oracle model.

Since the overhead (size) of a digital signature based on the integer factoring should be much larger than such a small message (e.g., 1024 bit signature is much larger than 100 bit message), an elliptic curve based signature scheme is more appropriate for applications with small messages because of its small signature and key sizes.

That is, the most appropriate signature schemes with message recovery should be elliptic curve based schemes, while there exists no *provably secure* elliptic curve based signature scheme with message recovery (even in the random oracle model).

1.2 Our Result

This paper solves this problem. That is, we, for the first time, present a *provably secure* (existentially unforgeable against adaptively chosen message attacks) DL type (e.g., *elliptic curve* based) signature schemes with *message recovery* under reasonable assumptions, the (elliptic curve) discrete logarithm assumption and random oracle model. We also give the concrete analysis of the reduction to prove the security of the proposed signature scheme.

When practical hash functions are used in place of truly random functions, the proposed scheme is almost as efficient as the (elliptic-curve) Schnorr signature scheme and the existing schemes with message recovery such as (elliptic-curve) Nyberg-Rueppel and Miyaji schemes.

1.3 Related Works

Although Miyaji claimed that her scheme [11] is as secure as the elliptic curve DSA, the security level investigated in [11] is the weakest (i.e., universally unforgeable against passive attacks) and it is unlikely that her scheme is provably secure in a stronger security definition. Note that the security of signature schemes should be investigated based on the strongest security definition (i.e., existentially unforgeable against adaptively chosen message attacks) [9], in order to ensure the security against various possible attacks.

Remark: Recently Canetti et al. [4] have demonstrated that it is possible to devise cryptographic protocols which are provably secure in the random oracle model but for which no complexity assumption property instantiates the random oracle modeled hash function. However, the examples they used to make the random oracle model paradigm fail were very contrived, so the concerns induced by these examples do not appear to apply any of the concrete practical schemes that have been proven secure in the random oracle model.

2 Proposed Scheme

This section introduces our signature scheme with message recovery. Although we can construct our scheme based on any finite group, as a typical example, we will present a construction on the group over an elliptic curve because of its efficiency.

Key generation: Each signer S generates elliptic curve parameters, q for a finite field $\mathbf{F}_q$; two elliptic curve coefficients a and b, elements of $\mathbf{F}_q$, that defines an elliptic curve E; a positive prime integer p dividing the number of points on E; and a curve point G of order p. Here $|p| = k$, and set (k_1, k_2) such that $|q| = k_1 + k_2$.

Signer S uniformly selects $x \in \mathbf{Z}/p\mathbf{Z}$, and calculates a point, Y, on E, where $Y = -x{\cdot}G$. The secret key of the signer is x, and its public-key is $(\mathbf{F}_q, E, G, Y)$.

The parameters, $(\mathbf{F}_q, E, G)$, of the elliptic curve domain can be fixed by the system and shared by many signers.

(In this paper, we follow the standard notations on the elliptic curve operation: the elliptic curve addition by $+$, and $G + \cdots + G$ (x times additions) by $x{\cdot}G$.)

Signature generation: S generates the signature, (r, z), of his message $m \in \{0,1\}^{k_2}$ using public random oracle functions, $F_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$, $F_2 : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$, $H : \{0,1\}^{k_1+k_2} \to \{0,1\}^{k}$ as follows:

$$m' = F_1(m)||(F_2(F_1(m)) \oplus m),$$

$$r = (\omega{\cdot}G)_X \oplus m',$$

$$c = H(r),$$

$$z = \omega + cx \bmod p,$$

where $\omega \in \mathbf{Z}/p\mathbf{Z}$ is uniformly selected. S sends (r, z) to verifier V. Here, P_X denotes the X-coordinate of point P on E, and $\oplus$ denotes the bit-wise exclusive-or operation.

Verification: Verifier V recovers the message m from signature (r, z), and checks its validity as follows:

$$m' = r \oplus (z{\cdot}G + c{\cdot}Y)_X,$$

$$m = [m']_{k_2} \oplus F_2([m']^{k_1}),$$

and check whether $[m']^{k_1} = F_1(m)$ holds. Here, $[m']^{k_1}$ denotes the most significant k_1 bits of m', and $[m']_{k_2}$ denotes the least significant k_2 bits of m'.

Remark 1: If (r, z) is correctly generated, m should be recovered correctly and V accepts (r, z) as valid since

$$z{\cdot}G + c{\cdot}Y = \omega{\cdot}G + (cx){\cdot}G - (cx){\cdot}G = \omega{\cdot}G.$$

Remark 2: A typical security parameters for the signature scheme are: $k = |p| = 160$, $|q| = 160$, $k_1 = k_2 = 80$. Then, the message size, $|m|$, is 80 bits.

Remark 3: In order to sign a longer message (e.g., $|m| > 80$) with a fixed size of parameters of elliptic curve E (e.g., $k = |p| = 160$, $|q| = 160$, $|k_1| = |k_2| = 80$), m should be divided into two parts, m_1 and m_2 and $|m_1| = k_1$ (e.g., $|m_1| = 80$). Then, signer S generates (r, z) as follows:

$$m' = F_1(m_1)||(F_2(F_1(m_1)) \oplus m_1),$$

$$r = (\omega{\cdot}G)_X \oplus m',$$

$$c = H(r, m_2),$$

$$z = \omega + cx \bmod p.$$

Signer S sends (r, z, m_2) to verifier V. V recovers m_1 from (r, z, m_2) as follows:

$$m' = r \oplus (z{\cdot}G + H(r, m_2){\cdot}Y)_X,$$

$$m_1 = [m']_{k_2} \oplus F_2([m']^{k_1}),$$

and checks whether $[m']^{k_1} = F_1(m_1)$ holds.

Remark 4: The essential part in designing the signature scheme is how to construct the redundancy coding, m', of message m. Our coding is based on random functions (oracles), so that m' distributes uniformly over the randomness of the random functions, regardless of the distribution of m. The property based on random functions is used in the proofs of Lemmas 8 and 12. The property on the uniform distribution of m' is used in the proof of Lemma 12 (especially for Case 2).

3 Security

This section proves that the proposed signature scheme with message recovery is *existentially unforgeable against adaptively chosen message attacks* under the (elliptic-curve) discrete logarithm assumption and the random oracle model.

We will follow the proof methodology, the ID-reduction technique, introduced by [16] to analyze the reduction cost.

3.1 Security Definition of the Signature Scheme

We will quantify the security of a signature scheme: Here we assume that the attacker can dynamically ask the legitimate user S to sign any message, m, using him as a kind of oracle. This model covers the very general attack of the signature situations, *adaptively chosen message attacks.*

Definition 1. *A probabilistic Turing machine (adversary) A breaks the proposed signature scheme with $(t, q_{sig}, q_{F_1}, q_{F_2}, q_H, \epsilon)$ if and only if A can forge a signature of a message with success probability greater than ϵ . We allow chosen-message attacks in which A can see up to q_{sig} legitimate chosen signatures participating in the signature generating procedure, and allow $q_{F_1}/q_{F_2}/q_H$ invocations of $F_1/F_2/H$, within processing time t. The probability is taken over the coin flips of A, F_1, F_2, H and signing oracle S.*

Definition 2. *The proposed signature scheme is $(t, q_{sig}, q_{F_1}, q_{F_2}, q_H, \epsilon)$-secure if and only if there is no adversary that can break it with $(t, q_{sig}, q_{F_1}, q_{F_2}, q_H, \epsilon)$.*

3.2 Intractability Definition of the Elliptic Curve Discrete Logarithm Problem

Definition 3. *A probabilistic Turing machine (adversary) A breaks the elliptic curve discrete logarithm problem, $(\mathbf{F}_q, E, G, Y)$, with (t, ϵ) if and only if A can find x from $(\mathbf{F}_q, E, G, Y)$ with success probability greater than ϵ within processing time t, where $Y = x{\cdot}G$. The probability is taken over the coin flips of A. Here, $\mathbf{F}_q$ denotes a finite field with q elements, E denotes an elliptic curve over $\mathbf{F}_q$, and G is a point of E with prime order p.*

Definition 4. *The elliptic curve discrete logarithm problem, $(\mathbf{F}_q, E, G, Y)$, is (t, ϵ)-secure if and only if there is no adversary that can break it with (t, ϵ).*

3.3 Identification Scheme Induced from our Signature Scheme

Here we introduce the identification scheme that is induced from the above-mentioned signature scheme. This identification scheme is useful to analyze the concrete security of our signature scheme, since the *ID Reduction Technique* in [16] with using this induced identification scheme is very effective for the security analysis.

In the identification scheme, prover P publishes a public key while keeping the corresponding secret key, and proves his identity to verifier V. Here, functions F_1 and F_2 are shared by P and V.

(Identification Scheme)

Key generation: Prover P generates a pair of a secret key, x, and a public key, $(\mathbf{F}_q, E, G, Y)$, using a key generation algorithm $\mathcal{G}$, where $Y = -x{\cdot}G$.

Identification Protocol: P proves his identity, and verifier V checks the validity of P's proof as follows:

- P selects m and generates r as follows:

$$m' = F_1(m)||(F_2(F_1(m)) \oplus m),$$

$$r = (\omega \cdot G)_X \oplus m',$$

where $\omega \in \mathbf{Z}/p\mathbf{Z}$ is uniformly selected. S sends r to verifier V.
- V generates random challenge $c \in \{0,1\}^k$ and sends it to P.
- P generates an answer z as follows:

$$z = \omega + cx \bmod p.$$

P sends z to V
- V checks the validity of (r, z) through whether $[m']^{k_1} = F_1(m)$ holds or not, where

$$m' = r \oplus (z \cdot G + c \cdot Y)_X,$$

$$m = [m']_{k_2} \oplus F_2([m']^{k_1}).$$

3.4 Security Definition of the Identification Scheme

Definition 5. *A probabilistic Turing machine (adversary) A breaks an identification scheme with $(t, q_{F_1}, q_{F_2}, \epsilon)$ if and only if A as a prover can cheat honest verifier V with a success probability greater than ϵ within processing time t. A is allowed to make q_{F_1} (and q_{F_2}) invocations of F_1 (and F_2). Here, the probability is taken over the coin flips of A, F_1, F_2 and V.*

Definition 6. *An identification scheme is $(t, q_{F_1}, q_{F_2}, \epsilon)$-secure if and only if there is no adversary that can break it with $(t, q_{F_1}, q_{F_2}, \epsilon)$.*

3.5 ID Reduction Lemmas of the Proposed Signature Scheme

ID Reduction Technique introduced by [16] is effective to analyze the security of a certain class of signature schemes.

We can straightforwardly obtain the following lemma from the corresponding lemma in [16].

Lemma 7. (ID Reduction Lemma)
1) If A_1 breaks the proposed signature scheme with $(t, q_{sig}, q_{F_1}, q_{F_2}, q_H, \epsilon)$, there exists A_2 which breaks the signature scheme with $(t, q_{sig}, q_{F_1}, q_{F_2}, 1, \epsilon')$, where $\epsilon' = \frac{\epsilon - \frac{1}{2^k}}{q_H}$.
2) If A_2 breaks the proposed signature scheme with $(t, q_{sig}, q_{F_1}, q_{F_2}, 1, \epsilon')$, there exists A_3 which breaks the signature scheme with $(t', 0, q_{F_1}, q_{F_2}, 1, \epsilon'')$, where $\epsilon'' = \epsilon' - \frac{q_{sig}}{2^k}$ and $t' = t +$ (the simulation time of q_{sig} signatures).
3) If A_3 breaks the proposed signature scheme with $(t', 0, q_{F_1}, q_{F_2}, 1, \epsilon'')$, there exists A_4 which breaks the induced identification scheme with $(t', q_{F_1}, q_{F_2}, \epsilon'')$

We neglect the time of reading/writing data on (random, communication, etc.) tapes, simple counting, and if-then-else controls. (Hereafter in this paper, we assume them.)

To analyze our scheme, the following lemma is additionally required, since random oracles F_1 and F_2 are used and shared by P and V.

Lemma 8. (Additional Reduction Lemma)
If A_4 breaks the identification scheme with $(t', q_{F_1}, q_{F_2}, \epsilon'')$, there exists A_5 which breaks the identification scheme with $(t', 1, 1, \epsilon''')$, where $\epsilon''' = \frac{1}{q_{F_1}}(\epsilon'' - \max\{\frac{1}{2^{k_1}}, \frac{1}{2^{k_2}}\})$.

Proof. Let Q_i be the i-th query from A_4 to random oracle F_1 and ρ_i be the i-th answer from F_1 to A_4. Let $R_j = \rho_i$ be the query from A_4 to random oracle F_2, which is consistent with Q_i.

Construct A_5 using A_4 as follows:

1. Select integer i with $1 \leq i \leq q_{F_1}$ randomly.
2. Run A_4 with random oracles, F_1 and F_2, and a random working tape, Θ, where only the i-th query, Q_i, to F_1 and the related consistent query, R_j, to F_2 are asked to F_1 and F_2, and the remaining $(q_{F_1} - 1)$ queries to F_1 and $(q_{F_2} - 1)$ queries to F_2 are asked to Θ. Here Θ contains $(q_{F_1} - 1)$ k_2-bit-random-strings and $(q_{F_2} - 1)$ k_1-bit-random-strings used for answers from Θ.
3. Output the same as that of A_4 (i.e., A_5 succeeds if A_4 succeeds) if (r, z) output by A_4 satisfies the following:

$$m = Q_i, \quad [m']^{k_1} = R_j,$$

where

$$m' = r \oplus (z \cdot G + c \cdot Y)_X,$$
$$m = [m']_{k_2} \oplus F_2([m']^{k_1}).$$

Otherwise A_5 fails and halts.

If A_4 succeeds in making V accept (r, z) there are two cases: 1) m was asked to random oracle F_1 and $[m']^{k_1}$ was asked to random oracle F_2, 2) otherwise.

In the latter case, the success probability of A_4 is at most $\max\{1/2^{k_1}, 1/2^{k_2}\}$, because of the randomness of the random oracle. Thus

$$\begin{aligned}
&\Pr[A_5 \text{ succeeds}] \\
&\geq \sum_{i=1}^{q_{F_1}} \Pr[A_5 \text{ selects } i] \Pr[A_4 \text{ succeeds} \wedge (m = Q_i, \quad [m']^{k_1} = R_j)] \\
&= \sum_{i=1}^{q_{F_1}} \frac{1}{q_{F_1}} \Pr[A_4 \text{ succeeds} \wedge (m = Q_i, \quad [m']^{k_1} = R_j)] \\
&= \frac{1}{q_{F_1}} \sum_{i=1}^{q_{F_1}} \Pr[A_4 \text{ succeeds} \wedge (m = Q_i, \quad [m']^{k_1} = R_j)] \\
&= \frac{1}{q_{F_1}} (\Pr[A_4 \text{ succeeds}] - \Pr[A_4 \text{ succeeds} \wedge A_4 \text{ makes no query to } F_1 \text{ or } F_2]) \\
&\geq \frac{1}{q_{F_1}} (\epsilon'' - \max\{\frac{1}{2^{k_1}}, \frac{1}{2^{k_2}}\}),
\end{aligned}$$

because $\Pr[A_4 \text{ succeeds}] \geq \epsilon''$.

3.6 Security of the Induced Identification Scheme

A Boolean matrix and heavy row will be introduced in order to analyze the security of the above-mentioned identification scheme induced from the proposed signature scheme. Assume that there is a cheater A who can break a one-round identification scheme with $(t, 1, 1, \epsilon)$.

Here there are two cases: (Case 1) A's query to F_1 is made before sending r, and (Case 2) A's query to F_1 is made after sending r.

Let $\epsilon_1 + \epsilon_2 = \epsilon$, and A's success probability with Case 1 is at least ϵ_1 and A's success probability with Case 2 is at least ϵ_2.

Definition 9. (Boolean Matrix of (A, V))
Let's consider the possible outcomes of the execution of (A, V) as a Boolean matrix $\mathcal{H}((RA, F_1, F_2), c)$ whose rows correspond to all possible choices of (RA, F_1, F_2), where RA is a private random tape of A; its columns correspond to all possible choices of c, which means $c \in RV$, where RV is a random tape of V. Its entries are 0 if V rejects A's proof or V accepts A's proof with Case 2, and 1 if V accepts A's proof with Case 1.

Definition 10. (Heavy Row)
A row of matrix of $\mathcal{H}$ is heavy if the fraction of 1's along the row is at least $\epsilon_1/2$, where the success probability of A with Case 1 is at least ϵ_1.

Lemma 11. (Heavy Row Lemma)
The 1's in $\mathcal{H}$ are located in heavy rows of $\mathcal{H}$ with a probability of at least $\frac{1}{2}$.

Lemma 12. (Security of the identification scheme induced from the signature scheme)
Let $\epsilon \geq \frac{10}{2^k}$. Suppose that the elliptic curve discrete logarithm problem, $(\mathbf{F}_q, E, G, Y)$, is (t^*, ϵ^*)-secure. Then the identification scheme induced from the signature scheme is $(t, 1, 1, \epsilon)$-secure, where

$$t^* = \frac{6(t + \Phi_1)}{\epsilon - 2/p} + \Phi_3 \quad \textit{and} \quad \epsilon^* = \frac{1}{2}\left(1 - \frac{1}{e}\right)^2 > \frac{9}{50}.$$

Here Φ_1 is the verification time of the identification protocol, Φ_3 is the calculation time of x in the final stage of the reduction, and e is the base of the natural logarithm.

Proof. Assume that there is a cheater A who can break an identification with $(t, 1, 1, \epsilon)$. We will construct a machine A^* which breaks the elliptic curve discrete logarithm problem, $(\mathbf{F}_q, E, G, Y)$, with (t^*, ϵ^*) using A.

First, we assume that $\epsilon_1 \geq \epsilon/2$, where either case occurs, $\epsilon_1 \geq \epsilon/2$ or $\epsilon_2 > \epsilon/2$, since $\epsilon_1 + \epsilon_2 = \epsilon$. (Later we consider the case when $\epsilon_2 > \epsilon/2$.)

We will discuss the following probing strategy of $\mathcal{H}$ to find two 1's along the same row in $\mathcal{H}$ [8]:

1. Probe random entries in $\mathcal{H}$ to find an entry $a^{(0)}$ with 1. Let $c^{(0)}$ be V's challenge message corresponding to $a^{(0)}$. We denote the row where $a^{(0)}$ is located in $\mathcal{H}$ by $\mathcal{H}^{(0)}$.
2. After $a^{(0)}$ is found, probe random entries along $\mathcal{H}^{(0)}$ to find another entry with 1. We denote it by $a^{(1)}$ and $c^{(1)}$ is V's challenge message corresponding to $a^{(1)}$. If $c^{(1)} \equiv -c^{(0)} \pmod p$, then discard it and find another entry with 1.

$a^{(i)}$ represents $(r^{(i)}, z^{(i)})$. Here, $[m^{(i)\prime}]^{k_1} = F_1(m^{(i)})$ holds, since $a^{(i)}$ is an entry with 1, where

$$m^{(i)\prime} = r^{(i)} \oplus (z^{(i)}{\cdot}G + c^{(i)}{\cdot}Y)_X,$$

$$m^{(i)} = [m^{(i)\prime}]_{k_2} \oplus F_2([m^{(i)\prime}]^{k_1}).$$

Two 1's, $a^{(0)}$ and $a^{(1)}$, in the same row $\mathcal{H}^{(0)}$ means $r^{(1)} = r^{(0)}$, $m^{(1)\prime} = m^{(0)\prime}$, and $m^{(1)} = m^{(0)}$. Therefore,

$$(z^{(1)}{\cdot}G + c^{(1)}{\cdot}Y)_X = (z^{(0)}{\cdot}G + c^{(0)}{\cdot}Y)_X,$$

where $c^{(0)} \neq c^{(1)}$. That is,

$$z^{(1)}{\cdot}G + c^{(1)}{\cdot}Y = \pm(z^{(0)}{\cdot}G + c^{(0)}{\cdot}Y).$$

Hence if this strategy succeeds, x with $Y = x{\cdot}G$ can be computed by

$$x = -\frac{z^{(1)} \mp z^{(0)}}{c^{(1)} \mp c^{(0)}} \bmod p,$$

since p is prime and $c^{(1)} \not\equiv -c^{(0)} \pmod p$.

Then we will show that this strategy succeeds with constant probability in just $O(1/\epsilon_1)$ probes, using Lemma 11 concerning a useful concept, *heavy* row, defined in Definition 10.

Let p_1 be the success probability of step 1 with $\frac{1}{\epsilon_1}$ repetition. $p_1 \geq 1 - (1-\epsilon_1)^{1/\epsilon_1} = p_1' > 1 - \frac{1}{e} > \frac{3}{5}$, because the fraction of 1's in $\mathcal{H}$ is at least ϵ_1. Let p_2 be the success probability of step 2 with $\frac{2}{\epsilon_1 - 1/p}$ repetition. $p_2 \geq \frac{1}{2} \times \left(1 - (1 - \frac{\epsilon_1 - 1/p}{2})^{2/(\epsilon_1 - 1/p)}\right) = p_2' > \frac{1}{2}(1 - \frac{1}{e}) > \frac{3}{10}$, because the probability that $\mathcal{H}^{(0)}$ is heavy is at least $\frac{1}{2}$ by Lemma 11 and the fraction of 1's (with $c^{(1)} \not\equiv -c^{(0)} \pmod p$) along a heavy row is at least $\frac{\epsilon_1 - 1/p}{2}$.

Let ϵ_1^* be the success probability of the above-mentioned procedure and t_1^* be the running time for procedure. Then

$$\epsilon_1^* = p_1 \times p_2 \geq p_1' \times p_2' > \frac{1}{2}(1 - \frac{1}{e})^2 > \frac{9}{50},$$

$$t_1^* \leq (t + \Phi_1) \times (\frac{1}{\epsilon_1} + \frac{2}{\epsilon_1 - 1/p}) + \Phi_3$$

$$< \frac{3(t + \Phi_1)}{\epsilon_1 - 1/p} + \Phi_3$$

$$\leq \frac{6(t+\Phi_1)}{\epsilon - 2/p} + \Phi_3.$$

Next, we consider the case when $\epsilon_2 > \epsilon/2$. Then A's success probability with Case 2 (A's query to F_1 is made after sending r) is greater than $\epsilon/2$.

Execute random trials of $((RA, F_1, F_2), c)$ to find a value of $((RA, F_1, F_2), c)$ in which A succeeds with Case 2. Here in each trial, the replies of F_1 and F_2 are set as follows: F_1's reply: $[m']^{k_1}$, and F_2's reply: $[m']_{k_2}$, where $m' = (\delta{\cdot}G)_X \oplus r$ and δ is uniformly selected from $\mathbf{Z}/p\mathbf{Z}$. Here note that although the distribution of m' is not guaranteed to be uniform (since $(\delta{\cdot}G)_X$ is not uniform), A succeeds with Case 2 only when the values of m' is in the distribution of $(\delta{\cdot}G)_X \oplus r$. Therefore, the success probability of A with Case 2 under the above-mentioned strategy of F_1 and F_2 is at least that under the uniform distribution of F_1 and F_2 (i.e., greater than $\epsilon/2$).

If a value of $((RA, F_1, F_2), c)$ in which A succeeds with Case 2 is found, x with $Y = x{\cdot}G$ can be computed by $x = (-z \pm \delta)/c \bmod p$, since $(z{\cdot}G + c{\cdot}Y)_X = m' \oplus r = (\delta{\cdot}G)_X$.

Let ϵ_2^* be the success probability of the above-mentioned procedure and t_2^* be the running time for procedure.

$$\epsilon_2^* \geq 1 - (1-\epsilon/2)^{2/\epsilon} = p_1' > 1 - \frac{1}{e} > \frac{3}{5},$$

$$t_2^* \leq (t+\Phi_1) \times \frac{2}{\epsilon} + \Phi_3.$$

Since the first step in the probing stage with Case 1 and the probing stage with Case 2 can be merged as the unified probing stage, we can obtain the total success probability and running time as follows:

$$t^* = \frac{6(t+\Phi_1)}{\epsilon - 2/p} + \Phi_3 \quad \text{and} \quad \epsilon^* = \frac{1}{2}\left(1 - \frac{1}{e}\right)^2 > \frac{9}{50},$$

because $t_1^* > t_2^*$ and $\epsilon_1^* < \epsilon_2^*$.

3.7 Security of the Proposed Signature Scheme

The following theorem is proven by combining Lemmas 7, 8 and 12.

Theorem 13. (Security of the proposed signature scheme) *Let $\epsilon \geq q_H(\frac{10q_{F_1}+q_{sig}}{2^k} + \max\{\frac{1}{2^{k_1}}, \frac{1}{2^{k_2}}\}) + \frac{1}{2^k}$. Suppose that the elliptic curve discrete logarithm problem, $(\mathbf{F}_q, E, G, Y)$, is (t^*, ϵ^*)-secure. Then the proposed signature scheme with message recovery is $(t, q_{sig}, q_{F_1}, q_{F_2}, q_H, \epsilon)$-secure, where*

$$t^* = \frac{6t'}{\epsilon''' - 2/p} + \Phi_3 \quad \textit{and} \quad \epsilon^* = \frac{1}{2}\left(1 - \frac{1}{e}\right)^2 > \frac{9}{50}.$$

Here

$$t' = t + \Phi_1 + \Phi_2 \qquad \textit{and} \qquad \epsilon''' = \frac{1}{q_{F_1}}(\frac{\epsilon - \frac{1}{2^k}}{q_H} - \frac{q_{sig}}{2^k} - \max\{\frac{1}{2^{k_1}}, \frac{1}{2^{k_2}}\})$$

where Φ_1 is the verification time of the identification protocol, Φ_2 is the simulation time of q_{sig} signatures, Φ_3 is the calculation time of x in the final stage of the reduction.

Remark: This theorem implies in an asymptotic sense that the proposed signature scheme with message recovery is *existentially unforgeable against adaptively chosen massage attacks* in the *random oracle model*, if the elliptic curve discrete logarithm (ECDL) problem, $(\mathbf{F}_q, E, G, Y)$, is *intractable*. This is because: if ECDL is intractable (i.e., t^* is not within k^{c_1} for constant c_1 with constant ϵ^*), it is not true that t is within k^{c_2} for constant c_2 and ϵ is at least $\frac{1}{k^{c_3}}$ for constant c_3, where $q_{sig}, q_{F_1}, q_{F_2}, q_H$ are at most polynomials in k, and $k_1 = c_4 k$ and $k_2 = c_5 k$ for constants c_4 and c_5.

4 Conclusion

This paper presented a *provably secure* signature scheme with *message recovery* based on the (elliptic-curve) *discrete logarithm*. The proposed scheme is proven to be secure in the strongest sense (i.e., existentially unforgeable against adaptively chosen message attacks) in the random oracle model under the (elliptic-curve) discrete logarithm assumption. We provided the concrete analysis of the security reduction. When practical hash functions are used in place of truly random functions, the proposed scheme is almost as efficient as the (elliptic-curve) Schnorr signature scheme and the existing schemes with message recovery such as (elliptic-curve) Nyberg-Rueppel and Miyaji schemes (because the additional computation of our scheme compared with the Schnorr signature scheme is just the function evaluation of F_1 and F_2, and data comparison).

References

1. M. Bellare and P. Rogaway, “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols,” Proc. of the First ACM Conference on Computer and Communications Security, pp.62–73, 1993.
2. M. Bellare and P. Rogaway, “The Exact Security of Digital Signatures –How to Sign with RSA and Rabin,” Proc. of Eurocrypt’96, Springer-Verlag, LNCS, pp.399–416, 1996. 378, 379
3. D. Bleichenbacher, “Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1,” Proc. of Crypto’98, LNCS 1462, Springer-Verlag, pp. 1–12, 1998. 378
4. R. Canetti, O. Goldreich and S. Halevi, “The Random Oracle Methodology, Revisited,” Proc. of STOC, ACM Press, pp.209–218, 1998. 379
5. J.S. , D. Naccache and J.P. Stern, “On the Security of RSA Padding,” Proc. of Crypto’99, Springer-Verlag, LNCS, 1999. 378
6. T. ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Transactions on Information Theory, IT-31, 4, pp.469–472, 1985.
7. A. Fiat and A. Shamir, “How to Prove Yourself,” Proc. of Crypto’86, Springer-Verlag, LNCS, pp.186–194.

8. U. Feige, A. Fiat and A. Shamir, "Zero-Knowledge Proofs of Identity," J. of Cryptology, 1, p.77–94, 1988. 385
9. S. Goldwasser, S. Micali and R. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. on Computing, 17, pp.281–308, 1988. 379
10. N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, 48, pp.203–209, 1987.
11. A. Miyaji, "A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves," Proc. of Asiacrypt'96, Springer-Verlag, LNCS, pp. 1–14, 1996. 378, 379
12. M. Naor and M. Yung, "Universal One-Way Hash Functions and Their Cryptographic Applications," Proc. of STOC, pp.33–43, 1989.
13. K. Nyberg and R.A. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery," Proc. of the First ACM Conference on Computer and Communications Security, 1993. 378
14. K. Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Proc. of Eurocrypt'94, Springer-Verlag, LNCS, pp.182–193, 1995. 378
15. K. Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Designs, Codes and Cryptography, 7, pp.61–81, 1996. 378
16. K. Ohta and T. Okamoto, "On the Concrete Security Treatment of Signatures Derived from Identification," Proc. of Crypto'98, Springer-Verlag, LNCS, 1998. 381, 382, 383
17. D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. of Eurocrypt'96, Springer-Verlag, LNCS, pp.387–398, 1996.
18. J. Rompel, "One-Way Functions are Necessary and Sufficient for Secure Signature," Proc. of STOC, pp.387–394, 1990.
19. R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of ACM, 21, 2, pp.120-126, 1978.
20. C.P. Schnorr, "Efficient Identification and Signatures for Smart Card," Proc. of Eurocrypt'89, Springer-Verlag, LNCS, pp.235–251, 1990.