DSA と同値なメッセージ復元型署名

宮地 充子

松下電器産業 (株)　マルチメディア開発センター
〒 571 大阪府 門真市 門真 1006 番
Email:miyaji@isl.mei.co.jp

最近，Nyberg-Rueppel により離散対数問題に基づくメッセージ復元型署名が初めて提案された ([12, 13]). この署名方式は，公開鍵証明書や鍵共有など転送データサイズや保管データサイズが重要な応用にとって有効な署名方式である．しかしながら発表されて間がないので，ElGamal や DSA のようにその安全性が広く受け入れられていない．本論文では，署名方式の同値なクラスについて議論し，メッセージ復元型署名で ElGamal や DSA と同値なものが構成できたので報告する．

離散対数問題，メッセージ復元型署名，攻撃

A message recovery signature scheme equivalent to DSA

Atsuko Miyaji

Multimedia Development Center
Matsushita Electric Industrial Co.,LTD.
1006, Kadoma, Kadoma-shi, Osaka, 571, Japan
Email:miyaji@isl.mei.co.jp

The ElGamal signature([3]) is based on the difficulty of the discrete logarithm problem(DLP). For the ElGamal signature scheme, many variants like the NIST Digital Signature Algorithm(DSA)([10]) and a new signature with a message recovery feature([12]) are proposed. The message recovery feature has the advantage of small signed message length, which is effective especially in applications like identity-based public key system([4]) and the key exchange protocol([2]). However, its security is not widely accepted because it has been only a few years since the scheme was proposed. Even the relative security between the new message recovery scheme and already-existing schemes is scarcely known. In this paper, we make a strict definition of a conception of equivalent classes([14]) between signature schemes. We prove that ElGamal is not strongly equivalent to DSA according to this definition. We show that an elliptic curve gives the message recovery signature equivalent to both DSA and ElGamal.

discrete logarithm problems, message-recovery signature, attack

1 Introduction

The ElGamal signature([3]) is based on the difficulty of the discrete logarithm problem(DLP). For the ElGamal signature schemes, many variants like the NIST Digital Signature Algorithm(DSA) [10] are proposed, any of which does not have a message recovery feature. Recently new variants with the message recovery feature are proposed([12]), which have an advantage of smaller signed message length. Therefore they are effective especially in applications like identity-based public key system([4]) and the key exchange protocol([2]). However, the new signatures have stood only for a few years, so its security is not widely accepted. Therefore we would construct an ElGamal-type message recovery signature whose security is proved to be equivalent to a widely known signature like ElGamal or DSA with some criterion. A conception is proposed to investigate the security relation between signature schemes([14]). The conception is useful, but it needs to be discussed more strictly.

In this paper, we make a strict definition of the conception of equivalent classes between signature schemes and show that ElGamal is not strongly equivalent to DSA according to this definition. The reason why a new attack([1]), called Bleichenbacher-attack, works for ElGamal but not for DSA can be also explained well by the conception. We found that the relation between modulo-p arithmetic and modulo q-arithmetic is important for the equivalences between ElGamal-type signatures, where $\mathbb{F}_p = GF(p)$ is an underlying field and q is the order of a basepoint. We know the ElGamal-type signatures can be also constructed on an elliptic curve([6, 7]), which have a good feature that they can be implemented in smaller size than finite fields([5]). We also know they have another remarkable feature that elliptic curve signatures can choose various modulo-q arithmetics on an underlying field $\mathbb{F}_p$. By using the feature, we show that the message recovery signature on a special elliptic curve is strongly equivalent to DSA on it.

This paper is organized as follows. Section 2 summarizes ElGamal, DSA and message recovery signature. Section 3 discusses the conception of security equivalent and some equivalent classes based on it. Section 4 investigates the security equivalent classes of signatures defined on elliptic curve, and also shows an elliptic curve gives the message recovery equivalent to DSA.

2 ElGamal, DSA and message recovery signature

This section summarizes ElGamal, DSA, and the message recovery signature called MR in this paper. We assume that in any signature schemes, the trusted authority uses system parameters, that are a large prime p, a large prime factor q of $p-1$ and a basepoint $g \in \mathbb{F}_p = GF(p) = \{0, \ldots, p-1\}$ whose order is q. These system parameters are known to all users. The signer Alice has a secret key x_A and publishes its corresponding public key $y_A = g^{x_A} \pmod p$. The original ElGamal signature([3]) uses a generator of $\mathbb{F}_p^* = \{1, \ldots, p-1\}$ as a basepoint. However for practical purposes([17, 14]), we use the above basepoint in $\mathbb{F}_p$. Here we summarize how each signature scheme is defined for a message $m \in \mathbb{F}_p^*$.

ElGamal

She chooses a random number $k \in \mathbb{F}_q^*$, and computes $r_1 = g^k \pmod p$ and $r_1' = r_1 \pmod q$. Then she computes $s \in \mathbb{F}_q^*$ from

$$sk = m + r_1' x_A \pmod q. \tag{1}$$

Here if $s = 0$, then she chooses the random number k again. Of course such a probability is negligibly small. Then the triplet $(m; (r_1, s))$ constitutes the signed message. The signature verification is done by checking that $(r_1, s) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ and the next equation,

$$r_1^s = g^m y_A^{r_1'} \pmod{p}. \tag{2}$$

We make the sign + of r_1' in Equation (1) coincide with that of DSA since the following discussion holds regardless of signs.

DSA

She chooses a random number $k \in \mathbb{F}_q^*$, and computes $r_1 = g^k \pmod{p}$ and $r_1' = r_1 \pmod{q}$. Then she computes $s \in \mathbb{F}_q^*$ from Equation (1). Here if $r_1' = 0$ or $s = 0$, then she chooses the random number k again. Then the triplet $(m; (r_1', s))$ constitutes the signed message. The signature verification is done by checking $(r_1', s) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ and the next equation,

$$r_1' = (g^{m/s} y_A^{r_1'/s} \pmod{p}) \pmod{q}. \tag{3}$$

Here we summarize Bleichenbacher-attack([1]) over ElGamal.

Bleichenbacher-attack:

Assume that a forger knows $\beta \in \mathbb{F}_p^*$ such as $\beta = 0 \pmod{q}$ and $\beta^t = g \pmod{p}$ for a known $t \in \mathbb{F}_q^*$. For $\forall m \in \mathbb{F}_p^*$, he sets $r_1 = \beta$ and $s = tm \pmod{q}$. Then (r_1, s) is a valid signature on m since $g^m y_A^{r_1} r_1^{-s} = g^m g^{-tm/t} = 1$.

For a given $\mathbb{F}_p$ and g, it would be difficult to find the above β. However, an authority can generate $\mathbb{F}_p$ and g with a trapdoor β by repeating a natural trial([1]): first set $\mathbb{F}_p$, a large prime $q|p-1$, and $p - 1 = qn$, next find $\beta = lq$ $(l \in \{1, \cdots, n-1\})$ such that the order of β is q, then set a basepoint $g = \beta^t$ for $1 < t < q - 1$. Generally, n is sufficiently large, so this algorithm may work well. Apparently the existence of the trapdoor β cannot be recognized easily. In the case of DSA-signature, such $r_1 = \beta$ is already removed. Therefore DSA is strong against the attack.

MR

MR can be derived from ElGamal by adding the message-mask equation (4) and replacing m (resp. r_1') by 1 (resp. r_2') in Equation (1). To sign a message $m \in \mathbb{F}_p^*$, she chooses a random number $k \in \mathbb{F}_q^*$, and computes $r_1 = g^k \pmod{p}$, and

$$r_2 = m^{-1} r_1 \pmod{p}. \tag{4}$$

Then she sets $r_2' = r_2 \pmod{q}$, and computes $s_m \in \mathbb{F}_q^*$ from

$$s_m k \equiv 1 + r_2' x_A \pmod{q}. \tag{5}$$

Here if $r_2 = 0$ or $s_m = 0$, then she chooses the random number k again. Then the signature is given by (r_2, s_m). The message can be recovered by checking $(r_2, s_m) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ and computing a recovery equation

$$m = g^{1/s_m} y_A^{r_2'/s_m} r_2^{-1} \pmod{p}. \tag{6}$$

Another message-mask equation $r_2 = m r_1^{-1} \pmod{p}$ and other signature equations are also proposed in [14]. The following discussion also holds for the message-mask equation and the signature equations in almost the same way.

3 Security equivalent classes

A conception of equivalent classes between signature schemes is proposed([14]). In this section, we will make a strict definition of this conception and discuss the security equivalent classes between signature schemes.

Let S1 and S2 be two signature schemes, I be a public information necessary for verifying these signatures. Then in order to forge a valid Alice's S1- or S2-signature for a given m without the knowledge of her secret key, we have to solve the next two problems, $\texttt{Pr\_S1}(I, m)$ or $\texttt{Pr\_S2}(I, m)$ respectively, where

$\texttt{Pr\_S1}(I, m)$ is the problem that on input I and m, outputs a valid S1-signature $\mathrm{S1}(m)$ of Alice,
$\texttt{Pr\_S2}(I, m)$ is the problem that on input I and m, outputs a valid S2-signature $\mathrm{S2}(m)$ of Alice.

Then the next proposition shows that the equivalence between $\texttt{Pr\_S1}(I, m)$ and $\texttt{Pr\_S2}(I, m)$ is related with transformability between two signatures S1 and S2.

Proposition 1 *(1) If any S1-signature can be transformed into an S2-signature by a function f in (expected) time polynomial in the size of public information for verifying S1-signature without knowledge of the secret key, then* $\texttt{Pr\_S2}(I, m)$ *is (expected) polynomial-time reducible to* $\texttt{Pr\_S1}(I, m)$.
(2) If any S1-signature can be transformed into an S2-signature by a function f in (expected) time polynomial in the size of public information for verifying S1-signature, and vice versa, without knowledge of the secret key, then $\texttt{Pr\_S1}(I, m)$ *and* $\texttt{Pr\_S2}(I, m)$ *are equivalent with respect to the (expected) polynomial-time Turing reducibility.*

proof: (1) For input I and m, output $\texttt{Pr\_S2}(I, m) := f(\texttt{Pr\_S1}(I, m))$. Since f runs in a (expected) polynomial-time, $\texttt{Pr\_S2}(I, m)$ is (expected) polynomial-time reducible to $\texttt{Pr\_S1}(I, m)$.
(2) It follows immediately from the discussion of (1).

From Proposition 1, we define "strong equivalences" between signature schemes as follows.

Definition 1 *Two signature schemes S1 and S2 are called strongly equivalent if any S1-signature can be transformed into an S2-signature in (expected) time polynomial in the size of public information for verifying S1-signature, and vice versa, without knowledge of the secret key.*

Note that the transitive law holds in strong equivalences: for three signature schemes S1, S2 and S3, if S1 and S2, and, S2 and S3 are strongly equivalent respectively, then S1 and S3 are strongly equivalent. In order to show that two signature schemes are strongly equivalent, we must show that any signature for a scheme can be transformed into another and vice versa. In [14], DSA and ElGamal were erroneously said to be strongly equivalent since they did not investigate ElGamal signatures that are not transformed into DSA signatures. The following theorem will show the correct relation between ElGamal and DSA.

Theorem 1 *Any DSA signature can be transformed in time polynomial in $|p|$ to an ElGamal signature without knowledge of the secret key, but some ElGamal signatures cannot be transformed. (i.e. DSA and ElGamal are not strongly equivalent.) If we add the condition of $r_1 \neq 0 \pmod q$ both to the signature generation and verification of ElGamal, then ElGamal is strongly equivalent to DSA.*

proof: Let $(r_1', s) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ be a DSA signature on $m \in \mathbb{F}_p^*$. First set

$$r_1 = g^{m/s} y_A^{r_1'/s} \pmod{p}.$$

Then (r_1, s) is an ElGamal signature on m since $(r_1, s) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$.

On the other hand, let $(r_1, s) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ be an ElGamal signature on $m \in \mathbb{F}_p^*$ such as $q | r_1$. Then the signature cannot be transformed explicitly to DSA signature since $r_1' = r_1 \pmod{q} = 0$. Therefore ElGamal is not strongly equivalent to DSA. Apparently if the condition of $r_1 \neq 0 \pmod{q}$ is added to both the signature generation and verification of ElGamal, then the ElGamal signature which cannot be transformed to DSA is removed. Therefore it is strongly equivalent to DSA.

Theorem 1 says that `Pr_ElGamal`(g, y_A, m) is polynomial-time reducible to `Pr_DSA`(g, y_A, m), but the opposite is not. In this sense we would say that DSA is stronger against attacks than ElGamal. Bleichenbacher-attack, which works for ElGamal but not for DSA, reflects this relation well. Theorem 1 also makes clear the condition on which ElGamal is made strongly equivalent to DSA, so we would say that the security relation between ElGamal and DSA become clear.

The relation between MR and DSA is correctly pointed out not to be strongly equivalent([14]). Here we summarize why MR is not strongly equivalent to DSA. We can make r_2 of MR-signature transform into r_1' of DSA-signature. But s_m of MR cannot be transformed into s of DSA by the following reason. The signature equation is computed on the modulo-q arithmetic, while the message-mask equation (4) in MR is computed on the modulo-p arithmetic. Therefore the next relation between the modulo-p arithmetic and the modulo-q arithmetic, that is

$$(m^{-1} r_1 \pmod{p}) \pmod{q} \neq m^{-1} r_1 \pmod{q}, \tag{7}$$

reduces non-equivalences. By the same reason, MR and ElGamal are not strongly equivalent. To sum up, we don't know the relative security of MR to DSA or ElGamal. We cannot guarantee the security of MR by either DSA or ElGamal, either.

We have seen that Bleichenbacher-attack works for ElGamal but not for DSA since they are not strongly equivalent. In the same way, we show an attack, called the redundancy attack, that works for MR but not for either DSA or ElGamal.

Redundancy attack

Assume that a forger gets Alice's MR-signature (r_2, s_m) for a message m. Then the forger can compute an MR-signature $(\tilde{r}_2, \tilde{s}_m)$ for a message $\tilde{m}$ without the knowledge of Alice's secret key by the following way:

1. computes $g^{1/s_m} y_A^{r_2'/s_m} = r_1 \pmod{p}$.
2. chooses any number $n \in \mathbb{F}_p$ such that $\tilde{r}_2 = r_2' + nq < p$. (There are about $|p/q|$ variants.)
3. sets a message $\tilde{m} = r_1 \tilde{r}_2^{-1} \pmod{p}$ and $\tilde{s}_m = s_m$.
4. sends $(\tilde{r}_2, \tilde{s}_m)$ as a signature of $\tilde{m}$.

We see that $(\tilde{r}_2, \tilde{s}_m)$ is a valid MR-signature for $\tilde{m}$ since

$$g^{1/\tilde{s}_m} y_A^{\tilde{r}_2/\tilde{s}_m} \tilde{r}_2^{-1} = r_1 \tilde{r}_2^{-1} = \tilde{m} \pmod{p}.$$

The redundancy attack utilizes the next facts: (i) there is redundancy between the signature $r_2 \in \mathbb{F}_p^*$ and the necessary value r_2' for Equation (5); (ii) the redundancy enables a forger to construct a new message $\tilde{m}$ and the valid signature $(\tilde{r}_2, \tilde{s}_m)$ by setting $\tilde{r}_2 \equiv r_2 \pmod{q}$ (and $\tilde{r}_2 \neq r_2$), $\tilde{s}_m = s_m$ and $\tilde{m} = r_1 \tilde{r}_2^{-1}$ (using Equation (4)). However, the fact (i) does not hold for r_1' of DSA, and the fact (ii) does not hold in ElGamal for lack of the message-mask equation (4). This is why the redundancy attack works for MR, but not for either DSA and ElGamal.

The redundancy attack is not a serious attack because it is an existential attack. However, there might exist another attack against MR that does not work for DSA since MR is not strongly equivalent to DSA. Especially it has been only a few years since MR was proposed, so its security is not widely accepted. If a message recovery signature is shown to be strongly equivalent to a widely known signature scheme like DSA, it would be safe to say that its security is guaranteed by DSA.

4 Aspect of elliptic curves in signature schemes

The ElGamal-type signatures can be constructed in other groups, as long as DLP is hard. So ElGamal, DSA, and MR can be also constructed on an elliptic curve, which are called ECElG, ECDSA, and ECMR respectively in this paper.

Elliptic curves, chosen suitably, can be implemented in smaller size than finite fields since the most serious attacks defined on finite fields cannot be applied to elliptic curves([11]). Furthermore there is a remarkable difference in conditions of the order q of a basepoint between elliptic curves and finite fields. In the case of finite fields, q is limited to a divisor of $p-1$. On the other hand, in the case of elliptic curves $E/\mathbb{F}_p$, q is chosen randomly in the range determined by Hasse's theorem([18]): $p+1-2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p+1+2\sqrt{p}$. For example, we can choose a basepoint $G \in E(\mathbb{F}_p)$ with the order $q > p$, which is impossible in the case of finite fields. In the previous section, we saw that the relation between the modulo-p arithmetic and the modulo-q arithmetic is important for the equivalence between signature schemes. Therefore such characteristics might be suitably used on signature schemes.

We assume that the trusted authority chooses an elliptic curve $E/\mathbb{F}_p$ and a basepoint $G \in E(\mathbb{F}_p)$ with a prime order q. The signer Alice has a secret key x_A and publishes the corresponding public key $Y_A = x_A G$. Here we summarize how each signature scheme is defined for a message $m \in \mathbb{F}_p^*$. The following discussion also holds in the case of $E/\mathbb{F}_{2^r}$.

ECElG

She chooses a random number $k \in \mathbb{F}_q^*$, and computes

$$R_1 = kG, \tag{8}$$

in E. Then she sets $r_1' = x(R_1) \pmod{q}$ and computes $s \in \mathbb{F}_q^*$ from Equation (1), where $x(R_1)$ denotes the x-coordinate of R_1. Here if $x(R_1) = 0$ or $s = 0$, then she chooses the random number k again. Then the triplet $(m; (R_1, s))$ constitutes the signed message. The signature verification is done by checking $x(R_1) \in \mathbb{F}_p^*$, $s \in \mathbb{F}_q^*$, and the next equation in E,

$$sR_1 = mG + r_1' Y_A, \tag{9}$$

where $r_1' = x(R_1) \pmod{q}$.

ECDSA
She chooses a random number $k \in \mathbb{F}_q^*$, computes Equation (8), and sets

$$r_1' = x(R_1) \pmod{q}. \tag{10}$$

Then she computes $s \in \mathbb{F}_q^*$ from Equation (1). Here if $r_1' = 0$ or $s = 0$, then she chooses the random number k again. Then the triplet $(m; (r_1', s))$ constitutes the signed message. The signature verification is done by checking $r_1', s \in \mathbb{F}_q^*$ and the next equation,

$$r_1' = x(\frac{m}{s}G + \frac{r_1'}{s}Y_A) \pmod{q}. \tag{11}$$

ECMR
She chooses a random number $k \in \mathbb{F}_q^*$, and computes Equation (8). Then she sets

$$r_2 = m^{-1}x(R_1) \pmod{p}, \tag{12}$$

$r_2' = r_2 \pmod{q}$ and computes $s_m \in \mathbb{F}_q^*$ from Equation (5). Here if $r_2 = 0$ or $s_m = 0$, then she chooses the random number k again. Then the signature is given by (r_2, s_m). The message can be recovered by checking $r_2 \in \mathbb{F}_p^*$ and $s_m \in \mathbb{F}_q^*$, and computing the recovery equation

$$m = x(\frac{1}{s_m}G + \frac{r_2'}{s_m}Y_A)r_2^{-1} \pmod{p}. \tag{13}$$

4.1 Equivalences among ECElG, ECDSA and ECMR

We discuss the strong equivalent classes between elliptic curve signature schemes. The equivalent classes are different according to the choice of elliptic curves. In this section, we deal with elliptic curves except for a special elliptic curve $E/\mathbb{F}_p$ with p-elements([8, 9]). For these dealed elliptic curves, the order q of G is always different from p from Hasse's theorem. As for the special elliptic curve, we will discuss in the next section.

Theorem 2 *(i) Any ECDSA signature can be transformed in time polynomial in $|p|$ to an ECElG signature without knowledge of the secret key.*
(ii) If $q > p$, then ECElG is strongly equivalent to ECDSA.
If $q < p$, then there exists ECElG that is not strongly equivalent to ECDSA.
(iii) If $p \neq q$, ECMR is not strongly equivalent to either ECDSA or ECElG.

proof: (i) Let (r_1', s) be an ECDSA signature on $m \in \mathbb{F}_p^*$. First compute

$$R_1 = \frac{m}{s}G + \frac{r_1'}{s}Y_A,$$

in E. Then (R_1, s) is an ECElG signature on m. In fact, (R_1, s) satisfies $x(R_1) \in \mathbb{F}_p^*$ and $s \in \mathbb{F}_q^*$ since $r_1' = x(R_1) \pmod{q}$ satisfies $r_1' \neq 0$.
(ii) Let (R_1, s) be an ECElG signature on $m \in \mathbb{F}_p^*$. First set $r_1' = x(R_1) \pmod{q}$. In the case of $q > p$, $x(R_1)$ satisfies $1 \leq x(R_1) \leq p - 1 < q$. So $r_1' = x(R_1)$. Therefore $(r_1's)$ is an ECDSA signature on m. Thus ECElG is strongly equivalent to ECDSA.

On the other hand, in the case of $q < p$, there exists an elliptic curve $E/\mathbb{F}_p$ with $E(\mathbb{F}_p) \ni R_1$ such as $x(R_1) \neq 0$ and $q|x(R_1)$. In the same way as Theorem 1, a signature with R_1 cannot be

transformed into an ECDSA signature. Therefore for $E/\mathbb{F}_p$ with $E(\mathbb{F}_p) \ni R_1$ such as $x(R_1) \neq 0$ and $q|x(R_1)$, ECElG is not strongly equivalent to ECDSA.
(iii) From the assumption of E, the order q is different from p. Therefore in the same way as the case of finite fields, the next relation between the modulo-p arithmetic and the modulo-q arithmetic, that is

$$(m^{-1}x(R_1) \pmod p) \pmod q \neq m^{-1}x(R_1) \pmod q, \tag{14}$$

reduces non-equivalences.

We can construct $E/\mathbb{F}_p$ and G with $q > p$, on which ECElG is strongly equivalent to ECDSA, since constraint of the order q is loose for elliptic curves. Furthermore we will show that ECElG, ECDSA, and ECMR on a special elliptic curve $E/\mathbb{F}_p$ are all strongly equivalent each other in the next section.

4.2 Message recovery signature equivalent to ECDSA

We deal with an elliptic curve $E/\mathbb{F}_p$ which has p-elements over $\mathbb{F}_p$, denoted E_p in this paper. Such an elliptic curve can be constructed as easily as the other elliptic curve([8, 9]). Then the system parameters are: an elliptic curve $E_p/\mathbb{F}_p$, a basepoint $G \in E_p(\mathbb{F}_p)$ whose order is p. For the equivalences among ECElG, ECDSA, and ECMR on $E_p/\mathbb{F}_p$, we have the next result.

Theorem 3 *Let $E_p/\mathbb{F}_p$ be an elliptic curve with $\#E_p(\mathbb{F}_p) = p$. For signature schemes on E_p, ECElG, ECDSA, and ECMR are strongly equivalent each other.*

proof: We show the next two facts,
(i) ECElG is strongly equivalent to ECDSA,
(ii) ECMR is strongly equivalent to ECDSA.
Then from the transitive law, ECElG, ECDSA, and ECMR are strongly equivalent each other.
(i) Any ECDSA signature can be transformed into an ECElG from Theorem 2. On the other hand, let (R_1, s) be an ECElG signature on a message $m \in \mathbb{F}_p^*$. We set $r_1' = x(R_1)$. Then (r_1', s) is a DSA signature since $r_1' \neq 0$. Thus ECElG is strongly equivalent to ECDSA.
(ii) Let (r_1', s) be an ECDSA signature on $m \in \mathbb{F}_p^*$. We set

$$R_1 = \frac{m}{s}G + \frac{r_1'}{s}Y_A,\ r_2 = m^{-1}r_1' \pmod p, \text{ and } s_m = s/m \pmod p.$$

Then $x(R_1) = r_1'$, and $(r_2, s_m) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ since $(r_1', s) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$, and m is recovered as follows,

$$m = x(\frac{1}{s_m}G + \frac{r_2}{s_m}Y_A)r_2^{-1}.$$

So (r_2, s_m) is an ECMR signature. Conversely, let (r_2, s_m) be an ECMR signature on $m \in \mathbb{F}_p^*$. We compute

$$R_1 = \frac{1}{s_m}G + \frac{r_2}{s_m}Y_A,$$

and recover $m = x(R_1)r_2^{-1}$. Then we set $s = ms_m \pmod p$ and $r_1' = x(R_1)$. Then $(r_1', s) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ since $r_2 = m^{-1}x(R_1) \pmod p \neq 0$. So (r_1', s) is an ECDSA signature. Thus ECMR is strongly equivalent to ECDSA.

ElGamal-type signature requires two modulo arithmetics. One is modulo-p arithmetic in underlying field $\mathbb{F}_p$. The other is modulo-q arithmetic for the order q of a basepoint. In ElGamal-type signature, the two modulo arithmetics are not independent. In fact a result of modulo-p arithmetic is the input for the next modulo-q arithmetic. In the case of a finite field, the relation between these two modulo arithmetics, as we see in Equation (7), makes the equivalences among signature schemes impossible. On the other hand, in the case of elliptic curves the order q is chosen randomly in the range determined by Hasse's theorem. Therefore there exists the above $E_p/\mathbb{F}_p$ with p elements. For such an elliptic curve, two modulo arithmetics are the same. This is why ECElG, ECDSA, and ECMR are strongly equivalent each other. This is an advantage of elliptic curves over finite fields.

As a concluding remark of Section 4, we discuss $E/\mathbb{F}_p$ and G which satisfies $q \geq p$. From Theorem 2 and 3, we see that if $q \geq p$, then ECElG is strongly equivalent to ECDSA. From Hasse's theorem, an elliptic curve with $q \geq p$ is limited to a prime-order elliptic curve, that is $\#E(\mathbb{F}_p) = q$. It is interesting that, for a prime-order elliptic curve, another feature is proved([16]). In the case of $E/\mathbb{F}_{2^r}$, we cannot generate such a prime-order elliptic curve by an usual construction of using Weil-conjecture: lifting E over a lower field, for example $E/\mathbb{F}_2$ or $E/\mathbb{F}_{2^2}$, to $E/\mathbb{F}_{2^r}$. Then $E(\mathbb{F}_{2^r})$ is never a prime-order since $\#E(\mathbb{F}_{2^r})$ is always divisible by the lifted $\#E(\mathbb{F}_2)$ or $\#E(\mathbb{F}_{2^2})$ respectively.

5 Conclusion

In this paper, we have strictly analyzed strong equivalences between signature schemes. We have proved that $\mathtt{Pr\_ElGamal}(g, y_A, m)$ is polynomial time reduced to $\mathtt{Pr\_DSA}(g, y_A, m)$ and shown that ElGamal is not strongly equivalent to DSA. We have discussed that the relation between modulo-p arithmetic and modulo q-arithmetic is important for the equivalences between ElGamal-type signatures. We have focussed our attention on elliptic curves which have a good feature, in addition to smaller size, that elliptic curve signatures can choose various modulo-q arithmetics on an underlying field $\mathbb{F}_p$. By using this feature, we have shown that ECElG is strongly equivalent to ECDSA on a prime-order elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = q \geq p$. Furthermore we have shown that ECElG, ECDSA, and ECMR on an elliptic curve $E_p/\mathbb{F}_p$ with $\#E_p(\mathbb{F}_p) = p$ are all strongly equivalent each other. Therefore such an elliptic curve $E_p/\mathbb{F}_p$ can construct a message recovery signature whose security is guaranteed by a widely known signature, ECDSA and ECElG.

Acknowledgements
The author would like to thank Hiroki Shizuya and Tatsuaki Okamoto for helpful conversations. The author wishes to thank Makoto Tatebayashi for helpful advice.

参考文献

[1] D. Bleichenbacher "Generating ElGamal signatures without knowing the secret key" to appear in *Advances in Cryptology-Proceedings of EUROCRYPT'96.*

[2] W. Diffie and M. Hellman, "New directions in cryptography" *IEEE Trans. Inform. Theory,* Vol. IT-22 (1976), 644-654.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms ", *IEEE Trans. Inform. Theory*, Vol. IT-31 (1985), 469-472.

[4] C. G. Günther "An identity-based key-exchange protocol", *Advances in Cryptology-Proceedings of Eurocrypt'89*, Lecture Notes in Computer Science, **434**(1990), Springer-Verlag, 29-37.

[5] G. Harper, A. Menezes and S. Vanstone, "Public-key cryptosystems with very small key lengths", *Advances in Cryptology-Proceedings of Eurocrypt'92*, Lecture Notes in Computer Science, **658**(1993), Springer-Verlag, 163-173.

[6] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, **48**(1987), 203-209.

[7] V. S. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology-Proceedings of Crypto'85*, Lecture Notes in Computer Science, **218**(1986), Springer-Verlag, 417-426.

[8] A. Miyaji, "On ordinary elliptic curves", *Advances in Cryptology-Proceedings of ASIACRYPT'91*, Lecture Notes in Computer Science, **739**(1993), Springer-Verlag, 460-469.

[9] A. Miyaji, "Elliptic curve over F_p suitable for cryptosystems", *Advances in Cryptology-Proceedings of AUSCRYPT'92*, Lecture Notes in Computer Science, **718**(1993), Springer-Verlag, 479-491.

[10] "Proposed federal information processing standard for digital signature standard (DSS)", *Federal Register*, v. 56, n. 169, 30 Aug 1991, 42980-42982.

[11] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, 80-89, 1991.

[12] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery", *Proceedings of 1st ACM Conference on Computer and Communications Security*, 1993.

[13] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", *Advances in Cryptology-Proceedings of Eurocrypt'94* , Lecture Notes in Computer Science, **950**(1995), Springer-Verlag, 182-193.

[14] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", *Designs Codes and Cryptography*, **7**(1996), 61-81.

[15] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol.21, No.2(1978), 120-126.

[16] K. Sakurai and H. Shizuya "Relationships among the computational powers of breaking Discrete Log cryptosystems", *Advances in Cryptology-Proceedings of Eurocrypt'95*, Lecture Notes in Computer Science, **921**(1995), Springer-Verlag, 341-355.

[17] C. P. Schnorr, "Efficient identification and signatures for smart cards", *Advances in cryptology-Proceedings of Crypto'89*, Lecture Notes in Computer Science, **435**(1989), Springer-Verlag, 239-252.

[18] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag, New York, 1986.