A message recovery signature scheme equivalent to DSA over elliptic curves

Atsuko Miyaji

Multimedia Development Center
Matsushita Electric Industrial Co., LTD.
E-mail : miyaji@isl.mei.co.jp

Abstract. 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 the conception of equivalent classes([14]) between signature schemes. According to this definition, we discuss the security relation between signature schemes. The reason why the Bleichenbacher-attack([1]) works for ElGamal but not for DSA can be also explained well by the conception. We show that an elliptic curve gives the message recovery signature equivalent to DSA. Furthermore we investigate the new attack over elliptic curves and present its new trapdoor generating algorithm. We also show that the trapdoor does not exist in the particular kind of elliptic curves.

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 need to be discussed more strictly.

In this paper, we make a strict definition of the conception of equivalent classes between signature schemes. According to this definition, we discuss the

security relation between signature schemes. 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. Furthermore we investigate how Bleichenbacher-attack is applied on elliptic curve signatures. As for Bleichenbacher-attack, a trapdoor generating algorithm is an important factor: whoever knows a trapdoor for a signature can generate a user's valid signature on any message. However, a trapdoor generating algorithm over elliptic curves has not been known. We present a new trapdoor generating algorithm over elliptic curves. We also show that the elliptic curve, which constructs the message recovery signature equivalent to DSA, does not have the trapdoor.

This paper is organized as follows. Section 2 summarizes ElGamal, DSA and message recovery signature. Section 3 discusses the conception of security equivalence 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 signature equivalent to DSA. Section 5 presents a new trapdoor generating algorithm over elliptic curves.

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 $m \in \mathbb{F}_p^*$, where m is typically the hashed value of a message but in the case of using the message recovery feature m is a message with redundancy.

ElGamal
Alice 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

Alice 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 $m \in \mathbb{F}_p^*$, Alice 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 $r_2 = mr_1^{-1} \pmod{p}$ 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 was proposed([14]), which is based on an idea of transformability. However, the relation between transformability of signature schemes and the security equivalence is not known. In this section, we will discuss the relation and will make a strict definition of this conception based on transformability.

Let S1 and S2 be two signature schemes, and I be a common 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 equivalence" between signature schemes as follows.

Definition 2. 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 and explain well why Bleichenbacher-attack works for ElGamal but not for DSA.

Theorem 3. *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 $(r_1, s) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ with $q | r_1$ be an ElGamal signature on $m \in \mathbb{F}_p^*$. 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.

For practical purposes, it might be insignificant to remove the case of $r_1 = 0 \pmod q$ from ElGamal-signatures. Importantly, the conception of *strong equivalence* is effective in discussing how attacks exist. Theorem 3 says that ElGamal removed the case of $r_1 = 0 \pmod q$ is strongly equivalent to DSA and strong against Bleichenbacher-attack also.

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, the relative security of MR to DSA or ElGamal is not known at this moment. 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 $q \geq p$, 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 $E/\mathbb{F}_p$(p is a large prime) and a basepoint $G \in E(\mathbb{F}_p)$ with a large 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
Alice 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 either $x(R_1) = 0$ 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
Alice 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 either $r_1' = 0$ 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
Alice 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 either $r_2 = 0$ 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, after checking $r_2 \in \mathbb{F}_p^*$ and $s_m \in \mathbb{F}_q^*$, by 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 elliptic curves dealt in this section, 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 4. *(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 3,

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 5. *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 4. 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,

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

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

4.3 Summary of known facts on elliptic curves

As a concluding remark of Section 4, we present the next known facts on elliptic curves $E/\mathbb{F}_p$, including this paper's result.

(A) If $E/\mathbb{F}_p$ is supersingular, then the elliptic curve discrete logarithm problem(EDLP) is vulnerable to MOV-reduction([11]): EDLP is reduced to in probabilistic polynomial time to DLP.
(B) If $E/\mathbb{F}_p$ is a prime-order elliptic curve, then some equivalences of cryptosystems based on EDLP are proved: the problems of breaking the Diffie-Hellman's key exchange scheme denoted by DH_E, the ElGamal's public-key cryptosystems denoted by EG_E, and the Shamir's 3-pass key-transmission scheme([19]) denoted by $\mathrm{3PASS}_E$ are all equivalent([16]).
(C) If $E/\mathbb{F}_p$ and G with the order q satisfies $q \geq p$, ECElG is strongly equivalent to ECDSA. Especially in the case of $E/\mathbb{F}_p$ and G with the order q satisfies $q = p$, ECElG, ECDSA, and ECMR are strongly equivalent each other(Theorem 4 and 5).

As for (A), an elliptic curve $E/\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1 (p \geq 5)$, where $\#E(\mathbb{F}_p) = p + 1$ is a composite number. As for (C), from Hasse's theorem an elliptic curve with $q \geq p$ is limited to a prime-order elliptic curve, that is $\#E(\mathbb{F}_p) = q \geq p$. To sum up, in the case of a prime-order elliptic curve with $\#E(\mathbb{F}_p) \geq p$, it has been known that such an elliptic curve is not supersingular, that some problems of cryptosystems based on EDLP are equivalent, and that ECDSA and ECELG are strongly equivalent. Furthermore, in the case of en elliptic curve with $\#E(\mathbb{F}_p) = p$, it has been also known that ECDSA,

ECElG and ECMR are strongly equivalent each other. Figure 1 presents the relations among (A), (B), and (C).

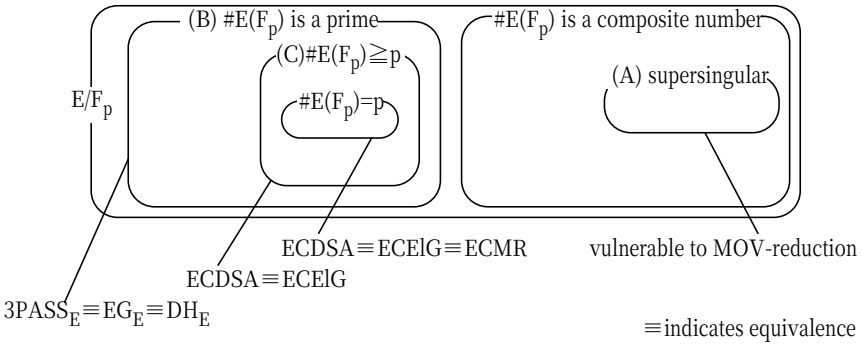

Fig. 1. Known facts on Elliptic curves over $\mathbb{F}_p (p \geq 5)$

In the case of $E/\mathbb{F}_{2^r}$, the order $\#E(\mathbb{F}_{2^r})$ of a supersingular elliptic curve is not necessarily a composite number though the facts (A), (B), and (C) hold. Therefore in the case of a prime-order elliptic curve with $\#E(\mathbb{F}_{2^r}) \geq 2^r$, it has been known that some problems of cryptosystems based on EDLP are equivalent, and that ECDSA and ECElG are strongly equivalent. We often construct elliptic curves by using Weil-conjecture: lifting E over a lower field, for example $E/\mathbb{F}_2$ or $E/\mathbb{F}_{2^2}$, to $E/\mathbb{F}_{2^r}$. However, in such a way we cannot construct a prime-order elliptic curve $E/\mathbb{F}_{2^r}$ since $\#E(\mathbb{F}_{2^r})$ is always divisible by the lifted $\#E(\mathbb{F}_2)$ or $\#E(\mathbb{F}_{2^2})$ respectively.

5 Bleichenbacher-attack over elliptic curves

We saw in Section 3 that Bleichenbacher-attack indicates the security relation between ElGamal and DSA:(i) ElGamal is not strongly equivalent to DSA and vulnerable to Bleichenbacher-attack, (ii) ElGamal removed the case of $r_1 = 0 \pmod q$ from the signatures is strongly equivalent to DSA and strong against Bleichenbacher-attack. As for elliptic curves, from Theorem 4 and 5, we saw that if $q \geq p$, then ECElG is always strongly equivalent to ECDSA, and if $q < p$, then there exists ECElG that is not strongly equivalent to ECDSA. Does Bleichenbacher-attack also indicate the security relation well? We also saw in Section 2 that a trapdoor algorithm is one of the important factors for Bleichenbacher-attack. The conception of a trapdoor might be used for a constructive purpose such as Key-Escrow system. Therefore we take interest in a technique of constructing a trapdoor algorithm over elliptic curves.

This section will investigate how Bleichenbacher-attack is applied to ECElG and also present a new trapdoor algorithm by using another feature of elliptic curves.

Bleichenbacher-attack against ECElG is as follows. Assume that a forger knows $B \in E(\mathbb{F}_p)$ such as $x(B) \in \mathbb{F}_p^*$, $x(B) = 0 \pmod q$, and $tB = G$ for a known $t \in \mathbb{F}_q^*$. For $m \in \mathbb{F}_p^*$, he sets $R_1 = B$ and $s = tm \pmod q$. Then (R_1, s) is a valid signature on m since

$$mG + x(R_1)Y_A - sR_1 = mG - tm/tG = \mathcal{O}.$$

In the case of ECDSA, such $R_1 = B$ is removed from the signatures. Therefore ECDSA is strong against the attack. In the case of ECElG, Theorem 4 and 5 say that the above B exists if and only if ECElG is not strongly equivalent to DSA. Therefore Bleichenbacher-attack also indicates the security relation between ECElG and ECDSA: ECElG is vulnerable to Bleichenbacher-attack if and only if ECElG is not strongly equivalent to ECDSA.

In the case of elliptic curves, a natural-trial trapdoor algorithm to generate $E/\mathbb{F}_p$ and G with a trapdoor B would be as follows: first set $E/\mathbb{F}_p$ and a large prime $q|\#E(\mathbb{F}_p)$, next find $B \in E(\mathbb{F}_p)$ such that the order of B is q, $x(B) \in \mathbb{F}_p^*$ and $x(B) = 0 \pmod q$, then set a basepoint $G = tB$ for $1 < t < q - 1$.

The above natural-trial trapdoor algorithm over elliptic curves seems to be more difficult than that over finite fields in Section 2 by the following reason. Usually in elliptic curves, we take p and q whose sizes are almost the same and smaller than finite fields([5]). Therefore for a fixed elliptic curve there are few points with the x-coordinate divisible by q. This is why the natural-trial algorithm seems not to be practical. Here we show a new algorithm generating the trapdoor over elliptic curves by using another feature that there exist many isomorphic elliptic curves for any elliptic curve.

Algorithm generating a trapdoor over elliptic curves
1. Choose an elliptic curve $E/\mathbb{F}_p$ and $R \in E(\mathbb{F}_p)$ with a prime order $q < p$ such that q is a quadratic residue modulo p, and that $x(R) = 1$, that is

$$E: \ y^2 = x^3 + ax + b \ (a, b \in \mathbb{F}_p), \ R = (1, r_y).$$

Here we set $u \in \mathbb{F}_p$ such that $u^2 = q \pmod p$.
2. Choose $1 < t < q$ and computes

$$tR = G = (g_x, g_y).$$

Then the order of G is q since t is relatively prime to q.
3. Define an isomorphism φ from E to E_q as follows

$$\varphi: \ E(\mathbb{F}_p) \ni (x, y) \to (qx, uqy) \in E_q(\mathbb{F}_p),$$

where $E_q/\mathbb{F}_p: \ y^2 = x^3 + aq^2x + bq^3$. Then the elliptic curve E_q, and a basepoint $\varphi(G)$ have a trapdoor $\varphi(R)$.

We show the above elliptic curve has a trapdoor. Since φ is isomorphism and

$\varphi(\mathcal{O}) = \mathcal{O}$, φ is homomorphism([18]). So E_q, $\varphi(G) = (qg_x, uqg_y)$, and $\varphi(R) = (q, uqr_y)$ satisfy that:

1. both the order of $\varphi(R)$ and $\varphi(G)$ are q;
2. $t\varphi(R) = \varphi(G)$;
3. the x-coordinate of $\varphi(R)$ is q, that is $x(\varphi(R)) = 0 \pmod q$.

This means that $\varphi(R)$ is a trapdoor of the elliptic curve E_q and the basepoint $\varphi(G)$.

Note that the existence of the trapdoor cannot be recognized easily by E_q and $\varphi(G)$. The coefficients of E_q are not necessarily divisible by q since the coefficients aq^2 and bq^3 are represented by modulo p. Furthermore if we choose a suitable t such as $qg_x, uqg_y > p$, then both x- and y-coordinate of $\varphi(G)$ are not necessarily divisible by q since they are represented by modulo p.

We discuss the running time of the above trapdoor generating algorithm. The above Algorithm requires only the next three conditions (adding to an original algorithm generating elliptic curves for ECElG, ECDSA, ECMR, etc): q is a quadratic residue modulo p, $x(R) = 1$, and $q < p$. The first and the third conditions are easy to be satisfied. The second condition also seems not to be so difficult since an algorithm generating elliptic curves with a basepoint of a small coordinate, implemented easily, is reported([9]). Therefore the above trapdoor generating algorithm is expected to be more practical than the natural-trial algorithm.

6 Conclusion

In this paper, we have investigated the next two facts:
(1) we have strictly analyzed strong equivalences between signature schemes. We have explained why Bleichenbacher-attack works for ElGamal but not for DSA, and shown that ElGamal removed the case of $r_1 = 0 \pmod q$ from the signatures is strongly equivalent to DSA and strong against Bleichenbacher-attack. 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.
(2) we have investigated how Bleichenbacher-attack is applied to ECElG. We have shown that Bleichenbacher-attack reflects the relation between ECElG and ECDSA: Bleichenbacher-attack works only for such ECElG that is not strongly equivalent to ECDSA. We have also presented a new trapdoor generating algorithm against the attack by using another feature of elliptic curves.

Acknowledgements
The author would like to thank Hiroki Shizuya for helpful conversations. The author is grateful to Daniel Bleichenbacher, Markus Michels, and Rainer A. Rueppel for sending me papers. The author wishes to thank Makoto Tatebayashi for helpful advice.

References

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.
19. A. Shamir, R. Rivest and L. Adleman, "Mental Poker", MIT/LCS, TM-125, (Feb. 1979).

This article was processed using the LaTeX macro package with LLNCS style