On the security relation among elliptic curve signature schemes

Atsuko Miyaji

1. Introduction: Recently a new ElGamal-type message recovery signature(MR) [4] was proposed. The message recovery feature has an advantage of smaller signed message length. However, the new signature has stood only for a few years, so its security is not widely accepted like ElGamal signature [1] or DSA [3]. This paper shows an elliptic curve can construct MR whose security is guaranteed by DSA and ElGamal.

2. ElGamal, DSA, and MR: Here we summarize how each signature scheme on elliptic curves is defined for a message $m \in \mathbb{F}_p^*$. In each scheme, 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, which are known to all users. The signer Alice has a secret key x_A and publishes the corresponding public key $Y_A = x_A G$. In any signature scheme, first she chooses a random number $k \in \mathbb{F}_q^*$, and computes $R_1 = kG$. In ElGamal, then she computes $s \in \mathbb{F}_q^*$ from $sk = m + x(R_1)x_A \pmod q$, 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 $(x(R_1), s) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ and $sR_1 = mG + x(R_1)Y_A$. In DSA, she computes $r_1' = x(R_1) \pmod q$ and $s \in \mathbb{F}_q^*$ from $sk = m + r_1' x_A \pmod q$. 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 $r_1' = x(\frac{m}{s}G + \frac{r_1^\prime}{s}Y_A) \pmod q$. In MR, she computes $r_2 = m^{-1}x(R_1) \pmod p$, $r_2' = r_2 \pmod q$ and $s_m \in \mathbb{F}_q^*$ from $s_m k \equiv 1 + r_2' x_A \pmod q$. 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 the recovery equation $m = x(\frac{1}{s_m}G + \frac{r_2^\prime}{s_m}Y_A)r_2^{-1} \pmod p$.

3. Security relation: Let us make a slightly strict definition of a conception [4] of equivalent classes between signature schemes.

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.

For the security equivalences, the relation between modulo-p arithmetic and modulo q-arithmetic is important. Elliptic curves have a good feature that there exist various modulo-q arithmetics on an underlying field $\mathbb{F}_p$. In fact, we can make two modulo arithmetics equal by using an elliptic curve $E_p/\mathbb{F}_p$ with p-elements [2]. The next theorem will show that $E_p/\mathbb{F}_p$ can construct MR whose security is guaranteed by both DSA and ElGamal.

Theorem 1 ElGamal, DSA, and MR on $E_p/\mathbb{F}_p$ with $\#E_p(\mathbb{F}_p) = p$ are strongly equivalent each other.

proof: We show the next two facts, (i) ElGamal is strongly equivalent to DSA, and (ii) MR is strongly equivalent to DSA. Then Theorem 1 follows from the transitive law. (i) Let (r_1', s) be a DSA signature on $m \in \mathbb{F}_p^*$. First compute $R_1 = \frac{m}{s}G + \frac{r_1^\prime}{s}Y_A$. Then (R_1, s) satisfies $(x(R_1), s) \in \mathbb{F}_p^* \times \mathbb{F}_q^*$ since $r_1' = x(R_1) \pmod q$ satisfies $r_1' \neq 0$. So (R_1, s) is an ElGamal signature on m. Conversely, let (R_1, s) be an ElGamal 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 ElGamal is strongly equivalent to DSA. (ii) Let (r_1', s) be an DSA signature on $m \in \mathbb{F}_p^*$. We set $R_1 = \frac{m}{s}G + \frac{r_1^\prime}{s}Y_A$, $r_2 = m^{-1}r_1' \pmod p$, 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 from $m = x(\frac{1}{s_m}G + \frac{r_2}{s_m}Y_A)r_2^{-1}$. So (r_2, s_m) is an MR signature. Conversely, let (r_2, s_m) be an MR signature on $m \in \mathbb{F}_p^*$. We compute $R_1 = \frac{1}{s_m}G + \frac{r_2}{s_m}Y_A$, recover $m = x(R_1)r_2^{-1}$ and 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 a DSA signature. Thus MR is strongly equivalent to DSA.

4. Conclusion: We have shown that an elliptic curve $E_p/\mathbb{F}_p$ with p-elements can construct MR whose security is guaranteed by DSA and ElGamal.

References

[1] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans.*

[2] A. Miyaji, "On ordinary elliptic curves", *ASIACRYPT'91*, Springer-Verlag, 460-469.

[3] "Proposed federal information processing standard for digital signature standard (DSS)"

[4] K. Nyberg and R. A. Rueppel, "Message recovery signature ...", *Designs Codes and Cryptography*, **7**(1996).