Signature equation suitable for message recovery schemes

Atsuko Miyaji

1. Introduction

Nyberg and Rueppel recently proposed a new ElGamal-type digital signature scheme with message recovery feature and its six variant schemes ([3]). For these schemes, six forgeries are presented ([3, 1, 2]). The author showed all six schemes are vulnerable to a kind of forgery of them ([1]). In this paper, we investigate a new signature equation suitable for message recovery scheme, which is strong against the forgery.

2. Message recovery signatures

This section summarizes Nyberg-Rueppel's message recovery signatures. In the signature schemes, the trusted authority chooses system parameters, that are a large prime p, a large integer factor q of $p-1$ and an element $g \in \mathbb{Z}_p^*$ 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 $y_A = g^{x_A}$. To sign a message $m \in \mathbb{Z}_p^*$, she chooses a random number $k \in \mathbb{Z}_q$, and computes $r_1 = g^k \pmod p$, $r_2 = mr_1^{-1} \pmod p$ and $r_2' = r_2 \pmod q$, and solves s from $ak \equiv b + cx_A \pmod q$, where (a, b, c) is a permutation of $(\pm 1, \pm r_2', \pm s)$. There are six signature-equations. Then the signature is given by (r_2, s). The message can be recovered by computing a recovery equation $m = g^{b/a} y_A^{c/a} r_2 \pmod p$ with Alice's public key y_A. An optimal one of the six schemes is as follows, which does not need inverses both in the signature generation and verification.

$$\textit{Optimal scheme:} \quad k \equiv s + r_2^{\theta} x_A \pmod q$$

3. Suitable signature equation

First we show a forgery against the optimal scheme ([3]). Assume that a signature (r_2, s) of a message m is given. Then it is possible to forge a signature $(\tilde{r_2}, \tilde{s})$ of a message $\tilde{m}$ without the knowledge of the secret key: the forger sets $\tilde{r_1} = (mr_2^{-1})g^{-1} = r_1 g^{-1} = g^{k-1} \pmod p$, $\tilde{m} = mg^{-1} \pmod p$, $\tilde{r_2} = r_2$, and $\tilde{s} = s - 1$. We see that $(\tilde{r_2}, \tilde{s})$ is a valid signature of $\tilde{m}$ since $g^{\tilde{s}} y_A^{\tilde{r_2}^{\theta}} \tilde{r_2} = g^{s-1} y_A^{r_2^{\theta}} r_2 = mg^{-1} = \tilde{m} \pmod p$. Since the forger can also generate another valid signature using $\tilde{r_1} = r_1 y_A^{-1}$ in the same way as the above, all the six schemes are vulnerable to this type of forgery ([1]). This forgery uses a feature that anyone can compute a new commitment $\tilde{r_1} = r_1/g = g^{k-1}$ or $\tilde{r_1} = r_1/y_A = g^{k-x_A}$, which he knows the discrete logarithm is equal to the value subtracted by 1 or x_A from the original discrete logarithm of r_1. Therefore he can find $(\tilde{m}, \tilde{r_2}, \tilde{s})$ satisfying the signature equation by converting signature-equation for the original r_2, s and k to that for the new $\tilde{r_2}, \tilde{s}$ and $k - x_A$ or $k - 1$.

We propose a new signature equation

$$\textit{Proposed scheme:} \quad r_2^{\theta} k \equiv (r_2^{\theta} + s + 1) + sx_A \pmod q$$

which avoids the above type of forgery. Let us apply the above forgery to the proposed scheme. In the case of $\tilde{r_1} = g^{k-1}$ the forger must find $(\tilde{r_2}, \tilde{s})$ that satisfy $(r_2', s + 1, s) = (\tilde{r_2}', \tilde{r_2}' + \tilde{s} + 1, \tilde{s})$. In the case of $\tilde{r_1} = g^{k-x_A}$ the forger must find $(\tilde{r_2}, \tilde{s})$ that satisfy $(r_2', r_2' + s + 1, s - r_2') = (\tilde{r_2}', \tilde{r_2}' + \tilde{s} + 1, \tilde{s})$. Therefore both cases succeed only in the case of $\tilde{r_2}' = r_2' = 0$ and $\tilde{s} = s$. So we can easily avoid the forgery by excepting such a trivial case: restricting $r_2' \in \mathbb{Z}_q$ to $\mathbb{Z}_q - \{0\}$. Furthermore the proposed scheme does not need inversions in the signature generation by precomputing $\frac{1}{x_A + 1}$. Only the signature verification needs one inversion. Clearly the computation amount added to the optimal scheme is negligible.

4. Conclusion

We have shown a signature equation suitable for message recovery schemes. This signature equation can avoid a type of forgery by adding a negligible computation amount to the original scheme. We have concluded that the DLP-based message recovery signature can be strengthened by changing the signature equation.

References

[1] A. Miyaji, "Weakness in message recovery signature schemes based on discrete logarithm problems 1", *IEICE Japan Tech. Rep.*, ISEC95-7, 1995.

[2] A. Miyaji, "Weakness in message recovery signature schemes based on discrete logarithm problems 2", *IEICE Japan Tech. Rep.*, ISEC95-12, 1995.

[3] 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.