Cryptanalysis of A Proxy-protected Proxy Signature Scheme Based on Elliptic Curve Cryptosystem

Shuhong Wang, Guilin Wang, Feng Bao, and Jie Wang

Abstract. Proxy signature allows original signer to delegate his/her signing capability to proxy signer such that the proxy signer can sign messages on behalf of the original signer. Based on elliptic curve, one can obtains better efficiency compared to conventional proxy signatures. In this letter, we present an original signer forgery attack on an elliptic curve based proxy signature proposed recently by Chen et al., by successfully constructing a forged proxy signature key pair.

Introduction: Proxy signature, as a variant of ordinary digital signature, allows one party (*Original signer*) to delegate his/her signing capability to another party (*Proxy signer*) such that the proxy signer can sign messages on behalf of the original signer. This interesting concept is first introduced by Mambo et al. [6], and they also give a classification (*full delegation, partial delegation, delegation by warrant*) according to the authenticated degree. From the aspect of whether the original signer knows the proxy private key, there are proxy-protected and proxy-unprotected schemes. The *proxy-protected* scheme is usually combined with a delegation by warrant, which specifies what kinds of messages are delegated. Being most in match with the practical applications and requirements, this kind of proxy signature scheme is developed most deeply and generally called as proxy signature.

Since the first scheme constructed by Mambo et al., variant kinds of proxy signature schemes have been proposed [2, 10, 5]. Most of them are based on ordinary discrete logarithm problem (DLP) and some of them are insecure (see [4, 9] for details) under the security definition in [5]. There are some modified secure proxy signatures such as that in [8], but with the drawback of losing efficiency. And consequently another solutions must be found.

Thanks to Koblitz [3] and Miller [7] who observed the intractability of discrete logarithm on elliptic curves (ECDLP) over finite fields, elliptic curve cryptography becomes an important topic in public key cryptography. Due to the low computation and storage costs of ECDLP based schemes, large numbers of researchers intend to find more efficient solutions based on ECDLP than that on DLP. Chen et al.s scheme [1] is one of such examples. However, as efficient it is, their scheme is not secure as they claim. Actually, we succeed in illustrating its insecurity through an original signer forgery by constructing a forged proxy private key pair.

Security Definitions: Precisely, a strong proxy signature [5] should provides following good security properties:

Verifiability: From the proxy signature, the verifier can be convinced of the original signer's agreement on the signed message.

Strong unforgeability: A designated proxy signer can create a valid proxy signature for the original signer. But any other parties including the original signer cannot create a valid proxy signature.

Strong identifiability: Anyone can determine the identity of the corresponding proxy signer from the proxy signature.

Strong undeniability: Once a proxy signer creates a valid proxy signature of an original signer, he/she cannot repudiate the signature creation.

Prevention of misuses: The proxy signer cannot sign messages that have not been authorized by the original signer.

Description of Chen et al.'s Scheme: Throughout this letter, we use the same notations as in Chen et al.'s scheme. Let $p > 3$ be a large odd prime, $a, b \in F_p$ such that $4a^3 + 27b^2 \neq 0$, and the equation of elliptic curve E over F_p defined by a, b is $y^2 = x^3 + ax + b \pmod p$. Let $B = (x_B, y_B)$ be a finite point of order t in $E(F_p)$ for some large prime number t. The ECDLP in $\langle B \rangle \subseteq E(F_p)$ is assumed to be difficult. We denote by (d_o, Q_o) and (d_p, Q_p) the *certified key pairs* of *original* signer and *proxy* signer respectively, where $Q_o = d_o \times B$ and $Q_p = d_p \times B$ and the sign " $\times$ " indicates the multiplication in $E(F_p)$. By the difficult of ECDLP, it is infeasible to find the integer d_o (or d_p), given Q_o (or Q_p) and B. In addition, we use x and y subscripted by a point (say, x_{Q_o}, x_{Q_p} etc.) to represent the corresponding x-coordinate and y-coordinate of this point. In the end, let $h(\cdot)$ be a collision resistant hash function and M_ω the *warrant* which specifies the delegation relationship between original signer and proxy signer as well the delegation period.

Phase 1. Proxy Delegation: In this phase, the original signer O needs to generate a triplet (M_ω, R_o, s_o) and sends it to the proxy signer P.

First, O selects $k_o \in_R Z_t^*$ not the same as d_o, and computes $R_o = k_o \times B$ with $x_{R_o} \neq 0$ and $s_o = d_o h - k_o \pmod t$, (where h is computed as $h = h(M_\omega, x_{Q_o}, x_{Q_p}, x_{R_o})$. And from now on, we simply use h (or $h^{'}$) instead of the whole expression in the same obvious way). Next, he sends (M_ω, R_o, s_o) to P. In fact, (R_o, s_o) can be regarded as the signature of M_ω using Schnorr's signature scheme.

P accepts (M_ω, R_o, s_o) as a valid delegation triplet if $x_{R_o^{'}} = x_{R_o} \pmod t$, where $R_o^{'}$ is computed as $R_o^{'} = h \times Q_o - s_o \times B$. The proxy delegation scenarios illustrated as Figure 1.

Original signer		*Proxy signer*
$k_o \in_R Z_t^* \backslash \{d_o\}$		
$R_o = k_o \times B$	$\xrightarrow{(M_\omega, R_o, s_o)}$	$R_o^{'} = h \times Q_o - s_o \times B$
$s_o = d_o h - k_o \pmod t$		checks $x_{R_o}^{'} \stackrel{?}{=} x_{R_o}$

Fig. 1. Proxy Delegation Phase

Note: In fact, (R_o, s_o) can be regarded as the signature of M_ω using Schnorr's signature scheme.

Phase 2. Proxy Key Pair Generation: If the proxy signer confirms the validity of the delegation parameter triplet (M_ω, R_o, s_o), then he computes the proxy secret key as $\overline{d}_p = d_p + s_o \pmod t$, and on receiving the proxy signature, the verifier V can recovers the corresponding proxy public key as $\overline{Q}_p = Q_p + h \times Q_o - R_o (= \overline{d}_p \times B)$

Note that the proxy signing and verification are the same as an ordinary ECDLP-based signature scheme. Note also that the result of the proxy signature to message m is a quaternity $(m, \sigma, R_o, M_\omega)$ with $\sigma = Sign_{\overline{d}_p}(m)$, where $Sign_{key}(\cdot)$ is the ECDLP-based signature algorithm actually used, and if the corresponding verification algorithm is denoted by $verify(\cdot)$, then the verification is to check whether $verify(m, \sigma, \overline{Q}_p) = true$. This scenario is depicted simply as Figure 2.

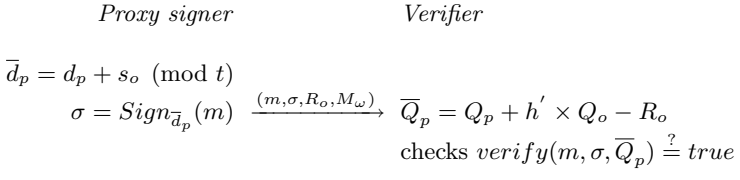

Fig. 2. Proxy Signature and Verification

Our Attack: In this subsection, we show that Chen et al.'s proxy-protected proxy signature is insecure against the original signer's forgery. Suppose that a dishonest original signer O wants to forge valid proxy signatures which looks as if they are generated by a proxy signer P on behalf of himself. He can do as follows:

1). Chooses a random $k_o \in_R Z_t^* \backslash \{d_o\}$ and computes $R_o = k_o \times B$.
2). Defines $R_o^{'} = Q_p + R_o$ and computes $h^{'} = h(M_\omega^{'}, x_{Q_o}, x_{Q_p}, x_{R_o^{'}})$. Note that the *warrant* $M_\omega^{'}$ may be different from M_ω.
3). Computes the proxy-signature signing key as $\overline{d}_p{}^{'} = h^{'} d_o - k_o \pmod t$.
4). Uses $\overline{d}_p{}^{'}$ to generate the proxy signature $\sigma^{'} = sign_{\overline{d}_p{}^{'}}(m^{'})$ of any message $m^{'}$. Then $(m^{'}, \sigma^{'}, R_o^{'}, M_w^{'})$ is a valid proxy signature. This is because:

$$\begin{aligned} Q_p^{'} &= Q_p + h(M_\omega^{'}, x_{Q_o}, x_{Q_p}, x_{R_o^{'}}) \times Q_o - R_o^{'} \\ &= Q_p + h^{'} \times Q_o - (Q_p + R_o) \\ &= (h^{'} * d_o) \times B - k_o \times B \\ &= (h^{'} d_o - k_o \bmod t) \times B \\ &= \overline{d}_p{}^{'} \times B \end{aligned}$$

Hence, the forged $(\overline{d}_p{}^{'}, Q_p^{'})$ with $R_o^{'}$ and $M_\omega^{'}$ is a valid proxy key pair and $(m^{'}, \sigma^{'}, R_o^{'}, M_w^{'})$ is a valid proxy signature.

Conclusion: In this letter, we mount an original signer forgery attack attack on Chen et al.'s scheme [1] to show its insecurity. This security flaw results in lose of the strong unforgeability and strong undeniability that a strong proxy signature scheme should provide to protect the proxy signer. Further researches are needed on constructing more secure and efficient proxy-protected proxy signature using elliptic curves.

References

1. Chen, T. S., Liu, T. P, and Chung, Y. F.: 'A Proxy-Protected Proxy Signature Scheme Based on Elliptic Curve Cryptosystem', *Proc. of IEEE TENCOM'02*, 2002, pp. 184-187
2. Kim, S., Park, S., and Won, D.: 'Proxy signatures, revisited', *Information and Communications Security - ICICS'97*, LNCS 1334, 1997, pp. 223-232
3. Koblitz, N.: 'Elliptic Curve Cryptosystems', *Mathematics of Computation*, Vol.48, 1987, pp. 203-209
4. Lee, J. Y., Cheon, J. H., and Kim, S.: 'An analysis of proxy signatures: Is a secure channel necessary?' *Topics in Cryptology - CT-RSA 2003*, LNCS 2612, 2003, pp. 68-79
5. Lee, B., Kim, H., and Kim, K.: 'Secure Mobile Agent Using Strong Non-designated Proxy Signature', *Proceedings of ACISP'01*, LNCS 2119, 2001, pp. 474-486
6. Mambo, M., Usuda, K., and Okamoto, E.: 'Proxy Signature: Delegation of the Power to Sign Messages', *IEICE Trans. Fundamentals*, Vol. E79-A, No.9, 1996, pp. 1338-1353
7. Miller, V. S.: 'Uses of Elliptic Curves in Cryptography', *Adavances in Cryptology - Crypo'85*, LNCS 218, 1985, pp. 417-426
8. Sun, H. M.: 'Improved Proxy Signature Schemes', *Proceedings of the International Computer Symposium - ICS'00*, 2000.
9. Wang, G., Bao, F., Zhou, J., and Deng, R.: 'Security Analysis of Some Proxy Signatures', *Information Security and Cryptology - ICISC'03*, 2004 (to appear). Preliminary version is available at http://eprint.iacr.org/2003/196.
10. Yi, L., Bai, G., and Xiao, G.: 'Proxy Multi-signature Scheme: A New Type of Proxy Signature scheme' *Electronics Letters*, Vol. 36(6), 2000, pp. 527-528

Authors' affiliations:

Shuhong Wang, Jie Wang (School of Mathematical Science, Peking University, Beijing, China 100871. email: {wshong, wangj}@math.pku.edu.cn)

Guilin Wang, Feng Bao (Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613. email: {glwang, baofeng}@i2r.a-star.edu.sg)

♣ This work was done during the first author being visiting Institute for Infocomm Research, Singapore.