Cryptoanalysis of ID-based proxy re-signature scheme with pairing-free

Jianhong Zhang
School of Electronic and Information Eng.
North China University of Technology
No5.Jinyuanzhuang, Beijing
China
zjhncut@163.com

Yuehai Wang
School of Electronic and Information Eng.
North China University of Technology
No5.Jinyuanzhuang, Beijing
China
waters.b@163.com

Abstract: .As a significant cryptographical primitive, proxy re-signature(PRS) technique is broadly applied to distributed computation, copyright transfer and hidden path transfer because it permits that a proxy translates an entity's signature into the other entity's signature on the identical data. Recently, to discard time-consuming pairing operator and intricate certificate-maintenance, Wang et al. proposed two efficient pairing-free ID-based PRS schemes, and declared that their schemes were provably secure in the ROM. Very unluckily, in this investigation, we point out that Wang et al.'s schemes suffer from attacks of universal forgery by analysing their security, i.e., anyone can fabricate a signature on arbitrary file. After the relevant attacks are shown, the reasons which result in such attacks is analyzed. Finally, we discuss the corresponding improved method.

Key–Words: ID-based PRS, integer factorization problem, universal forgeability, security attack

1 Introduction

As a crucial authentication technique, digital signature is broadly applied in some practical scenarios since it can identify the source of data, insure data intact and afford data origin's non-repudiation, such as E-passport,E-health, and E-currency. With the popularization of electronic and communication technology, a good deal of signature schemes with various functions have been put forth to satisfy practical requirement.

In most cases, the signer wishes that its message's signature is publicly validated in order that any one is capable knowing the origin of this message. However,in some specific scenarios, a user Alice wishes to transform the ownership of its digital product to another user Bob, and to convince all verifiers that the ownership of this digital product is from the user Bob. It is a challengeable problem since it contradicts non-reputation of digital signature, and the transformed signature also needs to be publicly verified without revealing the origin of this signature. Fortunately, proxy pre-signature can deal with the problem above. Proxy re-signature (PR S) notion was firstly defined by M.Blaze *et al.* in [4] . In a PRS scheme, a semi-trusted party (the proxy) is capable of translating a signature from Alice (the delegatee) into a signature from Bob(the delegator) on the identical data m by a re-signing key. Nevertheless, the proxy is unable to create a valid message-signature in name of the delegatee or the delegator independently. In 2005, G.Ateniese and S.Hohenberger provided a formal definition of PRS's security model and proposed two concrete instances: a single-use PRS and a multi-use PRS in [5]. After this seminal work[5], various PRS schemes [6, 7, 8, 9, 10] with special properties have been proposed successively to satisfy practical requirement. Whereas most PRS schemes are built on traditional public-key-infrastructure (PKI). In PKI, when the signer's public key is employed, its validity needs to be authenticated by a certificate issued by a certifier authority (CA). Whereas, maintenance of certificate might bring a heavy burden to the signer.

To remove intricate certificate maintenance, Shamir pioneered the idea of identity-based PKC (ID-PKC) in [11]. In the ID-based PKC, the user's unique identification information such as cell-phone number, identity-card number, e-mail address, etc., acts as its public key. ID-PKC abandons the inevitability for public key certificates, so that it makes that intricate certificate maintenance is avoided. ID-based PRS concept(for short, ID-PRS) was firstly put forth by Shao et al. in [9]. Their scheme is a secure multi-use ID-PRS scheme in the standard model. The only drawback in their scheme is relatively larger in terms of public parameters and computation costs. Subsequently, Hu et al. also proposed a novel ID-PRS scheme based on a harder mathematics problem in [7]. In 2015, Tian presented an efficient ID-PRS scheme

[19] based on lattice cryptography in the ROM, but the practicability of their scheme is very weak since its signature length and computation costs are very large.

Recently, to remove time-consuming pairing operation, Wang et al. suggested two efficient ID-based PRS schemes without pairing in [2]. Although they claimed that their schemes were secure against existential unforgeable attack in the ROM[15]. Unfortunately, by analyzing the security of their schemes, we manifest that their schemes exist universal attacks of forgery, i.e., any one can fabricate a signature on a message at will. After the detail attacks is launched , we analyze the relevant reasons to induce such attacks.

2 Preliminaries

In this part, we review security assumptions and interrelated mathematics knowledge which are the basic knowledge required throughout the paper.

2.1 Notions

For convenience, Table I shows quiet a few mathematic symbols and notions which are used in the remaining context.

2.2 Mathematic Hardness Problem

Large integer factorization problem. Let N denote a composite-integer which is written as $N = p \cdot q$,where p, q are two large primes, its target is to seek its decompositions p and q. This is known to all that it is a very hard problem to seek a PPT algorithm Alg to factorize the large-integer N.

Large integer factorization assumption. Let l be a security parameter, $N = pq$ is a composite-integer, where p and q are two l-bits large primes, we named that the (t_R, ε_R)-large composite-integer factorization assumption holds if no t_T-probabilistic polynomial-time (PPT) adversary is capable of decomposing the composite-integer N with a non-negligible probability ε_R.

Lemma1. Let $N = p_0 \cdot q_0$ be a product of primes p_0 and q_0, for $\alpha \in_R Q_N$ and $\alpha \neq 1$, we have $\alpha^{2\rho} \equiv \alpha \mod N$ where $\rho = \frac{N-p_0-q_0+5}{8}$.

Proof. Because Q_N is a cyclic-group with the order $\phi(N)/4 = (p_0-1)(q_0-1)/4$, for $\alpha \in Q_N$, we have $\alpha^{(p_0-1)(q_0-1)/4} \equiv 1 \mod N$. Then, we have

$$\begin{aligned}
\alpha^{(p_0-1)(q_0-1)/4} &\equiv 1 \mod N \\
&\Updownarrow \\
\alpha^{\frac{(p_0-1)(q_0-1)}{4}+1} &\equiv \alpha \mod N \\
&\Updownarrow \\
\alpha^{\frac{(N-p_0-q_0+5)}{4}} &\equiv \alpha \mod N \\
&\Updownarrow \\
\alpha^{\rho\cdot 2} &\equiv \alpha \mod N
\end{aligned}$$

where $\rho = \frac{(N-p_0-q_0+5)}{8}$. □

Note that, for a quadratic residue α, it should have four diverse square roots, namely $\pm r_1$ and $\pm r_2$. Only when $r_1 \neq \pm r_2 \mod N$ holds, N can be factorized by utilizing $GCD(r_1 - r_2, N)$ or $GCD(r_1 + r_2, N)$. Therefore, it means that given two diverse roots, the probability of factoring N is $\frac{1}{2}$.

The Extended Euclidean Algorithm: For any $a, b \in Z_N$, where $a, b \neq 0$, there exists an efficient algorithm which can output two integers $x \in Z_N$ and $y \in Z_N$ such that

$$ax + by = GCD(a, b)$$

3 Review of Wang et al.'s ID-PRS Scheme

Recently, to construct PRS scheme which appropriates for resource-limited devices, Wang *et al.* presented two free-pairing ID-PRS proposals which avoid the time-consuming pairing computation. To clearly analyze their security, a brief review of Wang *et al.*'s ID-PRS schemes is given. Please refer to [2] for more details if the readers are interested in Wang et al.'s scheme.

3.1 Interactive version of Wang *et al.*'s ID-PRS Scheme

- Setup (1^ι): Let ι denote a security parameter. On inputting ι, it outputs two safe large-primes p and q which are $\iota/2$ bits. And then compute $N = p \cdot q$ and $\rho = (N - p - q + 5)/8$. Subsequently, pick two hash functions $H(\cdot) : \{0,1\}^* \to Q_N$ and $h(\cdot) : \{0,1\}^* \to \{0,1\}^l$, where Q_N denotes a subgroup of quadratic residues in Z_N^* and l is the output bit-length of hash function. Finally, public parameters $mpk = (N, H(\cdot), h(\cdot))$ are published and master private key $msk = (p, q, \rho)$ is securely stored.

Table 1: Notions

Notions	Description
$a \in_R N$	a is chosen randomly in N
GCD(x,y)	The greatest common divisor (gcd) of x and y
Z_N	the set $\{1, \cdots, N\}$
p, q	two large primes
$\perp$	'invalid' mark
ϕ	the Euler's ϕ function
Q_N	the subgroup in Z_N^* with order $\phi(n)/4 = (p_0 - 1)(q_0 - 1)/4$
PPT	probabilistic polynomial time
EUF-CMA	existential unforgeability against adaptive chosen-message attack
EUF-CID-MA	existential unforgeability against adaptive identity-and-message attack
ECC	elliptic curve cryptography
ROM	random oracle model

- Extract(ID, msk, mpk): Given a user's identity information ID, on inputting ID, public parameters mpk and master private key msk, the algorithm calculates the user's private key as below:

$$sk_{ID} = H(ID)^{\rho} \mod N$$

- Re-signing key(sk_A, sk_B) On inputting private keys sk_A and sk_B of Alice and Bob, the algorithm outputs the relevant re-signing key $rk_{A\to B} = sk_B/sk_A$.

- Sign(m, sk): Given the signed message m, a user with identity ID makes use of its private key sk_{ID} to calculate the signature as below: it picks $r \in Z_N^*$ at random to calculate $R = r^2 \mod N$, then it calculates $\delta = r \cdot sk_{ID}^{h(m)} \mod N$. Finally, the obtained signature is $sig = (\delta, R)$ on message m .

- Re-signature$(m, sig_A, ID_A, rk_{A\to B})$: Given the delegatee Alice's signature $sig_A = ((\delta_A, R))$ on message m, Alice's identity ID_A and the re-signing key $rk_{A\to B}$, if the equation $\delta_A^2 = H(ID_A)^{h(m)} \cdot R$ holds, then the re-signature is

$$sig_B = (\delta_A \cdot rk_{A\to B}^{h(m)}, R)$$

- Verify(m, sig_i) For a signature $sig_i = (\delta, R, ID_i)$ where $i \in \{A, B\}$, the verifier checks whether

$$\delta^2 \overset{?}{=} R \cdot H(ID_i)^{h(m)}$$

  If it is true, then it signifies that sig_i is valid for $i \in \{A, B\}$, otherwise, $'\perp'$ is output.

3.2 Non-interactive verision of Wang et al.'s ID-PRS Scheme

- Setup (1^{ι}): In this algorithm, the generation process of all parameters is the same as that of the above interactive version.

- Extract(ID, msk, mpk): In this algorithm, the generation process of the user's private key is the same as that of the above interactive version.

- Re-signing key(sk_A, sk_B) For this algorithm, it inputs Alice's identity ID_A and Bob's secret key sk_B, whereafter outputs the re-signing key $rk_{A\to B} = sk_B/H(ID_A)$.

- Sign(m, sk): For this algorithm, it is the same as the interactive version.

- Re-signature$(m, sig_A, ID_A, rk_{A\to B})$: Given Alice's signature $sig_A = ((\delta_A, R))$ on message m, Alice's identity ID_A and the re-signing key $rk_{A\to B}$, if the equation $\delta_A^2 = H(ID_A)^{h(m)} \cdot R$ holds, then it randomly selects $r' \in Z_N^*$ to compute $R' = (r'R)^2 \mod N$. At last, it outputs $sig_B = (r' \cdot \delta_A^2 \cdot rk_{A\to B}^{h(m)}, R')$ as re-signature.

- Verify(m, sig_i) : For this algorithm, it is the same as the interactive version above.

4 Security Analysis

Although Wang *et al.* declared that their two schemes were proven secure against EUF-CMA, and provided the security proof. Unfortunately, we will show that Wang *et al.*'s two ID-PRS schemes are insecure. The detailed attacks are listed as below:

4.1 Attack on Wang et al.'s Interactive ID-PRS scheme

In the subsection, by analyzing Wang et al.'s interactive ID-PRS scheme, the scheme is indicated to be universally forgeable, this is to say, any one can fabricate the delegatee's signature or the delegator's signature (re-signature). The corresponding attack is executed as below:

1. Let Adv be an attacker and m^* be an arbitrary message. ID_B denotes the delegator Bob's identity.
2. Because $N = p \cdot q$ and p, q are two large primes, then $Gcd(H(ID_B), N) = 1$ with probability which is almost 1, otherwise, N can be factorized. The attacker Adv can obtain $H(ID_B)^{-1}$ with by using Extended Euclidean algorithm, namely, $H(ID_B) * x + N * y = Gcd(N, H(ID)) = 1$.
3. Then the attacker randomly $\hat{r} \in Z_N$ to calculate
$$R^* = \hat{r}^2 \cdot (H(ID_B)^{-1})^{h(m^*)} \mod N$$
and let $\delta^* = \hat{r}$.
4. At last, the fabricated re-signature on message m^* is $sig^* = (\delta^*, R^*)$.

Next, we demonstrate that the fabricated re-signature sig^* is valid. Because

$$\begin{aligned} R^* \cdot H(ID_B)^{h(m^*)} &= \hat{r}^2 \cdot (H(ID_B)^{-1})^{h(m^*)} \\ &\quad \cdot H(ID_B)^{h(m^*)} \\ &= \hat{r}^2 \\ &= (\delta^*)^2 \end{aligned}$$

Obviously, the fabricated signature satisfies the verification equation. It illustrates that the aforementioned attack is successful.

The reason to suffer the aforesaid attack is that R is free in the signature $sig = (\delta, R)$ and it is not constrained. It makes that any one can select a right R to cancel $H(ID_B)^{h(m)}$. To solve this attack, the core is to limit the form of R. Hence we modify $\delta = r \cdot sk^{h(m)}$ into $\delta = r \cdot sk^{h(m,R)}$, and the verification equation is modified $\delta^2 = R \cdot H(ID)^{h(m)}$ into $\delta^2 = R \cdot H(ID)^{h(m,R)}$.

4.2 Attack on Non-interactive version of Wang et al.'s IDPRS scheme

In [2], Wang et al. proposed a non-interactive ID-PRS scheme again. And they also declare that the non-interactive vision is secure in the ROM. In fact, by analyzing their non-interactive scheme, we also find that the scheme is also insecure since the verification equation is the same as that of interactive version. Thus, Wang et al.'s non-interactive ID-PRS scheme suffers from the same forgery attack as Wang et.al's interactive version.

In addition to the above forgery attack, Wang et al.'s non-interactive scheme also suffers from the delegator's (Bob's) private key leakage. For a proxy, it is a curious and semi-trusted entity. For a re-signing key, it wants to know the delegator's private key. In the following attack, we will show that a semi-trusted proxy can retrieve the delegator's private key. The detail attack is given as follows:

- Let $rk_{A\to B} = \frac{sk_B}{H(ID_A)}$ be a re-signing key.
- Then the proxy calculates $sk_B = rk_{A\to B} \cdot H(ID_A) \mod N$, thus, it can easily obtain the delegator's private key sk_B.

It indicates that the delegator's private key is revealed. Because

$$\begin{aligned} & rk_{A\to B} \cdot H(ID_A) \mod N \\ = & \frac{sk_B}{H(ID_A)} \cdot H(ID_A) \mod N \\ = & sk_B \mod N \end{aligned}$$

The reason to suffer this attack is that $H(ID_A)^{-1}$ can be obtained by Extended Euclidean algorithm.

From the above analysis, we can know that Wang et al.'s two ID-based PRS schemes are insecure. Their scheme not only exist universal forgery, but also suffers from the leakage problem of the delegator's private key .

5 Discussion on the Improved Method

To overcome aforementioned security flaw in Wang et al.'s two IDPRS schemes, we can consider the improved method. The detailed algorithms are described as below:

- Setup (1^ι): Let ι denote a security parameter, On inputting ι, the algorithm outputs two safe-large primes p and q which are $\iota/2$ bit-length. And compute $N = p \cdot q$ and $\rho = (N - p - q + 5)/8$. Next it picks two hash functions $H() : \{0,1\}^* \to Q_N$ and $h() : \{0,1\}^* \to \{0,1\}^l$, where Q_N denotes a subgroup of quadratic residues in Z_N^* and l is the output length of hash function, in general $l = 160$. At last, public parameters $mpk = (N, H(\cdot), h(\cdot))$ are published and master private key $msk = (p, q, d)$ is securely stored.

- Extract(ID, msk, mpk): Given a user's identity information ID, on inputting ID, master private key msk and public parameters mpk. The algorithm calculates the user's private key as below:

$$sk_{ID} = H(ID)^{\rho} \mod N$$

- Re-signing key(ID_A, ID_B, sk_B): On inputting the delegatee Alice's identity ID_A and the delegator Bob's private key sk_B, and then the algorithm picks $\gamma \in Z_N$ at random to produce the re-signing key

$$rk_{A\to B} = (rk^1_{A\to B}, rk^2_{A\to B}) = (\tau, \frac{\gamma \cdot sk_B^{h(\tau)}}{H(ID_A)})$$

where $\tau = \gamma^2$. Finally, $rk_{A\to B}$ is returned .

- Sign$_A(m, sk_A)$: It is an algorithm to produce the delegatee's signature. For a message m, a delegatee with identity ID_A makes use of its private key sk_A to execute as follows: it randomly picks $r \in Z_N^*$ to calculate $R_A = r^2 \mod N$, then it calculates $\delta_A = r \cdot sk_A^{h(m,R_A^2)} \mod N$. Finally, the signature on m is $sig_A = (\delta_A, R_A)$.

- Sign$_B(m, sk_B)$: It is an algorithm to produce the delegator's signature. For a message m, a delegator with identity ID_B calculates the following procedure by utilizing its private key sk_B:

  it randomly picks $r_2, r_3 \in Z_N^*$ to calculate $s_2 = r_2^2 \mod N$ and $s_3 = r_3^2 \mod N$, then it calculates $s_1 = r_2 \cdot (r_3 \cdot sk_B^{h(s_3)})^{h(m,s_2)} \mod N$. Finally, the produced signature on m is $sig_B = (s_1, s_2, s_3)$.

- Re-signature$(m, sig_A, ID_A, rk_{A\to B})$: Given the delegatee Alice's signature $sig_A = (\delta_A, R_A)$ of message m and Alice's identity ID_A, the proxy utilizes its re-signing key $rk_{A\to B}$ to calculate as below:

  1. Firstly, it verifies the validity of $sig_A = (\delta_A, R_A)$.
  2. If the equation $\delta_A^2 = R_A \cdot H(ID_A)^{h(m,R_A^2)}$ holds, then the re-signature is

$$\begin{aligned} sig_B &= (s_1, s_2, s_3) \\ &= (\delta_A^2 \cdot (rk^2_{A\to B})^{h(m,R_A)}, R_A^2, r^1_{A\to B}) \\ &= (R_A \cdot (\gamma \cdot sk_B^{h(\tau)})^{h(m,R_A)}, R_A^2, r^1_{A\to B}) \end{aligned}$$

- Verify(m, sig_i): Given a signature sig_i where $i \in \{A, B\}$, its verification is divided into two cases:

  1. if signature $sig_i = sig_A$, then the verifier computes

$$\delta^2 = R_A \cdot H(ID_A)^{h(m,R_A^2)}$$

  If it holds, then it means that sig_i is a valid signature, otherwise, output invalid.

  2. if signature $sig_i = sig_B$, then the verifier computes

$$s_1^2 = s_2 \cdot (s_3 \cdot H(ID_B)^{h(s_3)})^{h(m,s_2)}$$

  If it holds, then it means that sig_i is a valid signature, otherwise, output invalid.

Correctness: For the improved method, it is easily demonstrated to be correct since

$$\begin{aligned} & s_2 \cdot (s_3 \cdot H(ID_B)^{h(s_3)})^{h(m,s_2)} \\ = & R_A^2 \cdot (\gamma^2 \cdot H(ID_B)^{h(\gamma^2)})^{h(m,R_A^2)} \\ = & (R_A \cdot (\gamma \cdot sk_B^{h(\gamma^2)})^{h(m,R_A^2)})^2 \\ = & (s_1)^2 \end{aligned}$$

It means that a genuinely signed proxy re-signature must satisfy the above verification equations. Thus, our improved method is valid.

6 Conclusion

Pairing operation is an expensive operator in ECC. To avoid pairing operator in protocol, Wang *et al.* brought forward two efficient ID-PRS schemes without pairing based integer factorization problem, and declared that their schemes were EUF-CID-MA in the ROM. In this investigation, we analyze the security of their schemes and find that their two schemes are insecure. They suffer from universal forgeability attack. After the detailed attacks are executed, we also discuss an improve method.

References:

[1] Z.C Chai, Z.F. Cao, and X.L. Dong,(2007) Identity-based signature scheme based on quadratic residues.*Science in China Series F: Information Sciences,* vol.50(3): pp. 373–380.

[2] Zhiwei Wang, Aidong Xia, Mingjun He, ID-based proxy re-signature without pairing, Telecommunication Systems (2018) 69:217-222, https://doi.org/10.1007/s11235-018-0458-9

[3] Mihir Bellare, Adriana Palacio,(2002)GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks,Advances in Cryptology-CRYPTO02,LNCS 2442:162-177.

[4] Blaze M, Bleumer G, StraussM (1998) Divertible protocols and atomic proxy cryptography. In: Proc. Advances in Cryptology-Eurocrypt'98 LNCS 1921:127-144.

[5] Ateniese, G.,Hohenberger, S. (2005) Proxy re-signatures: New definitions, algorithms, and applications. In ACM CCS 2005,pp310-319.

[6] Hong X, Gao J, Pan J, Zhang B (2017) Universally composable secure proxy re-signature scheme with effective calculation. Cluster Computing vol.78(20):1-10.

[7] Hu X, Liu Y, Xu H, Wang J, Zhang X (2015) Analysis and improvement of certificateless signature and proxy re-signature schemes. In: Proc. Advanced Information Technology, Electronic and Automation Control Conference. pp. 166-170.

[8] Yang X, Gao G, Li Y, Li Y, Wang C (2015) On-line/off-line threshold proxy re-signature scheme through the simulation approach. Applied Mathematics and Information Sciences vol.9(6):3251-3261.

[9] Shao J, Cao Z, Wang L, Liang X (2007) Proxy re-signature schemes without random oracles,INDOCRYPT 2007,LNCS4859:197-209.

[10] Feng J, Lan C, Jia B (2014) ID-based proxy re-signature scheme with strong unforgeability. Journal of Computer Applications vol.34(11):3291-3294.

[11] Adi Shamir (1984) Identity-based cryptosystems and signature schemes.CRYPTO 1984, LNCS 196:47-53.

[12] Yvonne Hitchcock, Colin Boyd Juan Manuel, Gonzlez Nieto,(2004)Tripartite key exchange in the canetti-krawczyk proof model, INDOCRYPT'04, LNCS3348:17-32

[13] Yang X, Chen C, Ma T, Wang J, Wang C (2018) Revocable identity-based proxy re-signature against signing key exposure, PLoS ONE 13(3): e0194783. https://doi.org/10.1371/journal.pone.0194783

[14] Farash MS, Chaudhry SA, Heydari M, Sadough S, Mohammad S, Kumari S, Khan MK (2017) A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. International Journal of Communication Systems. https://doi.org/10.1002/dac.3019

[15] Ran Canetti, Oded Goldreichy, Shai Haleviz,(2004) The Random Oracle Methodology, Revisited, Journal of the ACM , Vol.51(4):557-594

[16] Shoup, V. (2005). A computational introduction to number theory and algebra . Cambridge: Cambridge University Press.

[17] Jia X, He D, Zeadally S, Li L (2017) Efficient revocable ID-based signature with cloud revocation server. IEEE Access 5: 2945-2954. https://doi.org/10.1109/ACCESS.2017.2676021

[18] Lee K, Lee DH, Park JH (2017) Efficient revocable ID-based encryption via subset difference methods, Designs, Codes and Cryptography vol.85(1): 39-76.

[19] Tian M,(2015) Identity-based proxy re-signatures from lattices. Information Processing Letters 115(4): 462-467.