A Novel Approach for RSA-based Certificateless Signature Scheme

Nishant Doshi

Abstract—In the conventional signature scheme, the sender will sign the message and send it to the receiver, who is verify based on the certificate of the sender (provided by trusted third party prior to communication). However, this lead to a certificate management problem as third party need to maintain all certificates and if there are many third parties (hierarchical). The solution to this problem lead to a certificateless signature scheme in which receiver only requires ID (unique identity) of the sender. The approaches in literatures are based on the bilinear map. However, the time for pairing is more as that of the exponent operation of the RSA (Public Key Cryptography) scheme. Recently, Zhang et al, proposed the RSA-based certificateless scheme. We show that this scheme is insecure and proposed the scheme that overcomes the attack on Zhang et al's scheme.

Index Terms—Certificateless Signature,Cryptanalysis, RSA, Discrete Log Problem.

1 Introduction

In a conventional Public Key Cryptosystem (PKC), the secret key of the user is an arbitrary string. To bind a relation between the arbitrary string and identity of user, the central authority (CA aka. Key Generation Center) issues the digital certificate. Therefore, it requires a huge effort for CA to generate and manage the certificates [1]. Thus in [2], the authors firstly proposes the concept of Identity Based Cryptography (IBC), in which the ID (unique identity like SSN, email id, name etc.)of user become the public key and based on that CA will generate the private key and give it to the user.

In IBC, CA can generate the secret key for any ID that lead to a key-escrow problem. Therefore in [3], the authors firstly propose the concept of certificateless public key cryptography (CL-PKC) to remove the key-escrow problem. In certificateless cryptography, the CA generates the partial private key while the remaining is generated by user. Since the CL-PKC is introduced, many certificateless signature and encryption schemes were proposed.

In [3], the authors firstly proposes the concrete construction of the CL-PKC. Thereafter many schemes proposed in literature to improve upon security, efficient etc. [4-13]. However, all of these schemes use the assumptions related to bilinear pairing.

The implementation of the pairing is much harder as that of exponent operations in RSA group. Even many companies use the RSA for decades. Therefore in [14] the authors propose the concept of RSA based CL-PKC that was enhanced by [15-16] subsequently.

1.1 Our Contribution

In [16], the authors claimed that their protocol is secure against adversary attack-I and attack-II. But in this paper we have shown that their scheme is vulnerable to Attack-I and thereafter we have proposed the new scheme that is secure against both attacks.

1.2 Organization of the paper

In section 2, we have given the definitions for complexity hardness as well as the construction for the CL-PKC scheme. In section 3, we have reviewed the scheme of [16] whereas in section 4 we have given the cryptanalysis of it. In section 5, we have given the proposed scheme. Conclusion and future work are given in section 6. References are at the end.

2 Preliminaries

2.1 Complexity assumptions [16]

Definition 1: (The RSA problem). Let $N = pq$ like RSA-based modulus, where p and q are large prime numbers. Z_N be the set of positive elements of order N. Let G be a cyclic group of order N. Given (n, e) and $z \in G$, the RSA problem is to find $u \in Z_N$ such that $z = u^e$.
Definition 2: (Discrete Logarithm Problem). Given $g \in G,\ y \in_R Z_N$ the discrete logarithm problem is to find x such that $y = g^x mod\ N$.

2.2 Certificateless (CL) Signature scheme

The certificateless signature scheme consists of the following seven polynomial time algorithms.
Setup: It is run Central Authority (CA), to generate the master public key (MPK) and master secret key (MSK) for the system based on the security parameter.
Partial-Private-Key-Extraction (MPK,MSK,ID): Based on the MPK, MSk and $ID \in \{0,1\}^*$, CA generates the partial private key d_{ID} and give it to user over secure channel.
Set-Secret-Value (MPK,ID): This is run by user. Based on MPK and ID, this algorithm outputs secret parameters X_{ID}, G_{ID}.

Set-Private-Key $(X_{ID}, G_{ID}, MPK, d_{ID})$: This is run by user. Based on the $X_{ID}, G_{ID}, MPK, d_{ID}$ the algorithm returns signing key SK_{ID}.
Set-Public-Key $(X_{ID}, G_{ID}, MPK, d_{ID})$: This is run by user. Based on the $X_{ID}, G_{ID}, MP??, d_{ID}$ the algorithm returns public key PK_{ID}.
CL-Sign (SK_{ID}, ID, M, MPK): This is run by user (Sender). Based on secret key, ID, public parameters, the algorithm gives the signature δ on the message M.
CL-Verify (MPK, δ, M, ID): Base on the signature, the user (Verifier) can verify the message and do ACCEPT or REJECT.

3 Review of Zhang et al. [16]'s scheme

Setup: Based on security parameter γ, the CA generates RSA parameteres as follows

- It generates two large random numbers p and q. compute $N = pq$. Generates e such that $gcd(e, \phi(N)) = 1$, where $\phi(N)$ is the Euler's totient function.
- Computes d such that $ed = 1 \ mod \ ?(N)$.
- Selects two cryptographic hash functions $H_0 : \{0,1\}^* \rightarrow Z_N$ and $H : Z_N^4 \times \{0,1\}^* \rightarrow \{0,1\}^l$, where l is based on security parameter.
- It sets $MSK = \{d\}$ and $MPK = \{N, e, H_0, H\}$

Partial-Key-Extract: Based on ID, CA computers $d_{ID} = H_0(ID)^{MSK} = H_0(ID)^d$ and send it to user securely.
Set-Secret-Value: User selects X_{ID} and set as secret value.
Set-Private-Key: The users sets $SK_{ID} = \{d_{ID}, X_{ID}\}$.
Set-public-Key: The user publishes his public key $PK_{ID} = H_0(ID)^{X_{ID}} \ mod \ N$.
Sign: The user follow the step as follow.

- It selects $r_1, r_2 \in_R Z_N$. Compute $R_1 = H_0(ID)^{r_1} \ mod \ N$, $R_2 = H_0(ID)^{r_2} \ mod \ N$.
- It computes $h = H(R_1, R_2, ID, PK_{ID}, M)$, $u_1 = d_{ID}^{r_1 - h} = H_0(ID)^{d \ (r_1 - h)} \ mod \ N$ and $u_2 = r_2 - X_{ID} h$.
- It gives $\delta = \{u_1, u_2, h\}$ as signature for message M.

Verify: The verifier computes the step as follow

- It computes $R_1' = u_1^e H_0(ID)^h \ mod \ N$ and $R_2' = H_0(ID)^{u_2} PK_{ID}^h \ mod \ N$.
- It checks whether, h and $H(R_1', R_2', ID, PK_{ID}, M)$. If they are equal then signature or otherwise rejects it.

4 Cryptanalysis of Zhang et al. [16]'s scheme

There are two types of adversary [17] considered for the certificateless signature scheme. They are known as type 1 adversary and type 2 adversary.

- In *type 1* adversary, the adversary is modeled as an outsider that can replace the public id of user with value he wishes. However, he does not have access to secret values.
- In *type 2* adversary, the adversary has access to CA's master key (that generates partial secret key f user). But the adversary cannot change the public key of the user.

In [16], the authors claims that their scheme is resist against both type of adversary. However we show that, the scheme is vulnerable against the type 1 adversary attack as follow.

- Let A be the type 1 adversary that replaces the public id of user as $PK_{ID}' = H_0(ID)^{X_{ID}'} \ mod \ N$, where X_{ID}' is select by adversary.
- A generates $r_1, r_2 \in_R Z_N$ and computes the $R_1 = H_0(ID)^{r_1} \ mod \ N, R_2 = H_0(ID)^{r_2} \ mod \ N$.
- A computes $h = H(R_1, R_2, ID, PK_{ID}', M)$ and check if $r_1 - h$ is divisible by e or not. If not divisible then repeat step 2 and 3.
- Assume that $r_1 - h$ is divisible by e and thus we can write $r_1 - h = eb$, where $b \in Z_N$.
- A computes $u_1 = H_0(ID)^b \ mod \ N$ and $u_2 = r_2 - X_{ID}' h$.
- The signature $\delta = \{u_1, u_2, h\}$ is valid signature on a M as follow,

$$H\left(R_1', R_2', ID, PK_{ID}', M\right)$$

$$= H(u_1^e H_0(ID)^h \ mod \ N, H_0(ID)^{u_2} \left(PK_{ID}'\right)^h \ mod \ N, ID, PK_{ID}', M)$$

$$= H\left(\left(H_0(ID)^b\right)^e H_0(ID)^h \ mod \ N, H_0(ID)^{r_2 - X_{ID}' h} \left(PK_{ID}'\right)^h \ mod \ N, ID, PK_{ID}', M\right)$$

$$= H\left(H_0(ID)^{be} H_0(ID)^h \ mod \ N, H_0(ID)^{r_2 - X_{ID}' h} \left(PK_{ID}'\right)^h \ mod \ N, ID, PK_{ID}', M\right)$$

$$= H\left(H_0(ID)^{r_1 - h} H_0(ID)^h \ mod \ N, H_0(ID)^{r_2 - X_{ID}' h} \left(PK_{ID}'\right)^h \ mod \ N, ID, PK_{ID}', M\right)$$

$$= H\left(H_0(ID)^{r_1} \ mod \ N, H_0(ID)^{r_2 - X_{ID}' h} \left(H_0(ID)^{X_{ID}'}\right)^h \ mod \ N, ID, PK_{ID}', M\right)$$

$$= H\left(H_0(ID)^{r_1} \ mod \ N, H_0(ID)^{r_2} \ mod \ N, ID, PK_{ID}', M\right)$$

$$= h$$

Let us assume that r_1 is a random number. Same way we can assume that h can also be treated random number. Thus A will get success with probability $1/e$ for every r_1. Now for a minimum value of $e = 3$, this probability holds with every 3^{rd} value of r_1 get succeed. As per the NIST standard as well other security standard for RSA, the public exponent for practical purpose is between 3 to 65537 [18-21]. Therefore, even with large public exponent value, A can break in polynomial time.

5 The Proposed Scheme

Here we assume that every user has one identity called GID along with ID. ID will be available publicly while GID is only known to the user itself.

5.1 Setup

Based on security parameter γ, the CA generates RSA parameters as follows

- It generates two large random numbers p and q. Compute $N = pq$. Generates e such that $gcd\ (e, \phi(N))$ =1, where $\phi(N)$ is the Euler's totient function.
- Computes d such that $ed = 1\ mod\ \phi(N)$.
- Selects two cryptographic hash functions $H_0 : \{0,1\}^* \rightarrow Z_N$ and $H : Z_N^4 \times \{0,1\}^* \rightarrow \{0,1\}^l$, where l is based on the security parameter.
- It sets $MSK = \{d\}$ and MPK= $\{N, e, H_0, H\}$

5.2 Partial-Key-Extract

Based on ID, CA computers $d_{ID} = H_0(ID)^{MSK} = H_0(ID)^d\ mod\ N$ and send it to user securely.

5.3 Set-Secret-Value

User selects X_{ID} and set as secret value.

5.4 Set-Private-Key

The user publishes his public key $PK_{ID} = \{H_0(ID)^{X_{ID}}\ mod\ N, H_0(ID)^{GID}\ mod\ N\}$.

5.5 Sign

- It selects $r_1, r_2 \in_R Z_N$.
- Compute $R_1 = X_{ID}^e H_0(ID)^{r_1}\ mod\ N$, $R_2 = H_0(ID)^{GID+2r_2}\ mod\ N$.
- It computes $h = H(R_1, R_2, ID, PK_{ID}, M)$, $u_1 = X_{ID} d_{ID}^{r_1-(\mathrm{GID}+h)}\ mod\ N$ and $u_2 = (GID + r_2 - X_{ID} h)\ mod\ N$.
- It gives $\delta = \{u_1, u_2, h\}$ as signature for message M.

5.6 Verify

The verifier computes the step as follow

- It computes $R_1' = u_1^e H_0(ID)^h\ mod\ N$ and $R_2' = H_0(ID)^{u_2} PK_{ID}^h\ mod\ N$.
- It checks whether, h and $H(R_1', R_2', ID, PK_{ID}, M)$. If they are equal then accept the signature otherwise rejects it.

5.7 Correctness

It is easy to show that the proposed certificateless scheme is correct as follows

$H(\mathrm{R}_1, \mathrm{R}_2, ID, PK_{ID}, M)$

- $= H(u_1^e H_0(ID)^h H_0(ID)^{GID}\ mod\ N,$ $H_0(ID)^{u_2} (PK_{ID})^h\ mod\ N, ID, PK_{ID}, M)$
- $= H((X_{ID} d_{ID}^{r_1-(GID+h)})^e H_0(ID)^{GID+h}\ mod\ N,$ $H_0(ID)^{GID+r_2-X_{ID}h} (PK_{ID})^h\ mod\ N, ID, PK_{ID}, M)$
- $= H(X_{ID}^e (\ d_{ID}^{r_1-(GID+h)})^e H_0(ID)^{GID+h}\ mod\ N,$ $H_0(ID)^{GID+r_2-X_{ID}h} (PK_{ID})^h\ mod\ N, ID, PK_{ID}, M)$
- $= H(X_{ID}^e H_0(ID)^{r_1-(GID+h)} H_0(ID)^{GID+h}\ mod\ N,$ $H_0(ID)^{GID+r_2-X_{ID}h} (PK_{ID})^h\ mod\ N, ID, PK_{ID}, M)$
- $= H(X_{ID}^e H_0(ID)^{r_1}\ mod\ N,$ $H_0(ID)^{GID+r_2-X_{ID}h} (H_0(ID)^{\mathrm{X_{ID}}})^h\ mod\ N, ID, PK_{ID}, M)$
- $= H(X_{ID}^e H_0(ID)^{r_1}\ mod\ N,$ $H_0(ID)^{GID+r_2}\ mod\ N, ID, PK_{ID}, M)$
- $= h$

As one can see that, we have randomized the u_1 term by multiplying it with X_{ID}^e. As attacker has no idea of the value of the GID, he cannot able to generate the u_2 term for the random r_2 and X_{ID}'.

6 Security Proof

Theorem 1: In the random oracle model, if a type I adversary A_I has advantage ϵ against proposed scheme in time T and ask q_{H_0} and q_H queries to random oracles H_0 and H, q_s signature queries, q_{ppk} partial private key queries, and q_p private key extract queries, q_{GID} queries to the random oracle, then there exists an algorithm B that solves the RSA problem with advantage

$$\varepsilon > \frac{(q_s+1)(q_s+q_{H0})\epsilon}{2^l q_H\ T(q_{ppk}+q_p+q_s+q_{GID})}$$

Theorem 2: In the random oracle model, if a type II adversary A_{II} has advantage ? against proposed scheme in time T and ask q_{H_0} and q_H queries to random oracles H_0 and H, q_s signature queries, q_{ppk} partial private key queries, and q_p private key extract queries, q_{GID} queries to the random oracle, then there exists an algorithm B that can make use of A_{II} to solve the DLP (Discrete Logarithm Problem).

7 Conclusion

In this paper, we have given the attack on the scheme of Zhang et al. Thereafter we have proposed the scheme to overcome this attack. One can extend the proposed scheme for the standard model and give rigorous proof based on better mathematical assumptions.

References

[1] P. Gutmann, "Pki: it's not dead, just resting," *Computer*, vol. 35, no. 8, pp. 41 – 49, aug 2002.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin Heidelberg, 1985, vol. 196, pp. 47–53. [Online]. Available: http://dx.doi.org/10.1007/3-540-39568-7_5

[3] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology - ASIACRYPT 2003*, ser. Lecture Notes in Computer Science, C.-S. Laih, Ed. Springer Berlin Heidelberg, 2003, vol. 2894, pp. 452–473. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-40061-5_29

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious kgc attacks in certificateless cryptography," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, ser. ASIACCS '07. New York, NY, USA: ACM, 2007, pp. 302–311. [Online]. Available: http://doi.acm.org/10.1145/1229285.1266997

[5] Q. Huang and D. Wong, "Generic certificateless encryption in the standard model," in *Advances in Information and Computer Security*, ser. Lecture Notes in Computer Science, A. Miyaji, H. Kikuchi, and K. Rannenberg, Eds. Springer Berlin Heidelberg, 2007, vol. 4752, pp. 278–291. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-75651-4_19

[6] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Cryptology and Network Security*, ser. Lecture Notes in Computer Science, Y. Desmedt, H. Wang, Y. Mu, and Y. Li, Eds. Springer Berlin Heidelberg, 2005, vol. 3810, pp. 13–25. [Online]. Available: http://dx.doi.org/10.1007/11599371_2

[7] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateless signature revisited," in *Information Security and Privacy*, ser. Lecture Notes in Computer Science, J. Pieprzyk, H. Ghodosi, and E. Dawson, Eds. Springer Berlin Heidelberg, 2007, vol. 4586, pp. 308–322. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-73458-1_23

[8] J. K. Liu, M. H. Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model: extended abstract," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, ser. ASIACCS '07. New York, NY, USA: ACM, 2007, pp. 273–283. [Online]. Available: http://doi.acm.org/10.1145/1229285.1266994

[9] Y. Yuan, D. Li, L. Tian, and H. Zhu, "Certificateless signature scheme without random oracles," in *Advances in Information Security and Assurance*, ser. Lecture Notes in Computer Science, J. Park, H.-H. Chen, M. Atiquzzaman, C. Lee, T.-h. Kim, and S.-S. Yeo, Eds. Springer Berlin Heidelberg, 2009, vol. 5576, pp. 31–40. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-02617-1_4

[10] Z. Zhang, D. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: Security model and efficient construction," in *Applied Cryptography and Network Security*, ser. Lecture Notes in Computer Science, J. Zhou, M. Yung, and F. Bao, Eds. Springer Berlin Heidelberg, 2006, vol. 3989, pp. 293–308. [Online]. Available: http://dx.doi.org/10.1007/11767480_20

[11] J. Zhang and J. Mao, "Security analysis of two signature schemes and their improved schemes," in *Computational Science and Its Applications ICCSA 2007*, ser. Lecture Notes in Computer Science, O. Gervasi and M. Gavrilova, Eds. Springer Berlin Heidelberg, 2007, vol. 4705, pp. 589–602. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74472-6_48

[12] D. Yum and P. Lee, "Generic construction of certificateless signature," in *Information Security and Privacy*, ser. Lecture Notes in Computer Science, H. Wang, J. Pieprzyk, and V. Varadharajan, Eds. Springer Berlin Heidelberg, 2004, vol. 3108, pp. 200–211. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-27800-9_18

[13] W.-S. Yap, S.-H. Heng, and B.-M. Goi, "An efficient certificateless signature scheme," in *Emerging Directions in Embedded and Ubiquitous Computing*, ser. Lecture Notes in Computer Science, X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, D. Lee, D. Kim, Y.-S. Jeong, and C.-Z. Xu, Eds. Springer Berlin Heidelberg, 2006, vol. 4097, pp. 322–331. [Online]. Available: http://dx.doi.org/10.1007/11807964_33

[14] J. Lai, R. Deng, S. Liu, and W. Kou, "Rsa-based certificateless public key encryption," in *Information Security Practice and Experience*, ser. Lecture Notes in Computer Science, F. Bao, H. Li, and G. Wang, Eds. Springer Berlin Heidelberg, 2009, vol. 5451, pp. 24–34. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-00843-6_3

[15] S. D. Selvi, S. Vivek, and C. Rangan, "Cca2 secure certificateless encryption schemes based on rsa," Cryptology ePrint Archive, Report 2010/459, 2010. [Online]. Available: http://eprint.iacr.org/2010/459

[16] J. Zhang and J. Mao, "An efficient rsa-based certificateless signature scheme," *Journal of Systems and Software*, vol. 85, no. 3, pp. 638 – 642, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121211002445

[17] L. Zhang, "Cryptanalysis of a certificateless multi-proxy signature scheme," in *Distributed Computing and Networking*, ser. Lecture Notes in Computer Science, L. Bononi, A. Datta, S. Devismes, and A. Misra, Eds. Springer Berlin Heidelberg, 2012, vol. 7129, pp. 544–548. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-25959-3_41

[18] "Pkcs, public key cryptography standards, pkcs #1 v2.1, rsa cryptography standard, draft 2,," 2001.

[19] D. Boneh, "Twenty years of attacks on the rsa cryptosystem," *Notices of The Ams*, pp. 203–213, 1999. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=?doi=10.1.1.42.2941

[20] "Wikipedia, rsa (algorithm)." [Online]. Available: http://en.wikipedia.org/wiki/RSA_(algorithm)

[21] B. W. P. W. S. M. Barker E., Barker W., *NIST Special Publication 800-57: Recommendation for Key Management Part1 - General*, 2007.