Malaysian Journal of Mathematical Sciences 9(S) June: 103-113 (2015)
Special Issue: The 4th International Cryptology and Information Security Conference 2014 (Cryptology 2014)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

On the Security of a Certificateless Short Signature Scheme

Rouzbeh Behnia, *Swee-Huay Heng and Syh-Yuan Tan

Faculty of Information Science and Technology,
Multimedia University, Jalan Ayer Keroh Lama,
75450 Bukit Beruang, Melaka, Malaysia

E-mail: shheng@mmu.edu.my

*Corresponding author

ABSTRACT

Certificateless cryptography has attracted much attention due to its distinctive features. By eliminating the certification costs in traditional public key cryptography and addressing the private key escrow problem in identity-based cryptography, certificateless cryptography has become a mesmeric paradigm for developing various cryptographic primitives. Digital signatures with short signature length have always been an attractive area given their applications in handheld devices which are operating with limited computational power in restricted communication bandwidth. However, there has always been a trade-off between the shortness and efficiency of the signatures and their security. In 2012, Tso et al. proposed a new short certificateless signature scheme which claimed to be more secure than the existing signature schemes by being secure against the strongest type adversary in certificateless paradigm (i.e. super adversary). In this paper, we mount a public key replacement attack on their scheme and show that their scheme is insecure against a Type I strong adversary which is much weaker than a super adversary.

Keywords: Certificateless cryptography, short signatures, super adversary, bilinear pairing.

1. INTRODUCTION

In traditional public key paradigms, the authenticity of the users' public keys is delivered by means of signed certificates that are usually published in public bulletins along with users' public keys. Though, the tasks of issuing and managing certificates would become quite costly when such

systems are deployed in a large scale. Shamir, 1985, conceptualised the idea of identity-based cryptography in order to eliminate the need of signed certificates by deriving the users' public keys from their publicly available information such as their email address, ID number, etc. A fully trusted authority called the Private Key Generator (PKG) would then be in place in order to compute the private keys of the users' based on the same publicly available information.

The knowledge of the PKG over the users' private keys introduces the private key escrow problem and establishes a highly repudiated environment if the PKG cannot be completely trusted. Therefore, the use of identity-based systems is limited to highly-trusted settings where the PKG is completely trusted and accepted by all the system users for instance, in cases where the CEO of a company acts as the PKG and all the data being communicated is owned by her/him.

With the aim of overcoming the flaws in the aforementioned cryptographic settings, Al-Riyami and Paterson, 2003, proposed the idea of certificateless cryptography. The new paradigm addresses the costly issues in traditional public key cryptography by eliminating the use of certificates and overcomes the private key escrow problem in identity-based cryptography by hiding the full private key from the trusted third party. Certificateless systems rely on a semi-trusted third party called the Key Generation Centre (KGC) which is in place to calculate a portion of the users' private key called the partial private key. The user's partial private key is derived from her publicly available information and is delivered to the user in a secure manner. The other portion of the user's private key called the secret value is calculated and kept secret by the user. Certificateless systems require the users to calculate and publish their own public keys.

Digital signatures with short signature length have always been an attractive area given their applications in handheld devices which are operating with limited computational power in a restricted communication bandwidth. The first short and efficient signature scheme was proposed by Boneh et al., 2001. Their work started a promising line of research and following their work, variety of short signature schemes with wide range of features have been proposed to the literature (Cha and Cheon, 2003; Hess, 2003; Huang et al., 2007; Katz and Wang, 2003; Yap et al., 2006). The first certificateless short signature scheme was put forth by Huang et al., (2007). The proposed scheme was as efficient as the scheme proposed by Boneh et al., 2001, with similar signature size.

Following the work of Huang et al. (2007), number of certificateless short signature schemes with varying security levels were proposed (Du and Wen, 2009; Fan et al., 2009; Tso et al., 2011). In Tso et al., 2012, put forth a new certificateless scheme with short signature length and proved its security under a weak assumption. The authors claimed that their scheme is better than the existing schemes in term of security as it is the only scheme that can withstand against strongest adversary type, namely super adversary, in the security models of certificateless systems.

1.1. Our Contribution

In this paper, we analyse Tso et al.'s scheme (2012) in detail and identify a weakness in their sign algorithm. We then exploit that weakness and mount a public key replacement attack on their scheme and demonstrate how a strong adversary (to be defined in Section 2.3) which is a weaker adversary than the strongest adversary type (i.e. super adversary) that their scheme is claimed to be secure against can break the unforgeability of their scheme. Our attack proves that although their scheme is slightly costlier than the existing schemes in the literature (Huang et al., 2007; Du and Wen, 2009; Fan et al., 2009; Tso et al., 2011), it does not provide any better security. Therefore, proposing a certificateless short signature scheme that is secure against stronger adversary types remains as an open problem.

1.2. Organisation

The rest of this paper is organised as follows. In Section 2, we provide some preliminary definitions and review the adversarial models in certificateless paradigm. In Section 3, we provide the structure and the security models of Tso et al.'s scheme. In Section 4, we show the details of our public key replacement attack. Finally, we conclude the paper in Section 5.

2. PRELIMINARIES

2.1. Bilinear Pairing

Let $\mathbb{G}_1$ be a cyclic group of prime order q with g as its generator, and $\mathbb{G}_2$ be another cyclic group of the same order (i.e. $|\mathbb{G}_1| = |\mathbb{G}_2| = q$). An admissible bilinear pairing $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is given which is to satisfy the following properties:

- *Bilinearity:* For $g, q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q$, we have $\mathrm{e}(g^a, q^b) = \mathrm{e}(g,\ q)^{\mathrm{ab}}$and $\mathrm{e}(g^a, q^b) = \mathrm{e}(g^{ab}, q)$.

- *Non-degeneracy:* There exists $g, q \in \mathbb{G}_1$ such that $\mathrm{e}(g, q) \neq 1$.
- *Computability:* For every g and $q \in \mathbb{G}_1$, $\mathrm{e}(g, q)$ is efficiently computable.

The Computational Diffie-Hellman (CDH) problem: Given (g, g^a, g^b), for g as a random generator of $\mathbb{G}_1$ and the random selection of $a, b \in \mathbb{Z}_q$ the CDH problem is to compute g^{ab}.

The Inverse Computational Diffie-Hellman (InvCDH) problem: Given (g, g^a), for g as a random generator of $\mathbb{G}_1$ and the random selection of $a \in \mathbb{Z}_q$ the InvCDH problem is to compute $g^{a^{-1}}$.

2.2. Certificateless Signature Scheme

Typically, a certificateless signature scheme consists of seven algorithms (Du and Wen, 2009; Fan et al., 2009; Tso et al., 2011; Tso et al., 2012) as follows.

Setup: Provided a security parameter k, admissible instances of groups $\mathbb{G}_1$ and $\mathbb{G}_2$ will be generated, the KGC's key pair (s, P_{Pub}) are computed where s is the master secret key and P_{Pub} is the corresponding public key. Finally, the system's public parameters $params$ are published in the system. For the sake of brevity, we omit $params$ as the input of the rest of the algorithms/protocols.

Partial-private-key-extraction: Provided the user's identity ID, the user partial private key D_{ID} will be computed by the KGC using its master secret key s.

Set-secret-value: Through this algorithm, the user with identity ID computes her secret value x_{ID}.

Set-private-key: Provided the user secret value x_{ID} and partial private key D_{ID}, the user uses this algorithm to computes her private key SK_{ID}.

Set-public-key: Provided the user secret value x_{ID} and identity ID the user computes her public key PK_{ID}.

Sign: Provided a message $m \in \{0,1\}^*$ to be signed, the user with identity ID uses her private key SK_{ID} to issue a signature σ which is valid for the tuple (m, ID, PK_{ID}).

Verify: Provided a message-signature pair (m, σ), the identity of the possible signer ID with public key PK_{ID}, this algorithm outputs a decision bit $d \in \{valid, invalid\}$ on the validity or invalidity of the signature.

2.3. Adversary Types in Certificateless Signature Schemes

Certificateless systems eliminate the use of certificates on public keys by providing implicit certification which takes place where the KGC computes a portion of the users' private keys. Therefore, since there is no certificate to convey the authenticity of the users' public keys, the security models of certificateless schemes always considers to types of adversaries (Al-Riyami and Paterson, 2003).

- **Type I Adversary:** Type I adversary A_I is similar to an ordinary adversary in conventional public key cryptosystems. This adversary has no possible knowledge on the system's secrets (i.e. the master secret key). However, due to the aforementioned property of certificateless systems, A_I is able to replace the users' public keys with public keys of its choice.

- **Type II Adversary:** Type II adversary A_{II} is acting as a malicious KGC. Since the trust level of the KGC has been remarkably reduced to its counterpart in identity-based systems, it must be ensured that a malicious KGC would not be able to compromise users. Given its knowledge on the master secret key, A_{II} is assumed to be able to compute the users' partial private keys. However, A_{II} is prohibited from replacing the public key of the target user.

In a real world scenario, the adversary that is trying to attack the target user is able to acquire valid signatures singed by the user either by eavesdropping or pretending as a legitimate user. In order to simulate the similar scenario in the security models of signature schemes, the adversary would have access to a sign oracle in order to receive signatures from arbitrary users in the system. The fact that the adversary is able to replace the users' public keys fairly complicates the situation and the dispute arises since the signatures could be valid under the user's genuine or replaced public key.

With the aim of clarifying the complicated situation in the security models of certificateless schemes, Huang et al., 2007, categorised the adversaries based on the capabilities as follows.

- **Normal Type I/II adversary:** Normal adversary is considered as the weakest type of adversary in the security models of certificateless schemes. This adversary is able to query the sign oracle and receive signatures that are valid under the original public of the user.

- **Strong Type I/II adversary:** Strong adversary is considered as a more powerful adversary comparing to normal adversary. Strong adversary is able to receive signatures that are valid under the replaced public keys given it provides the corresponding secret value to the sign oracle.

- **Super Type I/II adversary:** Super adversary is perceived as the strongest adversary type in the security models of certificateless systems. It has the ability to receive valid signatures under the replaced public keys without providing the sign oracle with the corresponding secret value.

More precisely, the relationships between the above adversary types can be shown as follows.

Super ⟶ Strong ⟶ Normal

This implies that if a cryptosystem is secure against a super adversary, then it is definitely secure against strong and normal adversaries.

2.4. Certificateless Signature Scheme (Tso et al., 2012)

In this section, we recall Tso et al., 2012, scheme and review its security. In order to avoid confusion, we use the same notations as in the original paper.

Setup: Provided a security parameter k, the KGC generates groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order $q \geq 2^k$, a generator g of $\mathbb{G}_1$ and an admissible bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. It also chooses two cryptographic hash functions: $H_0: \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_1: \{0,1\}^* \rightarrow \mathbb{G}_1$. Then, it picks $s \in \mathbb{Z}_q$ at random as the master secret key and calculates $P_{Pub} = g^s$ as the corresponding public key. The KGC's public key and the system's public parameters $params$ will be made available to all system users.

$$params = (q, \mathbb{G}_1, \mathbb{G}_2, g, P_{Pub}, H_0, H_1)$$

Partial-private-key-extraction: Provided the identity of the user ID, the KGC computes the user's partial private key as $D_{ID} = Q_{ID}^{s} = H_0(ID)^s$, and delivers it to the user in a secure manner.

Set-secret-value: The user with identity ID picks $x_{ID} \in \mathbb{Z}_q$ randomly as her secret value.

Set-private-key: After the user received her partial private key and computed her secret value, she forms her private key as $SK_{ID} = (x_{ID}, D_{ID})$.

Set-public-key: After computing her private key SK_{ID}, the user computes her public key as $PK_{ID} = \left(PK_{(ID,1)}, PK_{(ID,2)}\right) = \left(D_{ID}^{x_{ID}}, Q_{ID}^{x}\right)$.

Sign: In order to issue a signature on message $m \in \{0,1\}^*$, the signer with identity ID computes $\sigma = D_{ID} \cdot H_1(m \parallel ID \parallel PK_{ID})^{x_{ID}^{-1}}$.

Verify: Provided a message-signature pair (m, σ) and the signer's identity and public key pair (ID, PK_{ID}), the verifier checks if $e\left(P_{Pub}, PK_{(ID,2)}\right) = e(g, PK_{(ID,2)})$ and $e\left(\sigma, PK_{(ID,2)}\right) = e(PK_{(ID,1)} H_1(m \parallel ID \parallel PK_{ID}), Q_{ID}))$ hold, if so he outputs valid. Otherwise, he outputs invalid.

When Al-Riyami and Paterson proposed the notion of certificateless signature schemes and formulated the security models of such schemes for the first time, they considered the adversary to have the equivalent power as the super adversary (Huang et al., 2007) i.e., being able to receive valid signatures under the replaced public keys without requiring to provide the corresponding secret value. This assumption, however, is too strong and claimed to provide better security assurances.

Before Tso et al., 2012, work, all the certificateless short signature schemes were only secure against the normal adversary, i.e. the adversary is not provided with the signatures that are valid under the replaced public keys. More precisely, the security of the schemes would be compromised if the adversary is able to receive valid signatures for the replaced public keys. Tso et al., 2012, proposed the first certificateless short signature scheme which is secure against the super adversary and related the security of the proposed scheme against the Type I and Type II super adversaries to the hardness of the Computational Diffie-Hellman (CDH) and Inverse Computational Diffie-Hellman (InvCDH) problems, respectively.

Nevertheless, in order to achieve such level of security, the signature verification algorithm of the proposed scheme has two additional costly pairing evaluations comparing to the existing schemes (Huang et al., 2007; Du and Wen, 2009; Fan et al., 2009; Tso et al., 2011).

3. PUBLIC KEY REPLACEMENT ATTACK

As it was clearly highlighted in Section 2.3, if a certificateless scheme is secure against the super adversary, then it would be definitely secure against the strong and the normal adversaries. The strong adversary is a much weaker adversary than the super adversary. Moreover, the existence of a strong adversary is a much weaker assumption than a super adversary. In Tso et al., 2012, the authors claimed that their proposed scheme is secure against the super adversary type. In this section, we exploit a weakness in the sign algorithm of their scheme and mount a public key replacement attack to prove that their proposed scheme is not even secure against the strong adversary.

In order to mount the attack, a strong Type I adversary A_I performs the following steps:

- First, A_I picks $x'_{ID} \in \mathbb{Z}_{q^*}$ at random and forms $PK'_{ID} = \left(PK'_{(ID,1)}, PK'_{(ID,2)}\right) = (P_{Pub}^{x'_{ID}}, g^{x'_{ID}})$.
- Next, it replaces the public key of the signer PK_{ID} with PK'_{ID}, provides x'_{ID} to the signer and queries for a signature on message $m \in \{0,1\}^*$.
- Upon receiving such request, the signer outputs the signature as $\sigma^* = D_{ID} \cdot H_1(m \parallel ID \parallel PK'_{ID})^{x'^{-1}_{ID}}$.

  Finally, the adversary A_I computes $H_1(m \parallel ID \parallel PK'_{ID})^{x'^{-1}_{ID}}$ and extracts the signer's partial private key by computing:

$$D_{ID} = \frac{\sigma^*}{H_1(m \parallel ID \parallel PK'_{ID})^{x'^{-1}_{ID}}}$$

- Consequently, by having knowledge on the signer's partial private key D_{ID}, the adversary can generate a new public key as $PK''_{ID} = \left(PK''_{(ID,1)}, PK''_{(ID,2)}\right) = (D_{ID}^{x'_{ID}}, Q_{ID}^{x'_{ID}})$ and forge signatures on any arbitrary message on behalf of the signer at will.

In Step 1, it is trivial to see that the replaced public key $PK'_{ID} = \left(PK'_{(ID,1)}, PK'_{(ID,2)}\right) = (P_{Pub}^{x'_{ID}}, g^{x'_{ID}})$ can pass the public key verification test since $e\left(P_{Pub}, PK'_{(ID,2)}\right) = e(g, PK'_{(ID,2)})$.

In Step 2, when the adversary replaces the public key of the target signer (with identity ID), then, based on the definition of the strong Type I adversary (see Section 2.3), the corresponding secret value should also be presented to the signer's signing oracle. Thus, the output of the oracle would be computed using the secret value that is provided by the adversary.

While the scheme proposed by Tso et al., 2012, was shown to be secure against super adversary, the above public key replacement attack is mounted by a strong adversary which is considered to be much weaker adversary than the super adversary (Huang et al., 2007). Hence, as discussed in Section 2.3 if a scheme is not secure against the strong adversary then it definitely cannot be secure against the super adversary.

4. CONCLUSION

In this paper, we broke the security of Tso et al.'s scheme (2012) by mounting a public key replacement attack and showing that their scheme is not secure against the strong Type I adversary. The proposed scheme could be considered as the most secure efficient certificateless signature scheme in the literature as it provides the shortest signatures. The authors claimed that their scheme is secure against the strongest adversary type (i.e. super adversary) in the security models of certificateless signatures. However, our attack illustrated that their scheme could not withstand attacks against the strong adversary which is considered to be much weaker than the super adversary. Our attack emphasises that proposing certificateless short signature schemes that are secure against either the strong adversary or super adversary remains an open problem.

ACKNOWLEDGEMENT

This research was supported by the FRGS grant (FRGS/2/2013/ICT04/MMU/01/1) and Multimedia University Graduate Research Assistant Scheme.

REFERENCES

Al-Riyami, S. and Paterson, K. (2003). Certificateless public key cryptography, in: C.-S. Laih (Ed.), *Advances in Cryptology - ASIACRYPT 2003*, Vol. 2894 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 452-473.

Boneh, D., Lynn, B. and Shacham, H. (2001). Short signatures from the Weil pairing, in: C. Boyd (Ed.), *Advances in Cryptology - ASIACRYPT 2001*, Vol. 2248 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 514-532.

Cha, J. C. and Cheon, J. H. (2003). An identity-based signature from gap Diffe-Hellman groups, in: Y. Desmedt (Ed.), *Public Key Cryptography - PKC 2003*, Vol. 2567 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 18-30.

Du, H. and Wen, Q. (2009). Efficient and provably-secure certificateless short signature scheme from bilinear pairings. *Computer Standards & Interfaces*. **31**(2): 390- 394.

Fan, C., Hsu, R. and Ho, P. (2009). Cryptanalysis on Du-Wen certificateless short signature scheme. *Proceedings of JWIS09*. Available at http://jwis2009. nsysu.edu.tw/location/paper/Cryptanalysis.

Hess, F. (2003). Efficient identity based signature schemes based on pairings, in: K. Nyberg, H. Heys (Eds.), *Selected Areas in Cryptography*, Vol. 2595 of Lecture Notes in Computer Science, Springer Berlin/ Heidelberg, pp. 310-324.

Huang, X., Mu, Y., Susilo, W., Wong, D. and Wu, W. (2007). Certificateless signature revisited, in: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), *Information Security and Privacy*, Vol. 4586 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 308-322.

Katz, J. and Wang, N. (2003). Efficiency improvements for signature schemes with tight security reductions, in: *Proceedings of the 10th ACM conference on Computer and communications security*, CCS '03, ACM, New York, USA, pp. 155 -164.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes, in: G. Blakley, D. Chaum (Eds.), *Advances in Cryptology - CRYPTO 85*, Vol. 196 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 47-53.

Tso, R., Huang, X. and Susilo, W. (2012). Strongly secure certificateless short signatures. *Journal of Systems and Software*. **85**(6): 1409-1417.

Tso, R., Yi, X. and Huang, X. (2011). Efficient and short certificateless signatures secure against realistic adversaries. *The Journal of Supercomputing*. **55**:173 -191.

Yap, W. S., Heng, S. H. and Goi, B. M. (2006). An efficient certificateless signature scheme, in: X. Zhou, O. Sokolsky, L. Yan, E.S. Jung, Z. Shao, Y. Mu, D. Lee, D. Kim, Y.-S. Jeong, C.-Z. Xu (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing*, Vol. 4097 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 322-331.