Cryptanalysis of Wang et al's Certificateless Signature Scheme without Bilinear Pairings

Kuo-Hui Yeh

[1]*Department of Information Management, National Dong Hwa University, Hualien 97401, Taiwan, R.O.C.*
khyeh@mail.ndhu.edu.tw

***Abstract*—In these years, the design of certificateless signature (CLS) scheme without bilinear pairings has been thoroughly investigated owing to its effectiveness on solving the key escrow problem in identity-based cryptography. In this paper, we identify that Wang et al.'s certificateless signature scheme cannot fulfil its security claims. We present a series of attack processes to demonstrate that Wang et al.'s scheme is insecure against a super type I adversary.**

Keywords – certificateless cryptography; digital signature; cryptanalysis

I. INTRODUCTION

In traditional public key cryptography, digital signature allows a user to sign a message with his/her private key and provide appropriate security, such as non-repudiation property or transaction confidentiality. However, each signature activity must accompany with corresponding certificates to complete. To solve the certificate management problem, Shamir [1] introduced the concept of identity-based cryptosystem, where every user does not have an explicit public key as before. The public key is replaced by his/her publicly available identity information, which can uniquely identify him/her and can be undeniably associated with him/her. The corresponding private key is computed from a one-way trapdoor function of privileged information known only to the system authority, such as key generation center (KGC). Compared to certificate-based cryptosystem, identity-based cryptosystem does not require extra effort and information for users to validate the authenticity of public keys. Later, Al-Riyami and Paterson [2] proposed an approach, namely certificateless public key cryptography (CL-PKC). In this approach, KGC generates partial private key, each user then generates his/her private key and public key using user's secret value and partial private key. This concept was to oppose to KGC having access to each user's private key in identity-based approach and was the absence of digital certificates and their important management overhead. After that, based on the idea of self-certified cryptosystem presented by [2], many researches have focused on the design of certificateless cryptography. Recently, Wang et al. [3] proposed a certificateless signature (CLS) scheme without bilinear pairings. The authors claimed that their proposed scheme is secure against the super adversary. Nevertheless, the security claim is not solid. In this paper, we present a series of attack processes to point out that Wang et al.'s scheme is insecure against a super type I adversary.

II. ADVERSARIES AGAINST CERTIFICATELESS SIGNATURE SCHEME

In general, there exist two categories of adversaries against certificateless signature scheme, i.e. type I and type II Adversaries [2]. The type I adversary models an outside adversary who does not know the master secret key of KGC; however, the type I adversary is able to replace any entity's public key with specific values chosen by the adversary itself. The type II adversary models a malicious KGC who is allowed to access to the master secret key of KGC. Nevertheless, the type II adversary cannot replace the public keys of other entities. In addition, based on the security model defined by Huang et al. [4], type I and II adversaries against CLS schemes can further be classified into three categories: normal, strong and super levels. A normal-level type I (and II) adversary only has the ability to learn valid signatures. A strong-level type I (and II) adversary is able to replace a public key to forge a valid signature when the adversary possesses a corresponding secret value. A super-level type I (and II) adversary is able to learn valid signatures for a replaced public key without any submission. Here, we present the definition of the super-level type I adversary *j* which will mainly be involved with the cryptanalysis of Wang et al.'s CLS scheme [3].

The game is performed between a challenger C and a super-level type I adversary *j* for a CLS scheme as follows.

Initialization: C runs *Setup* phase and generates a master secret key *s*, public system parameters $params$. Next, C keeps s and gives $params$ to the adversary *j*.

Queries: The adversary *j* can adaptively issue the following oracle queries, i.e. *ExtractPartialPrivateKey*(*i*), *ExtractSecretValue*(*i*), *RequestPublicKey*(*i*), *ReplacePublicKey*(*i*), and *Sign*(*i*, *m*), to C.

Output: Eventually, the adversary *j* outputs (ID_t, m_t, σ_t). The adversary *j* wins the game if

(1) *ExtractPartialPrivateKey*(*t*) and *Sign*(*t*, m_t) queries have never been queried.
(2) $1 \leftarrow Verify(params, m_t, PK_t, P_{pub}, \sigma_t)$. Note that PK_t and P_{pub} may be replaced by the adversary *j*.

Definition: A CLS scheme is existentially unforgeable against a super-level type I adversary, if for any polynomially bounded super-level Type I adversary *j*, $Succ_j$ is negligible, where $Succ_j$ is the success probability that *j* wins in the above game.

III. CRYPTANALYSIS OF WANG ET AL.'S CLS SCHEME

In this section, we review the Wang et al.'s CLS scheme and then present the robustness analysis of their scheme.

A. Review of Wang et al.'s scheme

Wang et al.'s CLS scheme includes six phases, i.e. Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Public-Key, Sign and Verify.

Setup: Give *k*, KGC runs the following steps.

(1) Generate a group G of elliptic curve points with prime order n and determine a generator P of G. Randomly select the master secret key $s \in Z_p^*$, compute the master public key $P_{pub} = s \cdot P$.

(2) Choose two secure hash functions $H_1: \{0,1\}^* \times G \times G \rightarrow Z_q^*$ and $H_1: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \rightarrow Z_q^*$. Publish $params = (G, P, P_{pub}, H_1, H_2)$ as system parameters, keep s in secret.

Partial-Private-Key-Extract: Give $params$, s and the user with identity ID_i, KGC runs the following steps.

(1) Randomly select $r_i \in Z_n^*$, compute $R_i = r_i \cdot P$, $h_i = H_1(ID_i, R_i, P_{pub})$ and $s_i = r_i + h_i \cdot s \bmod n$. Return the partial private key $D_i = (s_i, R_i)$ to the user.

(2) Once the user has received D_i, the user can verify the validity of D_i by checking whether the equation $s_i \cdot P = (r_i + h_i \cdot s) \cdot P = R_i + h_i \cdot P_{pub}$ holds.

Set-Secret-Value: Give $params$, the user with identity ID_i randomly selects $x_i \in Z_n^*$ as his/her secret value.

Set-Public-Key: Give $params$ and x_i, the user with identity ID_i computes the user's public key as $PK_i = x_i \cdot P$.

Sign: Give $params$, D_i, x_i and a message m, the user with identity ID_i runs the following steps to generate a signature on m.

(1) Randomly select $t_i \in Z_n^*$, compute $T_i = t_i \cdot P$, $k_i = H_2(ID_i, m, T_i, PK_i, R_i, P_{pub})$ and $\tau_i = t_i + k_i \cdot x_i + s_i \bmod n$.

(2) (R_i, T_i, τ_i) comprises the signature σ_i on m.

Verify: Give $params$, ID_i, PK_i, m and $\sigma_i = (R_i, T_i, \tau_i)$, the verifier runs the following steps to verify the validity of σ_i.

(1) Compute $h_i = H_1(ID_i, R_i, P_{pub})$ and $k_i = H_2(ID_i, m, T_i, PK_i, R_i, P_{pub})$.

(2) Check whether the equation $\tau_i \cdot P = T_i + k_i \cdot PK_i + R_i + h_i \cdot P_{pub}$ holds, σ_i is accepted if the equation holds.

Correctness:

$$\begin{aligned} &\tau_i \cdot P \\ &= (t_i + k_i \cdot x_i + s_i) \cdot P \\ &= t_i \cdot P + k_i \cdot x_i \cdot P + s_i \cdot P \\ &= t_i \cdot P + k_i \cdot x_i \cdot P + (r_i + h_i \cdot s) \cdot P \\ &= T_i + k_i \cdot PK_i + R_i + h_i \cdot P_{pub} \end{aligned}$$

B. Cryptanalysis of Wang et al.'s scheme

The Wang et al.'s scheme is vulnerable to a type I adversary with the following attack procedures. Suppose there exists a malicious type I adversary *j* which intends to forge a valid signature $\sigma_i = (R_i, T_i', \tau_i')$ on a message *m'* chosen by the adversary *j*.

(3) The adversary j eavesdrops a valid signature $\sigma_i = (R_i, T_i, \tau_i)$ with message m issued by the user i from any previous session, where $T_i = t_i \cdot P$, $R_i = r_i \cdot P$, $h_i = H_1(ID_i, R_i, P_{pub})$, $k_i = H_2(ID_i, m, T_i, PK_i, R_i, P_{pub})$ and $s_i = r_i + h_i \cdot s \bmod n$, $\tau_i = t_i + k_i \cdot x_i + s_i \bmod n$.

(4) The adversary j performs the following computations to forge a valid signature on a chosen message *m'*. Since the adversary j is a Type I adversary, j can issue an oracle query of *ExtractSecretValue*(i) and replace any entity's public key including KGC's public key.

- Known values retrieved from previous session: $T_i = t_i \cdot P$, $R_i = r_i \cdot P$, $PK_i = x_i \cdot P$, $P_{pub} = s \cdot P$, $h_i = H_1(ID_i, R_i, P_{pub})$ and $k_i = H_2(ID_i, m, T_i, PK_i, R_i, P_{pub})$.

- The adversary j chooses a random number $t_a \in Z_n^*$, and derives

$$\begin{aligned} T_a &= t_a \cdot P, T_i' = T_a + T_i, \\ k_i' &= H_2(ID_i, m', T_i', PK_i, R_i, P_{pub}) \text{ and} \\ \tau_i' &= \tau_i - k_i \cdot x_i + k_i' \cdot x_i + t_a \\ &= t_i + k_i \cdot x_i + s_i - k_i \cdot x_i + k_i' \cdot x_i + t_a \\ &= (t_i + t_a) + k_i' \cdot x_i + s_i \bmod n \end{aligned}$$

- Now, the adversary j can forge a valid signature $\sigma_i' = (R_i, T_i', \tau_i')$ on the chosen message *m'*. Note that the secret x_i can be retrieved via *ExtractSecretValue*(i) query.

$$\begin{aligned} &\tau_i' \cdot P \\ &= [(t_i + t_a) + k_i' \cdot x_i + s_i] \cdot P \\ &= (t_i + t_a) \cdot P + k_i' \cdot x_i \cdot P + (r_i + h_i \cdot s) \cdot P \\ &= (T_a + T_i) + k_i' \cdot PK_i + r_i \cdot P + h_i \cdot s \cdot P \\ &= T_i' + k_i' \cdot PK_i + R_i + h_i \cdot P_{pub} \end{aligned}$$

IV. CONCLUSIONS

In this paper, we have demonstrated that Wang et al.'s CLS scheme is vulnerable to a malicious attack processes launched by a super type I adversary. This security vulnerability results from the weak design of value τ_i. In the future, the redesign of the CLS scheme will be concentrated.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," In *Proceedings of CRYPTO'84*, Lecture Notes in Computer Science, Vol. 196, pp. 47–53, 1985.

[2] S. Al-Riyami and K. Paterson, Certificateless public key cryptography. In *Proceedings of ASIACRYPT 2003*, Lecture Notes in Computer Science, Vol. 2894, pp. 452–473, 2003.

[3] Liangliang Wang, Kefei Chen, Yu Long, Xianping Mao and Huige Wang, "A Modified Efficient Certificateless Signature Scheme without Bilinear Pairings," 2015 International Conference on Intelligent Networking and Collaborative Systems (INCOS), DOI: 10.1109/INCoS.2015.10, 2015.

[4] X. Huang, Y. Mu, W. Susilo, D.S.Wong and W. Wu, Certificateless signature revisited. In *Proceedings of ACISP 2007*, Lecture Notes in Computer Science, Vol. 4586, pp. 308–322, 2007.