Security Analysis of One Lightweight Certificateless Mutual Authentication Scheme Based on Signatures for IIoT

Zhengjun Cao, Lihua Liu

Abstract. We show that the certificateless signature scheme [IEEE ITJ, 26852-26865, 2024] is insecure against public key replacement attack. An adversary can forge signatures for any message by replacing the signer's public key. We find the two components δ_A and T_A of signature $\sigma_A = (m_A, ID_A, \delta_A, T_A)$ are not tightly bound to the target message m_A and the singer's identity ID_A. The inherent flaw results in that the adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm. The findings could be helpful for researchers unfamiliar with the designing techniques for certificateless signatures.
Keywords: Certificateless signature, forgery attack, signing algorithm, verification algorithm.

1 Introduction

Digital signature provides a means for an entity to bind its identity to a piece of information. The process of signing entails transforming the message and some secret information held by the entity into a tag called a signature. A verification algorithm is a method for verifying that a digital signature is authentic (i.e., was indeed created by the specified entity). For a signature scheme, the goal of an adversary is to forge signatures—produce signatures which will be accepted as those of some other entity.

Certificateless public key cryptography introduced by Al-Riyami and Paterson [1], does not require the use of certificates to guarantee the authenticity of signer's public key. But the system parameters and signer' ID must be authentic. Very recently, Yin and Gong [4] have proposed a certificateless signature scheme. Though the scheme is interesting, we find it is insecure. An adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm, even though he cannot compute the private key information of any signer. This drawback is due to that the two components of final signature are not tightly bound to the target message and the singer's certificateless public key.

Z. Cao, Department of Mathematics, Shanghai University, Shanghai, 200444, China.
L. Liu, Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

2 Review of Yin-Gong certificateless signature

The scheme consists of five phases: Setup, User registration, Signature generation, Signature verification, and Batch signature verification. The involved notations are listed below (Table 1).

Table 1: Notations and descriptions

Notation	Description
KGC	semitrusted third party
IIoT device	Industrial Internet of Things device
G_1	additive cyclic group of prime order q
P	a generator of G_1
P_{pub}	system public key
ID_i	identity of user u_i
$\|$	string concatenation
R_i	partial public key of user u_i
y_i	partial private key of user u_i
$SK_i = (x_i, D_i)$	full private key of user u_i
$PK_i = (P_i, R_i)$	full public key of user u_i

Setup. The KGC chooses a group G_1 with prime order q, and its generator P. Choose two hash functions $H_1 : \{0,1\}^* \times G_1 \to Z_q^*$, and $H_2 : \{0,1\}^* \times \{0,1\}^* \times G_1 \times G_1 \times G_1 \times G_1 \times \{0,1\}^* \to Z_q^*$. KGC randomly selects $s \in Z_q^*$ as the master key, and generates the system public key $P_{pub} = sP$. Publish the system parameter $params = \{G_1, q, P, P_{pub}, H_1, H_2\}$.

The User Registration, Signature Generation, and Signature Verification phases can be depicted as follows (Table 2)

Notice that in the above verification process, the verifier Bob needs to use P_A, R_A to verify the signature σ_A.

3 Insecure against forgery attack

In the considered scenario, it assumes that there are two types of attackers (§D, page 26857, [4]):

- *attacker $\mathcal{A}_1$ who can replace any user's public key and get any information in the public channel, but cannot access the master key*;
- attacker $\mathcal{A}_2$ who can obtain the master key of KGC and any information in the public channel, but cannot change any user's public key.

The verification process of Yin-Gong certificateless signature scheme is to check if

$$T_A = \delta_A R_A - H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A)P$$

where ID_A, ID_B, P, P_{pub} are authentic and cannot be replaced. But P_A, R_A are not authentic, and can be replaced, because they are not guaranteed by any certificate.

Table 2: The Yin-Gong certificateless signature

U_i	Reg.	KGC
Pick $x_i \in Z_q^*$, compute $P_i = x_i P$.	$\xrightarrow{ID_i, P_i}$	Pick $r_i \in Z_q^*$, compute $Q_i = H_1(ID_i, P_i)$, $y_i = 1/(r_i + sQ_i)$, $R_i = r_i P + Q_i P_{pub}$.
Compute $D_i = x_i y_i$. Store $PK_i = (P_i, R_i)$, and $SK_i = (x_i, D_i)$.	$\xleftarrow{R_i, y_i}$	
Alice	**Sig./Ver.**	**Bob**
Given m_A, pick $a \in Z_q^*$, compute $T_A = aP_A$, $h_{1,A} = H_2(ID_A, ID_B$, $T_A, P_A, R_A, P_{pub}, m_A)$, $\delta_A = D_A(h_{1,A} x_A^{-1} + a)$, $\sigma_A = (m_A, ID_A, \delta_A, T_A)$.	$\xrightarrow{\sigma_A}$	Given σ_A, compute $h'_{1,A} = H_2(ID_A, ID_B$, $T_A, P_A, R_A, P_{pub}, m_A)$, $T'_A = \delta_A R_A - h'_{1,A} P$. Check if $T'_A = T_A$.

We find the signature scheme is insecure because the adversary $\mathcal{A}_1$ can forge signatures for any message. Given the system public parameters G_1, q, P, P_{pub}, H_2, any message m_A, and target identities ID_A, ID_B, the adversary picks $\theta_1, \theta_2 \in Z_q^*$, and replaces the target public key R_A with

$$R_A \leftarrow \theta_1 P.$$

Then compute $T_A = \theta_2 P$ and

$$\delta_A = \theta_1^{-1}(\theta_2 + H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A)) \bmod q.$$

Output the signature (T_A, δ_A).

Correctness. The forged signature will be accepted because

$$\begin{aligned}
&\delta_A R_A - H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A)P \\
=&\theta_1^{-1}(\theta_2 + H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A))\theta_1 P - H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A)P \\
=&(\theta_2 + H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A))P - H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A)P \\
=&\theta_2 P = T_A.
\end{aligned}$$

4 Further discussions

In certificateless public key cryptogrphy, the signer's public key should be tightly bound to the system public key. One can check the dependency so as to confirm that the signer's public key is really unreplaced by any adversary. But Yin and Gong [4] have forgotten the necessary

requirement. The user's public key is simply set as

$$P_i = x_i P, \quad R_i = r_i P + H_1(ID_i, P_i) P_{pub},$$

where x_i is only known to the user, and r_i is only known to the KGC. It has not specified any mechanism to check the necessary dependency. So, it seems difficult to fix the scheme without a thorough Setup phase and Registration phase.

For readers' conveniences, we now restate the certificateless signature scheme [2] to clarify the mechanism for authenticating the signer's public key and the signature concurrently (Table 3).

Table 3: The Chen et al.'s certificateless signature

Setup. Let G_1 be an additive cyclic group of prime order q, G_T be a multiplicative cyclic group of the same order, $P \in G_1$ be a generator, and $e : G_1 \times G_1 \to G_T$ be a bilinear pairing. $H_0 : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to G_1$ and $H_2 : \{0,1\}^* \to G_1$ are three hash functions. The KGC selects a master key $s \in Z_q^*$ to compute $P_{pub} = sP$. Set $param = \{G_1, G_2, e, q, P, P_{pub}, H_0, H_1, H_2\}$.
Partial-Private-Key-Extract. For the identifier $ID \in \{0,1\}^*$, the KGC chooses $x \in Z_q^*$ to compute $pk_{ID,2} = xP$ and $D_{ID} = x + sH_0(ID \| pk_{ID,2} \| P_{pub})$. Send $D_{ID}, pk_{ID,2}$ to the user via a secure channel.
Set-Private-Key. The user selects $r_{ID} \in Z_q^*$ as the private key.
Set-Public-Key. The user sets the public key $pk_{ID} = \{pk_{ID,1}, pk_{ID,2}\}$, where $pk_{ID,1} = r_{ID} P$.
Sign. Given a message M, the signer computes $T_1 = H_1(m \| ID \| pk_{ID} \| P_{pub})$, $T_2 = H_2(m \| ID \| pk_{ID} \| P_{pub})$, and the signature $\sigma = r_{ID} T_1 + D_{ID} T_2$.
Verify. Given M, σ, ID, pk_{ID}, and $param$, the verifier computes $h = H_0(ID \| pk_{ID,2} \| P_{pub})$, $T_1 = H_1(m \| ID \| pk_{ID} \| P_{pub})$, $T_2 = H_2(m \| ID \| pk_{ID} \| P_{pub})$. Then check that $e(\sigma, P) = e(pk_{ID,1}, T_1) e(pk_{ID,2} + hP_{pub}, T_2)$.

In the Chen et al.'s certificateless signature scheme [2], the verification equation is actually expressed as

$$\begin{aligned} e(\sigma, P) =& e(pk_{ID,1}, H_1(m \| ID \| pk_{ID} \| P_{pub})) \\ & \cdot e(pk_{ID,2} + H_0(ID \| pk_{ID,2} \| P_{pub}) P_{pub}, H_2(m \| ID \| pk_{ID} \| P_{pub})) \end{aligned}$$

The red-colored parameters P, P_{pub}, ID are authentic and cannot be replaced. Though the blue-colored parameters (the signer's public key) are not directly authenticated, they are tightly and synchronously bound to these authentic parameters by using hash functions and the bilinear map e. In this case, the adversary is forced to solve the elliptic curve discrete logarithm problems of $H_1(m \| ID \| pk_{ID} \| P_{pub})$, $H_2(m \| ID \| pk_{ID} \| P_{pub})$, $H_0(ID \| pk_{ID,2} \| P_{pub}) P_{pub}$, with respect to the base point P.

The Yin-Gong signature scheme uses the system public parameter P_{pub} in a very simple

mode, i.e., invoking P_{pub} as a padding parameter in isolation for the hashing

$$H_2(ID_A, ID_B, T_A, P_A, R_A, P_{pub}, m_A).$$

It fails to make use of the explicit dependency between the system public key P_{pub} and the master key s to construct a true intractable problem. The security argument for Lemma 1 (page 26863, [4]) misused the Forking Lemma [3].

5 Conclusion

We show that the Yin-Gong certificateless signature scheme cannot resist public key replacement attack. We also restate a secure certificateless signature scheme to illustrate the basic mechanism for constructing intractable problems in certificateless signature schemes. The analysis techniques developed in this note could be helpful for the future work on designing such schemes.

References

[1] S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In Chi-Sung Laih, editor, *Proc. ASIACRYPT'03*, volume 2894 of *Lecture Notes in Computer Science*, pages 452–473. Springer, 2003.

[2] Y. C. Chen, R. Tso, W. Susilo, X. Huang, and G. Horng. Certificateless signatures: Structural extensions of security models and new provably secure schemes. Cryptology ePrint Archive, Paper 2013/193, 2013.

[3] D. Pointcheval and J. Stern. Security proofs for signature schemes. In *Proc. EUROCRYPT'96*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398. Springer, 1996.

[4] D. Yin and B. Gong. A lightweight certificateless mutual authentication scheme based on signatures for iiot. *IEEE Internet Things J.*, 11(16):26852–26865, 2024.