Insecurity of One Ring Signature Scheme with Batch Verification for Applications in VANETs

Zhengjun Cao, Lihua Liu

Abstract. We show that the Negi-Kumar certificateless ring signature scheme [Wirel. Pers. Commun. 134(4): 1987-2011 (2024)] is insecure against forgery attack. The signer's public key PK_j and secret key PSK_j are simply invoked to compute the hash value $H_{2_j} = h_5(m_j \| PSK_j \| PK_j \| t_j)$, which cannot be retrieved by the verifier for checking their dependency. The explicit dependency between the public key and secret key is not properly used to construct some intractable problems, such as Elliptic Curve Discrete Logarithm (ECDL), Computational Diffie-Hellman (CDH), and Decisional Diffie-Hellman (DDH). An adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm. The findings in this note could be helpful for the newcomers who are not familiar with the designing techniques for certificateless ring signature.

Keywords: Ring signature, Certificateless signature, Forgery attack, Batch verification.

1 Introduction

Digital signature is a fundamental cryptographic primitive in authentication, authorization, and nonrepudiation. Its purpose is to provide 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 [8]. 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.

Ring signature, introduced by Rivest, Shamir and Tauman [12], refers to the anonymous way of singing the message without revealing the real identity of the user in a group. Hara and Tanaka [4, 5] discussed some tightly secure ring signatures in the standard model. Odoom et al. [11] presented a forward-secure key-insulated linkable ring signature scheme in ID-based setting. Ishizaka and Fukushima [6] proposed an identity-based ring signature based on linearly homomorphic signatures. Yamashita and Hara [13] showed the black-box impossibility of multi-designated verifiers signature schemes from ring signature schemes. Nakanishi et al. [9] designed a short DL-based blacklistable ring signature from dual ring. Kolby et al. [7] proposed some multi designated verifier ring signatures.

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

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 must be authentic. Chen et al. [3] investigated the structural extensions of security models for certificateless signatures. Bouakkaz and Semchedin [2] presented a certificateless ring signature scheme with batch verification for applications in Vehicular Adhoc Networks (VANETs).

Very recently, Negi and Kumar [10] have proposed a certificateless signature scheme with batch verification for VANETs. 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 signer's public key PK_j and secret key PSK_j are simply invoked to compute the hash $H_{2_j} = h_5(m_j \| PSK_j \| PK_j \| t_j)$. The explicit dependency between the public key and secret key is not properly used to construct some intractable problems. Besides, we also correct some typos in their presentation so as to clarify some misunderstandings.

2 Review of Negi-Kumar ring signature scheme

The scheme involves three parties: OBUs, RSUs and TRA. Each communication device OBU is pre-installed on the vehicles, can be used for exchanging messages. A road side unit RSU is used as mediator between OBUs and TRA. TRA is a trusted authority to generate the public parameters and other necessary information. The security requirements include authentication, privacy, unforgeability, non-repudiation, and traceability (see page 1991, [10]).

For a certificateless signature, it assumes that there are two types of attackers [3]:

- 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 TRA and any information in the public channel, but cannot change any user's public key.

The involved notations and their descriptions are listed below (see Table 1). The scheme can be described as follows (Table 2).

Table 1: Symbols and descriptions

symbol	description	symbol	description
OBU	On Board Unit	RSU	Road Side Unit
TRA	Trusted Root Authority	$h_1, \cdots, h_5$	hash functions
p	prime number	$\mathbb{Z}_p^*$	$\{1, 2, \cdots, p-1\}$
G_{add}	additive group of order p	G_{mul}	multiplicative group
T_{pbk}	system public key	T_{msk}	system master key
ID_k	identity of k-th entity	PK_k	public key for ID_k
PSK_k	partial private key for ID_k	SK_k	private key for ID_k
$L_k = \cup_{k=1}^{n}\{ID_k\}$	list of identities	$L_{PK} = \cup_{k=1}^{n}\{PK\}_k$	List of public key

Table 2: The Negi-Kumar ring signature scheme

Setup. TRA chooses groups G_{add}, G_{mul} of prime order p, with a generator $X \in G_{add}$, and the bilinear map $e : G_{add} \times G_{add} \to G_{mul}$. Choose $r \in \mathbb{Z}_p^*$ as T_{msk}, compute the system public key $T_{pbk} = rX$. Choose hash functions $h_2 : \{0,1\}^* \times G_{add} \times G_{add} \times G_{add} \to \mathbb{Z}_p^*$, $h_1 : \{0,1\}^* \to G_{add}$, $h_3 : \{0,1\}^* \to \mathbb{Z}_p^*$, $h_4 : \{0,1\}^* \to \mathbb{Z}_p^*$, $h_5 : \{0,1\}^* \to \mathbb{Z}_p^*$. publish the system parameters $vars = \{G_{add}, G_{mul}, X, p, T_{pbk}, h_1, \cdots, h_5\}$.
Registration. Each entity (RSU or OBU) with the identifier $ID_k \in \{0,1\}^*$, picks $v_k \in \mathbb{Z}_p^*$ to compute $V_k = v_k h_1(ID_k), D_k = v_k X$. Send (V_k, D_k) to TRA for registration.
Partial key generation. For the request (V_k, D_k) from ID_k, TRA picks $o_k \in \mathbb{Z}_p^*$ to compute $O_k = o_k X$, $H_{1_k} = h_2(ID_k, V_k, D_k, O_k)$, $PSK_k = rH_{1_k} h_1(ID_k)$. Return O_k, PSK_k, H_{1_k} to the requester.
Secret key generation. Store the secret key $SK_k = (v_k, PSK_k)$ and set the certificateless public key as $PK_k = (V_K, D_K)$.
Signing. For the ring $L_{ID} = \{ID_1, \cdots, ID_n\}$ and $L_{PK} = \{PK_1, \cdots, PK_n\}$, the signer ID_k picks $t_j \in$ to compute $H_{2_j} = h_5(m_j \| PSK_j \| PK_j \| t_j)$, $T_j = H_{1_j}(t_j + H_{2_j})V_j$. For other public keys in $L_{PK} \backslash \{j\}$, pick $T_k \in G_{add}$ for $k \in \{1, \cdots, n\} \backslash \{j\}$ to compute $H_{T_j} = \sum_{k=1}^{n} h_4(m_j \| T_k)$, $H_{3_j} = h_5(m_j \| L_{ID} \| L_{PK} \| H_{T_j})$, $U_j = (t_j + H_{2_j}) H_{3_j} v_j PSK_j$. Send $\sigma_j = (H_{T_j}, T_j, U_j)$ and the message m_j to the verifier.
Verification. The verifier check that $e(U_j, X) = e(h_5(m_j \| L_{ID} \| L_{PK} \| H_{T_j}) T_j, T_{pbk})$. If true, accept the signature. Otherwise, reject it.
Batch verification. For n signatures $\sigma_j = (H_{T_j}, T_j, U_j)$ and m_j, $j = 1, \cdots, n$, RSU checks that $e(\sum_{j=1}^{n} U_j, X) = e(\sum_{j=1}^{n} h_5(m_j \| L_{ID} \| L_{PK} \| H_{T_j}) T_j, T_{pbk})$.

3 Insecure against forgery attack

3.1 Some typos

The original presentation of the Negi-Kumar certificateless ring signature scheme has some typos. For example, in the signing and verification phases, the below expressions (Fig.1, see page 1997, Ref.[10]) are inconsistent.

(i) The OBU ID_j randomly selects $t_j \in \mathbb{Z}_p^*$.
(ii) Computes $H_{2_j} = h_5(m_j \| PSK_j \| PK_j \| t_j) \in \mathbb{Z}_p^*$.
(iii) Computes $t_j = H_{1_j}(t_j + H_{2_j})V_j \in G_{add}$.

(i) Computes $H_{3_j}{}' = h_5(m_j \| L_{ID} \| L_{PK} \| H_{T_j}) \in \mathbb{Z}_p^*$.
(ii) RSU ID_r verifies the following equation:

$e(U_j, X) = e(H_{3_j}{}', T_j, T_{pbk})$

Figure 1: Some typos

They should be corrected as

$$t_j = H_{1_j}(t_j + H_{2_j})V_j \quad \longrightarrow \quad T_j = H_{1_j}(t_j + H_{2_j})V_j,$$
$$e(U_j, X) = e(h_3', T_j, T_{pbk}) \quad \longrightarrow \quad e(U_j, X) = e(h_3' T_j, T_{pbk}).$$

because

$$t_j \in \mathbb{Z}_p^*, \quad H_{2_j} = h_5(m_j \| PSK_j \| PK_j \| t_j) \in \mathbb{Z}_p^*,$$
$$H_{1_j} = h_2(ID_j, V_j, D_j, O_j) \in \mathbb{Z}_p^*, \quad (t_j + H_{2_j}) \in \mathbb{Z}_p^*,$$
$$V_j = v_j h_1(ID_j) \in G_{add}$$

Clearly, $t_j \in \mathbb{Z}_p^*$, $H_{1_j}(t_j + H_{2_j})V_j \in G_{add}$, and the equality $t_j = H_{1_j}(t_j + H_{2_j})V_j$ does not hold. The original presentation has confused the elements in two different groups. Besides, we want to stress that the bilinear map e has two arguments, not three arguments.

3.2 Forge signatures for any message

As we see, the verification equation is eventually specified as

$$e(U_j, X) = e(h_5(m_j \| L_{ID} \| L_{PK} \| H_{T_j})T_j, T_{pbk}) \tag{1}$$

where U_j, H_{T_j}, T_j consist of the signature σ_j. Both X and T_{pbk} are two system public parameters. They are authenticated, and cannot be replaced. But the certificateless public key $L_{PK} = \{PK_1, \cdots, PK_n\}$ is used simply and in isolation to compute the hash value $h_5(m_j \| L_{ID} \| L_{PK} \| H_{T_j})$. We find the signature scheme cannot resist neither attacker $\mathcal{A}_1$ nor attacker $\mathcal{A}_2$. For instance, given a message m, an adversary picks two random integers $\theta_1, \theta_2 \in \mathbb{Z}_p^*$ to compute

$$T_j = \theta_1 X, \quad H_{T_j} = \theta_2 X, \quad U_j = h_5(m \| L_{ID} \| L_{PK} \| H_{T_j})\theta_1 T_{pbk},$$

where L_{ID}, L_{PK} are publicly accessible. Output the forged signature (U_j, H_{T_j}, T_j) and the message m.

We now show that the forged signature can pass the verification phase. In fact,

$$\begin{aligned} e(U_j, X) &= e(h_5(m \| L_{ID} \| L_{PK} \| H_{T_j})\theta_1 T_{pbk}, X) \\ &\xrightarrow{\text{[bilinear]}} e(T_{pbk}, X)^{h_5(m \| L_{ID} \| L_{PK} \| H_{T_j})\theta_1} \\ &= e(T_{pbk}, h_5(m \| L_{ID} \| L_{PK} \| H_{T_j})\theta_1 X) \\ &= e(T_{pbk}, h_5(m \| L_{ID} \| L_{PK} \| H_{T_j})T_j) \\ &\xrightarrow{\text{[communicative]}} e(h_5(m \| L_{ID} \| L_{PK} \| H_{T_j})T_j, T_{pbk}) \end{aligned}$$

By the way, the security proof for Theorem 1 (page 1998, Ref.[10]) is flawed because the adversary is not forced to extract the partial private key. The original claim that "*Eve I cannot run the Q_3 to extract the partial private key*" makes no sense, because it cannot be logically reduced to any intractable problem.

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 Negi and Kumar [10] have forgotten the necessary

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

$$V_k = v_k h_1(ID_k), \quad D_k = v_k X,$$

where v_k is only known to the signer. It has not specified any mechanism to check the necessary dependency. Actually, in the original presentation, the explicit dependency between the signer's certificateless public key and secret key is not used at all.

In the Negi-Kumar certificateless ring signature scheme, the signer's public key PK_j and secret key PSK_j are simply invoked to compute the hash value

$$H_{2_j} = h_5(m_j \| PSK_j \| PK_j \| t_j), \tag{2}$$

which cannot be retrieved by the verifier for checking their dependency. The explicit dependency between the public key and secret key is not properly used to construct some intractable problems, such as Elliptic Curve Discrete Logarithm (ECDL), Computational Diffie-Hellman (CDH), and Decisional Diffie-Hellman (DDH). So, it seems difficult to fix the Negi-Kumar ring signature scheme without thorough Setup phase, Registration phase, and Secret key generation phase. For readers' conveniences, we refer to the certificateless signature schemes [3] for the techniques to clarify the mechanism for authenticating the signer's public key and the signature concurrently.

5 Conclusion

We show that the Negi-Kumar certificateless ring signature scheme is insecure against forgery attack, because an adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm. We hope the findings 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, Heidelberg, 2003. Springer.

[2] S. Bouakkaz and F. Semchedine. A certificateless ring signature scheme with batch verification for applications in VANET. *J. Inf. Secur. Appl.*, 55:102669, 2020.

[3] 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.

[4] K. Hara. A logarithmic-sized accountable ring signature scheme in the standard model. *Theor. Comput. Sci.*, 997:114516, 2024.

[5] K. Hara and K. Tanaka. Tightly secure ring signatures in the standard model. *Theor. Comput. Sci.*, 892:208–237, 2021.

[6] M Ishizaka and K Fukushima. Wildcarded identity-based ring signatures based on linearly homomorphic signatures. *J. Inf. Secur. Appl.*, 75:103499, 2023.

[7] S. Kolby, E. Pagnin, and S. Yakoubov. Multi designated verifier ring signatures. *IACR Commun. Cryptol.*, 1(3):28, 2024.

[8] A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, USA, 1996.

[9] T. Nakanishi, A. Iriboshi, and K. Imai. Short dl-based blacklistable ring signatures from dualring. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 107(3):464–475, 2024.

[10] L. Negi and D. Kumar. A bilinear mapping based ring signature scheme with batch verification for applications in vanets. *Wirel. Pers. Commun.*, 134(4):1987–2011, 2024.

[11] J. Odoom, X. Huang, and L. Wang. Stateless forward-secure key-insulated linkable ring signature scheme in id-based setting. *J. Syst. Archit.*, 129:102600, 2022.

[12] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret: Theory and applications of ring signatures. In Oded Goldreich, Arnold L. Rosenberg, and Alan L. Selman, editors, *Theoretical Computer Science, Essays in Memory of Shimon Even*, volume 3895 of *Lecture Notes in Computer Science*, pages 164–186, Heidelberg, 2006. Springer.

[13] K. Yamashita and K. Hara. On the black-box impossibility of multi-designated verifiers signature schemes from ring signature schemes. *J. Math. Cryptol.*, 18(1), 2024.