Cryptanalysis of an Identity-Based Convertible Undeniable Signature Scheme

Rouzbeh Behnia, Syh-Yuan Tan(✉), and Swee-Huay Heng

Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia
{rouzbeh,sytan,shheng}@mmu.edu.my

Abstract. In this paper, we cryptanalyze an identity-based convertible undeniable signature scheme which claimed to be secure under the random oracle model. Our result shows that the signature leaks information on signer identity and fails to provide both invisibility and anonymity under the known message attack. We propose a fix for the vulnerability by removing some information from the signature with the need for the signer to keep the record of every signed message.

Keywords: Cryptanalysis · Anonymity · Invisibility · Undeniable signature

1 Introduction

Chaum and van Antwerpen [2] introduced the notion of undeniable signature schemes to enable the signer to control the verifiability of her signature. The verification can only take place with the direct participation of the signer in the confirmation or disavowal protocol. Boyar et al. [1] introduced a new extension, namely, convertible undeniable signature (CUS) which enables the signer to selectively, or universally convert one or all of her undeniable signatures to publicly verifiable ones. If universal conversion is performed, an undeniable signature scheme turns into an ordinary signature scheme.

The ultimate goal in undeniable signatures and its extensions is to protect the privacy of the signer. Traditionally, the notion of invisibility [3] was the main requirement for an undeniable signature scheme. Invisibility implies the inability of a user to distinguish an undeniable signature from a random element in the signature space. However, as the main objective of undeniable signature is to hide the link between the signer's public key and the signature and as shown by Galbraith and Mao [4], the notion of anonymity has become the most relevant security notion for undeniable signatures and its extensions in multiuser settings. Given an undeniable signature and public keys of two or more possible signers, the notion of anonymity implies the infeasibility to determine which user has issued the signature. Galbraith and Mao highlighted that the notions of invisibility and anonymity are equivalent and proved that if an undeniable

R.C.-W. Phan and M. Yung (Eds.): LNCS 10311, Mycrypt 2016, pp. 474–477, 2017.
DOI: 10.1007/978-3-319-61273-7_23

signature scheme has the property of invisibility, then it also has anonymity, and vice versa. The importance of anonymity in the context of CUS schemes was further stressed on by Huang et al. [5].

Our Contribution. In this paper, we cryptanalyze the invisibility and anonymity of the first identity-based convertible undeniable signature (IBCUS) scheme proposed by Wu et al. [7]. We find that while the scheme was claimed to be invisible, it is vulnerable to known message attack and does not provide any sense of invisibility as well as anonymity for the signer and the other involved users. Subsequently, we propose a workaround for the discovered vulnerability to resist the known message attack.

The organization of the paper is as follows. In Sect. 2, we briefly review the construction of the Wu et al.'s IBCUS [7] scheme. In Sect. 3, we demonstrate our known message attack and discuss the quick fix on the Wu et al. IBCUS scheme. Finally, we conclude the paper in Sect. 4.

2 Wu et al.'s IBCUS Scheme

In this section, we briefly recall Wu et al.'s IBCUS [7] scheme. We do not describe the confirmation, disavowal and conversion protocol due to page limit. Reader can refer to [7] for the full description.

Setup: On the input of security parameters k, generate groups $\mathbb{G}$ with the generator $g \in \mathbb{G}$ and $\mathbb{G}_1$ of prime order $q > 2^k$, and a pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$. Next, randomly select $s \in \mathbb{Z}_q$ as the master secret key, and compute $P_{Pub} = g^s$. Set the master public key as $mpk = (\mathbb{G}, \mathbb{G}_1, e, g, P_{pub}, H_1, H_2, H_3, H_4)$ where $H_1, H_2 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_3 : \mathbb{G} \times \mathbb{G}_1 \rightarrow \mathbb{G}$, and $H_4 : \{0,1\}^* \rightarrow \mathbb{Z}_q$.

Extract: Given the user's identity ID and the master secret key s, compute the user's private keys as $SK_{ID} = H_1(ID)^s$ and $VK_{ID} = H_1(ID, undeniable)^s$. SK_{ID} is kept secret while VK_{ID} can be published as the universal conversion token at a later time.

Sign: On the input of (SK_{ID_S}, VK_{ID_S}) and a message $m \in \{0,1\}^*$ where ID_S is the signer identity, compute $U = e(VK_{ID_S}, H_2(m)), V = g^v$ and $W = SK_{ID_S} + vH_3(U, V)$ for a randomly chosen $v \in \mathbb{Z}_q$. The undeniable signature is published as $\sigma = (U, V, W)$.

Verify: Provided a message-signature pair $(m, \sigma = (U, V, W))$, check if $e(W, P) = e(H_1(ID_S), P_{Pub})e(H_3(U, V), V)$ and reject the corrupted signature if the equality does not hold. Otherwise, decide on the validity/invalidity of the pair by checking if $U = (H_2(m), VK_{ID_S})$. If the equality holds, it means that the signature is indeed generated by the signer herself and is valid.

3 The Known Message Attack

In this section, we mount known message attacks on the invisibility and anonymity of Wu et al.'s IBCUS scheme. In precise, we construct a distinguisher $\mathcal{D}_1$ who is given a challenge tuple $(m^*, \sigma^* = (U, V, W), ID_s^*)$ which

says the message-signature pair (m^*, σ^*) may or may not be a valid signature of the random signers ID_s^*. $\mathcal{D}_1$ confirms the signature is valid if the equation $e(W, P) = e(H_1(ID_s^*), P_{Pub})e(H_3(U, V), V)$ holds. Otherwise, it is not a valid signature.

Next, we show that the anonymity of Wu et al.'s IBCUS is broken also by constructing a distinguisher $\mathcal{D}_2$ in a similar way. Provided a valid message-signature pair $(m^*, \sigma^* = (U, V, W))$ and public keys (in this case the *mpk* and identities) of two random signers ID_0^* and ID_1^*, $\mathcal{D}_2$ can decide which user has generated the signature by checking which identity (i.e. public key) satisfies the equation $e(W, P) = e(H_1(ID_b), P_{Pub})e(H_3(U, V), V)$ where $b \in \{0, 1\}$. This shows that the IBCUS completely violates the privacy that is promised to the signer.

3.1 Discussion

Although Wu et al.'s IBCUS scheme was claimed to be proven secure as the same confirmation and disavowal protocols were used in the Libert and Quisquater's provably secure IBCUS [6] scheme, the two protocols are not exactly the same. Moreover, the signing algorithm differs a lot in both schemes where the former uses two keys while the latter uses one key. Thus, it is not trivial for Wu et al.'s scheme to enjoy the security assurance from [6].

A direct yet inefficient solution is readily available for the vulnerability shown in this work. Recall that the signature is composed of three elements (U, V, W) in which U is actually the undeniable signature of Libert and Quisquater's IBCUS scheme. The elements (V, W) were added to provide a universal conversion proof but accidentally leaked information on the signing key which violates invisibility and anonymity. A workaorund is to publish (U, W) as the undeniable signature and keep V for the purpose of verification, confirmation/disavowal and conversions. However, this approach is not practical as it requires a huge storage for all signed messages and their corresponding V elements.

4 Conclusion

We mounted a known message attack on Wu et al.'s IBCUS scheme and showed that the main security properties, namely, invisibility and anonymity do not hold. This finding shows that if we extends a scheme which is provably secure, the extended scheme may not necessary inherit the provable security.

Acknowledgment. The authors would like to thank the Malaysia government's Fundamental Research Grant Scheme (FRGS/2/2014/ICT04/MMU/03/1) and (FRGS/1/2015/ICT04/MMU/03/5) for supporting this work.

References

1. Boyar, J., Chaum, D., Damgård, I., Pedersen, T.: Convertible undeniable signatures. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 189–205. Springer, Heidelberg (1991). doi:10.1007/3-540-38424-3_14

2. Chaum, D., van Antwerpen, H.: Undeniable signatures. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 212–216. Springer, New York (1990). doi:10.1007/0-387-34805-0_20
3. Chaum, D., Heijst, E., Pfitzmann, B.: Cryptographically strong undeniable signatures, unconditionally secure for the signer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 470–484. Springer, Heidelberg (1992). doi:10.1007/3-540-46766-1_38
4. Galbraith, S.D., Mao, W.: Invisibility and anonymity of undeniable and confirmer signatures. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 80–97. Springer, Heidelberg (2003). doi:10.1007/3-540-36563-X_6
5. Huang, X., Mu, Y., Susilo, W., Wu, W.: Provably secure pairing-based convertible undeniable signature with short signature length. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 367–391. Springer, Heidelberg (2007). doi:10.1007/978-3-540-73489-5_21
6. Libert, B., Quisquater, J.-J.: Identity based undeniable signatures. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 112–125. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24660-2_9
7. Wu, W., Mu, Y., Susilo, W., Huang, X.: Provably secure identity-based undeniable signatures with selective and universal convertibility. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 25–39. Springer, Heidelberg (2008). doi:10.1007/978-3-540-79499-8_4