Security-Mediated Certificateless Undeniable Signature Scheme

Tsz Hon Yuen and Swee-Huay Heng

Abstract Certificateless cryptosystems overcome the key escrow problem in identity-based cryptography. Mediated cryptography allows immediate revocation of public keys. Undeniable signatures limit the public verifiability of ordinary digital signatures. In this paper, we formalize the security models of undeniable signatures in a security-mediated certificateless setting for the first time and put forth the first example of such schemes in the literature. We also prove the security of our scheme under some well-studied assumptions in the random oracle model.

Keywords Certificateless · Undeniable signatures · Security mediated

1 Introduction

In public key infrastructure (PKI), digital certificates are used to authenticate users' public keys. However, the burden of certificate issuance and management would become costly when PKI systems are implemented in a large scale. Shamir [13] proffered identity-based cryptography to eliminate the need of certificates by using the user's identifying information (e.g., email address) as her public key. The user private key is computed by a trusted third party called the private key generator (PKG). Unfortunately, the knowledge of the PKG on the users' private keys results in a key escrow problem.

Al-Riyami and Paterson [1] proposed certificateless cryptography to overcome the key escrow problem in identity-based systems and eliminate the need of certificates in traditional public key cryptography (PKC) at the same time. This is achieved by

T. H. Yuen
Huawei Singapore, Singapore, Singapore
e-mail: yuen.tsz.hon@huawei.com

S.-H. Heng (✉)
Faculty of Information Science and Technology,
Multimedia University, Melaka, Malaysia
e-mail: shheng@mmu.edu.my

X.-S. Yang et al. (eds.), *Third International Congress on Information and Communication Technology*, Advances in Intelligent Systems and Computing 797, https://doi.org/10.1007/978-981-13-1165-9_3

computing the user's private key from two distinct secrets: secret value chosen by the user and the (identity-based) partial private key computed by a semi-trusted key generation center (KGC). The user's public key has to be computed (based on the secret value) and made publicly available.

Efficient revocation of public keys has always been a critical issue in PKC. As pointed out in [6, 12], the situation is worsened in identity-based and certificateless systems. A possible solution in such systems is to concatenate validity periods to identities and reissue new private keys (or partial private keys) at the beginning of each period. Unfortunately, this approach does not provide fine-grained revocation for environments that demand instant revocation.

Boneh et al. [3] proposed security-mediated cryptography to provide immediate revocation in a RSA-type cryptosystem. It relies on an online semi-trusted security mediator (SEM) which holds a portion of each user's private key to issue message-specific tokens. The user is unable to undergo any main cryptographic function (e.g., sign or decrypt) without acquiring the token from the SEM. Accordingly, instantaneous revocation is achieved by instructing the SEM to stop issuing tokens for revoked public keys. Ju et al. [10] proposed security-mediated certificateless (SMC) cryptography and gave an encryption and a signature scheme, without defining the security details. Chow et al. [6] defined the notion of SMC cryptography and proposed a SMC encryption with security proofs. Later, Yap et al. [14] formalized the security models of SMC signatures and proposed a novel SMC signature without pairing.

Digital signatures can be verified publicly with the knowledge of the signer's public key. However, this property may not be desirable in some situations (e.g., two business parties signing a confidential contract). Chaum and van Antwerpen [5] introduced the notion of undeniable signatures, such that the verifier can only verify the validity or invalidity of an undeniable signature with the direct help of its signer via the confirmation or disavowal protocol.

Motivation. Security-mediated cryptography is a well-known approach to effectively provide immediate public key revocation. The goal of undeniable signature schemes is to preserve the signer's privacy by limiting the public verifiability of her signatures. The notion of security-mediated undeniable signature scheme combines the aforementioned features and results in introducing new applications and recuperating the current applications of undeniable signature schemes.

The leakage of the signer's secret information in undeniable signature scheme is more catastrophic than in ordinary signatures. Not only the leakage of her secret information enables the adversary to sign new signatures (similar to the case of ordinary signatures), but it also assists the adversary to prove the validity/invalidity of her existing signatures to unauthorized parties or even convert[1] them to ordinary signatures. Aside from the well-studied features of security-mediated schemes [3, 6, 12, 14], a security-mediated undeniable signature can tackle this problem by protecting

[1] The feature of convertibility is provided by many undeniable signature schemes [4, 7–9, 11, 15] which enables the signer to convert her undeniable signatures to ordinary digital signatures to be universally verifiable.

the signer's secret information from any single point of failure since the adversary would need the cooperation of the SEM in order to sign on behalf of the signer. For example, a security-mediated undeniable signatures can enable the company to assign a trusted supervisor to work as a SEM and have control over the operation of the company's representatives. This can help to immediately revoke the public key of the representatives in the case of private key compromisation or privilege revocation. The new notion can also establish a proactive supervisory control and cogently impoverish the possible malicious intentions of a disgruntled employee.

Contribution. In this paper, we propose the first security-mediated undeniable signature scheme. We extend the security models of undeniable signatures in a SMC setting. Our scheme complies with the fundamental definitions of security-mediated cryptography [3] by preventing the signer from performing any cryptography operation (i.e., signature or proof generation) without the help of the online SEM, while hiding the SMC infrastructure from the verifiers (verifiers can verify proofs without the need to interact with the SEM). Furthermore, our scheme employs the non-interactive designated verifier proofs of [9] in the confirmation and disavowal protocols so as to prevent blackmailing and man-in-the-middle attacks. In order to enhance the efficiency for multiple signature verification, we equipped our scheme with batch verification [2] which enables the signer/verifier to generate/verify proofs on the validity or invalidity of multiple signatures at the same time in a more efficient approach. To the best of our knowledge, our scheme is the first undeniable signatures which provides batch verification in its proof generation and verification protocols. Finally, we prove the security of our scheme based on some well-known assumptions in the random oracle model.

Organization. In Sect. 2, we recall some mathematical backgrounds. In Sect. 3, we define the notion and security models of SMC undeniable signatures. In Sect. 4, we propose our concrete scheme. We provide a security analysis for our scheme in Sect. 5 and conclude our paper in Sect. 6.

2 Preliminaries

Bilinear Pairing. Let $\mathbb{G}_1$ denote an additive cyclic group of prime order q with generator P and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order. An admissible bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is given which satisfies:

1. **Bilinearity**: $\forall\ P, Q \in \mathbb{G}_1,\ \forall\ a, b \in \mathbb{Z}_q$ we have: $e(aP, bQ) = e(P, Q)^{ab}$ and $e(aP, bQ) = e(abP, Q)$.
2. **Non-degeneracy**: There exist P and $Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
3. **Computability**: e is efficiently computable.

3 Security Model of SMC Undeniable Signatures

3.1 Definition of SMC Undeniable Signatures

Our proposed notion involves three parties: the KGC, the signer, and the SEM.

- **Setup**: On input the system security parameter(s), the KGC outputs its key pair (s, P_{Pub}) where s is the master secret key and P_{Pub} is the corresponding public key. It also generates and outputs the system public parameters *params* which are shared in the system. For simplicity, we omit the inclusion of *params* as the input of the remaining algorithms.
- **Set-user-key**: On input identity ID, the user generates a secret value x_{ID} and the corresponding public key P_{ID}.
- **Register**: On input the identity ID and public key P_{ID}, the KGC computes the user's main partial private key D_{ID} (which is kept secure by the KGC), partial private key D_{ID}^{USER}, and the SEM's private key D_{ID}^{SEM}.
- **Sign**: An interactive protocol between the signer (with identity ID_A and public key P_A) and the SEM. The common input is a message m to be signed, and the private inputs are the SEM's private key D_A^{SEM} and the signer's secret value x_A and partial private key D_A^{USER}. The final output of the protocol is either $\perp$ (where the SEM refuses to cooperate) or a valid signature σ on (m, ID_A, P_A).
- **Confirmation/disavowal protocol**: A three-party protocol between the signer, the SEM, and the verifier (possibly designated). The common input is a message–signature pair (m, σ), and the private inputs are the SEM's private key D_A^{SEM} and the signer's secret value x_A and partial private key D_A^{USER}. The final output of the protocol is either $\perp$ (where the SEM refuses to cooperate) or a non-transferable proof transcript on the validity/invalidity of the message–signature pair (m, σ) for the claimed signer.

3.2 Security Models

The security model will be given in the full version of the paper due to the space limit. In short, it includes Unforgeability for three types of adversaries: Type I adversary $\mathcal{A}_I$ and Type II adversary $\mathcal{A}_{II}$ similar to the existing security model of undeniable signatures, and new insider forger $\mathcal{F}_I$ that is willing to generate signatures without the help of the SEM. As a legitimate user, $\mathcal{F}_I$ is assumed to successfully generate its secret value and public key and register itself in order to receive a valid partial private key. The notion of Invisibility means that the adversary is not able to confirm the validity/invalidity of an undeniable signature without the signer's help. The notion of Non-transferability refers to the inability of the verifier to transfer the proof of the validity or invalidity of an undeniable signature to a third party.

4 Proposed SMC Undeniable Signature Scheme

In this section, we propose our SMC undeniable signature scheme and discuss its characteristics and features.

- **Setup**: Provided the security parameters k and l, the KGC generates groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order $q \geq 2^k$, picks an arbitrary generator $P \in \mathbb{G}_1$, selects a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, and chooses five cryptographic hash functions: $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0, 1\}^* \times \{0, 1\}^l \times \{0, 1\}^* \rightarrow \mathbb{G}_1$, $H_3 : \{0, 1\}^* \times \{0, 1\}^l \times \{0, 1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{G}_1$, and $H_4, H_5 : \{0, 1\}^* \rightarrow \mathbb{Z}_q$. Next, it randomly generates its master secret key $s \in \mathbb{Z}_q$ and calculates the public key $P_{Pub} = sP$. Lastly, the KGC publishes the system public parameters as $params = (q, \mathbb{G}_1, \mathbb{G}_2, P, P_{Pub}, H_1, H_2, H_3, H_4, H_5)$.
- **Set-user-key**: On input identity ID, the user randomly chooses $x_{ID} \in \mathbb{Z}_q$ as the secret value and computes the public key $P_{ID} = x_{ID}P$.
- **Register**: Provided the user's identity ID and public key P_{ID}, the KGC authenticates the user and computes the main partial private key $D_{ID} = sQ_{ID} = sH_1(ID)$. Next, it selects the partial private key of the user $D_{ID}^{USER} \in \mathbb{G}_1$ at random and computes the SEM's private key $D_{ID}^{SEM} = D_{ID} - D_{ID}^{USER}$. Lastly, the KGC delivers D_{ID}^{USER} and D_{ID}^{SEM} to the user and the SEM in a secure manner.
- **Sign**: On input a message $m \in \{0, 1\}^*$, the signer's public key P_A, and identity ID_A, the signer Alice and the SEM work as follows.

1. Alice randomly chooses $r \in \{0, 1\}^l$, computes $O_2 = H_2(m, r, ID_A)$ and $O_3 = H_3(m, r, ID_A, P_A)$, and sends (ID_A, P_A, O_2) to the SEM.
2. The SEM first authenticates Alice and checks if ID_A has been revoked, and it rejects and outputs $\perp$. Otherwise, it computes $\mathcal{U}^{SEM} = e(O_2, D_A^{SEM})$ and sends $\mathcal{U}^{SEM}$ to Alice.
3. Alice computes $\lambda = e(O_3, x_A Q_A)e(O_2, D_A^{USER})\mathcal{U}^{SEM}$ and outputs the signature as $\sigma = (\lambda, r)$.

- **Confirmation**: Provided a valid message–signature pair $(m, \sigma = (\lambda, r))$, Alice computes a confirmation proof for a designated verifier Bob (with public key P_B and identity ID_B) as follows.

1. Alice computes and sends $O_2 = H_2(m, r, ID_A)$ to the SEM in order to request a proof on the provided message–signature pair $(m, \sigma = (\lambda, r))$. Upon receiving such request, the SEM first authenticates Alice and checks if ID_A has been revoked, and it rejects and outputs $\perp$. Otherwise, it picks $W^{SEM} \in \mathbb{G}_1$ at random, computes $k_1^{SEM} = e(P, W^{SEM})$ and $k_2^{SEM} = e(O_2, W^{SEM})$, and sends (k_1^{SEM}, k_2^{SEM}) to Alice.
2. Next, Alice computes $Q_B = H_1(ID_B)$ and $O_3 = H_3(m, r, ID_A, P_A)$ and picks $U, W^{USER} \in \mathbb{G}_1$ and $\beta, \tau, v \in \mathbb{Z}_q$ at random to calculate:

$$\begin{aligned} n_1 &= e(P_{Pub}, Q_B)^v e(P, U), \; n_2 = vP_B + \tau P, \\ g_1 &= e(P, W^{USER})k_1^{SEM}, \quad g_2 = e(P, P)^{\beta}, \\ g_3 &= e(O_3, Q_A)^{\beta} e(O_2, W^{USER})k_2^{SEM}. \end{aligned}$$

She then sets $h_C = H_4(n_1, n_2, g_1, g_2, g_3, \sigma)$ and $h = (h_C + v)$ and sends h to the SEM.

3. Upon receiving h, the SEM computes $R^{SEM} = W^{SEM} - hD_A^{SEM}$ and sends R^{SEM} to Alice.
4. Lastly, Alice sets the values of $b = \beta - (h_C + \nu)x_A$, $R^{USER} = W^{USER} - (h_C + \nu)D_A^{USER}$, and $R = R^{USER} + R^{SEM}$ and sends the confirmation proof transcript as (U, v, τ, b, R, h_C).

Upon receiving (U, v, τ, b, R, h_C), the designated verifier Bob sets $O_2 = H_2(m, r, ID_A)$ and $O_3 = H_3(m, r, ID_A, P_A)$ and computes the following:

$$\begin{aligned}
&n_1^{'} = e(P_{Pub}, Q_B)^v e(P, U), \quad n_2^{'} = vP_B + \tau P,\\
&g_1^{'} = e(P, R)e(P_{Pub}, Q_A)^{(h_C+v)}, \quad g_2^{'} = e(P, P)^b e(P, P_A)^{(h_C+v)},\\
&g_3^{'} = e(O_3, Q_A)^b e(O_2, R)\lambda^{(h_C+v)}.
\end{aligned}$$

Bob accepts the proof if $h_C = H_4(n_1^{'}, n_2^{'}, g_1^{'}, g_2^{'}, g_3^{'}, \sigma)$ or rejects it otherwise.

- **Disavowal**: Provided an invalid message–signature pair $(m, \sigma = (\lambda, r))$, Alice generates a disavowal proof for a designated verifier Bob as follows.

1. Alice first parses σ into (λ, r) and computes $Q_B = H_1(ID_B)$, $O_2 = H_2(m, r, ID_A)$, and $O_3 = H_3(m, r, ID_A, P_A)$. Then, she picks $U \in \mathbb{G}_1$ and $\tau, v \in \mathbb{Z}_q$ at random in order to compute the values of $n_1 = e(P_{Pub}, Q_B)^v e(P, U)$ and $n_2 = vP_B + \tau P$. Next, she passes O_2 to the SEM in order to request for a partial signature.
2. The SEM first authenticates Alice and checks if ID_A has been revoked, and it rejects and outputs $\perp$. Otherwise, it computes $\mathcal{U}^{SEM} = e(O_2, D_A^{SEM})$ and sends $\mathcal{U}^{SEM}$ to Alice.
3. Alice picks $\omega \in \mathbb{Z}_q$ and computes $C = (\frac{e(O_3, x_A Q_A)e(O_2, D_A^{USER})\mathcal{U}^{SEM}}{\lambda})^{\omega}$. She proves the knowledge of a tuple $(T, \mu, \alpha) \in \mathbb{G}_1 \times \mathbb{Z}_q \times \mathbb{Z}_q$ where $C = \frac{e(O_3, \mu Q_A)e(O_2, T)}{\lambda^{\alpha}}$, $\frac{e(P, T)}{e(Q_A, P_{Pub})^{\alpha}} = 1$ and $\frac{\alpha P_A}{\mu P} = 1$.

   (a) Again, she sends O_2 to the SEM to request for a proof. The SEM picks $X^{SEM} \in \mathbb{G}_1$ at random, computes $z_1^{SEM} = e(P, X^{SEM})$ and $z_2^{SEM} = e(O_2, X^{SEM})$, and sends (z_1^{SEM}, z_2^{SEM}) to Alice.

   (b) Next, Alice picks $X^{USER} \in \mathbb{G}_1$ and $a, i \in \mathbb{Z}_q$ at random and computes:

$$\begin{aligned}
j_1 &= \frac{e(P, X^{USER})z_1^{SEM}}{e(Q_A, P_{Pub})^a}, \quad j_2 = \frac{e(P, P)^i}{e(P, P_A)^a},\\
j_3 &= \frac{e(O_3, Q_A)^i e(O_2, X^{USER})z_2^{SEM}}{\lambda^a}
\end{aligned}$$

   She then sets $h_D = H_5(C, n_1, n_2, j_1, j_2, j_3, \sigma)$ and $h = \alpha(h_D + v)$ and sends h to the SEM.

   (c) Upon receiving h, the SEM computes $Y^{SEM} = X^{SEM} - hD_A^{SEM}$ and sends Y^{SEM} to Alice.

(d) Lastly, Alice sets the values of $w_1 = i - (h_D + v)\mu$, $w_2 = a - (h_D + v)\alpha$, $Y^{USER} = X^{USER} - (h_D + v)\alpha D_A^{USER}$, and $Y = Y^{USER} + Y^{SEM}$. She outputs the proof transcript: $(C, U, \tau, v, h_D, Y, w_1, w_2)$.

4. Upon receiving $(C, U, \tau, v, h_D, Y, w_1, w_2)$, Bob first checks if $C = 1$, he rejects and outputs $\perp$. Otherwise, he calculates $O_2 = H_2(m, r, ID_A)$ and $O_3 = H_3(m, r, ID_A, P_A)$ and verifies the proof by computing the following:

$$n_1^{'} = e(P_{Pub}, Q_B)^v e(P, U), \quad n_2^{'} = vP_B + \tau P,$$
$$j_1^{'} = \frac{e(P, Y)}{e(Q_A, P_{Pub})^{w_2}}, \quad j_2^{'} = \frac{e(P, P)^{w_1}}{e(P, P_A)^{w_2}},$$
$$j_3^{'} = \frac{e(O_3, Q_A)^{w_1} e(O_2, Y)}{\lambda^{w_2}} C^{(h_D+v)}$$

Bob accepts the proof if $h_D = H_5(C, n_1^{'}, n_2^{'}, j_1^{'}, j_2^{'}, j_3^{'}, \sigma)$ or rejects it otherwise.

Characteristics and Features. The feature of batch verification and convertibility will be given in the full version of the paper.

5 Security Analysis

In the full version of the paper, we show that our scheme is secure (both unforgeable and invisible) against the aforementioned adversary types (Type I/II adversary and insider forger) in the random oracle model, given the hardness of some well-known complexity assumptions.

6 Conclusion

We proposed the first security-mediated undeniable signature scheme. We also formalized the security models of such schemes in a certificateless setting for the first time. We provided a formal security proof for our scheme in the random oracle model so as to rely its security on the intractability of the BDH and the DBDH assumptions. As a result, our construction allows the design of undeniable signature scheme in a SMC setting. The direction for future research would be to propose SMC schemes which are more efficient and require less pairing evaluations while satisfying all the security requirements.

Acknowledgements The authors wish to acknowledge the Malaysia government's Fundamental Research Grant Scheme (FRGS/1/2015/ICT04/MMU/03/5) for supporting this work.

References

1. Al-Riyami S, Paterson K (2003) Certificateless public key cryptography. In: Laih C-S (ed) Advances in cryptology-ASIACRYPT, vol 2894. Lecture notes in computer science. Springer, Berlin, pp 452–473
2. Bellare M, Garay J, Rabin T (1998) Fast batch verification for modular exponentiation and digital signatures. In: Nyberg K (ed) Advances in cryptology-EUROCRYPT 98, vol 1403. Lecture notes in computer science. Springer, Berlin, pp 236–250
3. Boneh D, Ding X, Tsudik G, Wong CM (2001) A method for fast revocation of public key certificates and security capabilities. In: Proceedings of the 10th conference on USENIX security symposium, vol 10
4. Boyar J, Chaum D, Damgård I, Pedersen T (1991) Convertible undeniable signatures. In: Menezes A, Vanstone S (eds) Advances in cryptology-CRYPTO, vol 537. Lecture notes in computer science. Springer, Berlin, pp 189–205
5. Chaum D, van Antwerpen H (1989) Undeniable signatures. In: Brassard G (ed) Advances in cryptology-CRYPTO, vol 435. Lecture notes in computer science. Springer, Berlin, pp 212–216
6. Chow S, Boyd C, Nieto JG (2006) Security-mediated certificateless cryptography. In: Yung M, Dodis Y, Kiayias A, Malkin T (eds) Lecture notes in computer science, vol 2894. Public key cryptography-PKC 2006, volume 3958 (Lecture notes in computer science). Springer, Berlin, pp 508–524
7. Huang Q, Wong DS (2013) Short and efficient convertible undeniable signature schemes without random oracles. Theor Comput Sci 476:67–83
8. Huang X, Mu Y, Susilo W, Wu W (2007) Provably secure pairing-based convertible undeniable signature with short signature length. In: Takagi T, Okamoto T, Okamoto E, Okamoto T (eds) Pairing-based cryptography, vol 4575. Lecture notes in computer science. Springer, Berlin, pp 367–391
9. Jakobsson M, Sako K, Impagliazzo R (1996) Designated verifier proofs and their applications. In: Maurer U (ed) Advances in cryptology-EUROCRYPT, vol 1070. Lecture notes in computer science. Springer, Berlin, pp 143–154
10. Ju H, Kim D, Lee D, Lim J, Chun K (2005) Efficient revocation of security capability in certificateless public key cryptography. In: Khosla R, Howlett R, Jain L (eds) Lecture notes in computer science, vol 2894. Knowledge-based intelligent information and engineering systems, volume 3682 of Lecture notes in computer science. Springer, Berlin, pp 453–459
11. Laguillaumie F, Vergnaud D (2005) Time-selective convertible undeniable signatures. In: Menezes A (ed) Lecture notes in computer science, vol 3376. Topics in cryptology-CT-RSA. Lecture notes in computer science. Springer, Berlin, pp 154–171
12. Libert B, Quisquater J-J (2003) Efficient revocation and threshold pairing based cryptosystems. In: Proceedings of the twenty-second annual symposium on principles of distributed computing, PODC ’03. ACM, New York, pp 163–171
13. Shamir A (1985) Identity-based cryptosystems and signature schemes. In: Blakley G, Chaum D (eds) Advances in cryptology-CRYPTO, vol 196. Lecture notes in computer science. Springer, Berlin, pp 47–53
14. Yap W-S, Chow S, Heng S-H, Goi B-M (2007) Security mediated certificateless signatures. In: Katz J, Yung M (eds) Lecture notes in computer science, vol 2894. Applied cryptography and network security, volume 4521 of Lecture notes in computer science. Springer, Berlin, pp 459–477
15. Yuen TH, Au MH, Liu JK, Susilo W (2007) (Convertible) undeniable signatures without random oracles. In: Qing S, Imai H, Wang G (eds) Information and communications security, 9th international conference, ICICS 2007, vol 4861. Lecture notes in computer science. Springer, Berlin, pp 83–97