Provably Secure and Subliminal-Free Variant of Schnorr Signature

Yinghui Zhang, Hui Li, Xiaoqing Li, Hui Zhu

Provably Secure and Subliminal-Free Variant of Schnorr Signature

Yinghui Zhang[1,*], Hui Li[1], Xiaoqing Li[1], Hui Zhu[1,2]

[1] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, P.R. China
[2] Network and Data Security Key Laboratory of Sichuan Province, Chengdu 611731, P.R. China
*Corresponding author: yhzhaang@163.com

Abstract. Subliminal channels present a severe challenge to information security. Currently, subliminal channels still exist in Schnorr signature. In this paper, we propose a subliminal-free variant of Schnorr signature. In the proposed scheme, an *honest-but-curious* warden is introduced to help the signer to generate a signature on a given message, but it is disallowed to sign messages independently. Hence, the signing rights of the signer is guaranteed. In particular, our scheme can completely close the subliminal channels existing in the random session keys of Schnorr signature scheme under the intractability assumption of the discrete logarithm problem. Also, the proposed scheme is proved to be existentially unforgeable under the computational Diffie-Hellman assumption in the random oracle model.

Keywords: Digital signature; Information hiding; Subliminal channel; Subliminal-freeness; Provable security

1 Introduction

The notion of subliminal channels was introduced by Simmons [1]. He proposed a prison model in which authenticated messages are transmitted between two prisoners and known to a warden. The term of "subliminal" means that the sender can hide a message in the authentication scheme, and the warden cannot detect or read the hidden message. Simmons discovered that a secret message can be hidden inside the authentication scheme and he called this "hidden" communication channel as the subliminal channel. The "hidden" information is known as subliminal information.

As a main part of information hiding techniques [2–6], subliminal channels have been widely studied and applied [7–12]. However, they also present a severe challenge to information security. To the best of our knowledge, subliminal channels still exist in Schnorr signature [13].

Our Contribution. In this paper, we propose a subliminal-free variant of Schnorr signature scheme, in which an *honest-but-curious* warden is introduced to help the signer to generate a signature on a given message, but it is disallowed to sign messages independently. In addition, the signer cannot control outputs of the signature algorithm. To be specific, the sender has to cooperate with the warden to sign a given message. Particularly, our scheme is provably secure and can completely close the subliminal channels existing in the random session keys in Schnorr signature scheme.

Related Work. Plenty of researches have been done on both the construction of subliminal channels and the design of subliminal-free protocols [7–11, 14–17]. Since the introduction of subliminal channels, Simmons [18] also presented several narrow-band subliminal channels that do not require the receiver to share the sender's secret key. Subsequently, Simmons [15] proposed a broad-band subliminal channel that requires the receiver to share the sender's secret key. For the purpose of information security, Simmons then proposed a protocol [19] to close the subliminal channels in the DSA digital signature scheme. However, Desmedt [14] showed that the subliminal channels in the DSA signature scheme cannot be completely closed using the protocol in [19]. Accordingly, Simmons adopted the cut-and-choose method to reduce the capacity of the subliminal channels in the DSA digital signature algorithm [20]. However, the complete subliminal-freeness still has not been realized. To be specific, the computation and communication costs significantly increase with the reduction of the subliminal capacity. On the other hand, subliminal channels in the NTRU cryptosystem and the corresponding subliminal-free methods [21] were proposed. Also, a subliminal channel based on the elliptic curve cryptosystem was constructed [8, 17]. As far as the authors know, the latest research is mainly concentrated on the construction [10, 11, 16] of subliminal channels and their applications [7, 12, 22, 23].

Outline of the Paper. The rest of this paper is organized as follows. In Section 2, we introduce some notations and complexity assumptions, and then discuss subliminal channels in probabilistic digital signature. In Section 3, we lay out the abstract subliminal-free signature specification and give the formal security model. The proposed provably secure and subliminal-free variant of Schnorr signature scheme is described in Section

4. Some security considerations are discussed in Section 5. Finally, we concludes the work in Section 6.

2 Preliminaries

2.1 Notations

Throughout this paper, we use the notations, listed in Table 1, to present our construction.

Table 1. Meaning of notations in the proposed scheme

Notation	Meaning
$s \in_R \mathbb{S}$	s is an element randomly chosen from a set $\mathbb{S}$.
l_s	the bit length of the binary representation of s.
$s_1 \parallel s_2$	the concatenation of bit strings s_1 and s_2.
$\gcd(a, b)$	the greatest common divisor of two integers a and b.
x^{-1}	the modular inverse of x modulo q such that $x^{-1}x = 1 \mod q$, where x and q are relatively prime, *i.e.*, $\gcd(x, q) = 1$.
$\mathbb{G}_{g,p}$	a cyclic group with order q and a generator g, where q is a large prime factor of $p-1$ and p is a large prime. That is, $\mathbb{G}_{g,p} = \{g^0, g^1, \cdots, g^{q-1}\} =< g >$, which is a subgroup in the multiplicative group $GF^*(p)$ of the finite field $GF(p)$.

2.2 Complexity Assumptions

Discrete Logarithm Problem (DLP): Let $\mathbb{G}$ be a group, given two elements g and h, to find an integer x, such that $h = g^x$ whenever such an integer exists.
Intractability Assumption of DLP: In group $\mathbb{G}$, it is computationally infeasible to determine x from g and h.
Computation Diffie-Hellman (CDH) Problem: Given a 3-tuple $(g, g^a, g^b) \in \mathbb{G}^3$, compute $g^{ab} \in \mathbb{G}$. An algorithm $\mathcal{A}$ is said to have advantage ϵ in solving the CDH problem in $\mathbb{G}$ if

$$\Pr\left[\mathcal{A}(g, g^a, g^b) = g^{ab}\right] \geq \epsilon,$$

where the probability is over the random choice of g in $\mathbb{G}$, the random choice of a, b in $\mathbb{Z}_q^*$, and the random bits used by $\mathcal{A}$.
CDH Assumption: We say that the (t, ϵ)-CDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the CDH problem in $\mathbb{G}$.

2.3 Subliminal Channels in Probabilistic Digital Signature

Probabilistic digital signature [25] can serve as the host of subliminal channels. In fact, the subliminal sender can embed some information into a subliminal channel by controlling the generation of the session keys. After verifying a given signature, the subliminal receiver uses an extraction algorithm to extract the embedded information. Note that the extraction algorithm is only possessed by the authorized subliminal receiver. Hence, anyone else cannot learn whether there exists subliminal information in the signature [26], not to mention extraction of the embedded information.

In a probabilistic digital signature scheme, the session key can be chosen randomly, and hence one message may correspond to several signatures. More specifically, if different session keys are used to sign the same message, different digital signatures can be generated. This means that redundant information exists in probabilistic digital signature schemes, which creates a condition for subliminal channels. The subliminal receiver can use these different digital signatures to obtain the subliminal information whose existence can hardly be learnt by the others.

In particular, there exists subliminal channels in a typical probabilistic digital signature, namely Schnorr Signature [13].

3 Definition and Security Model

3.1 Specification of Subliminal-Free Signature

A subliminal-free signature scheme consists of three polynomial-time algorithms **Setup**, **KeyGen**, an interactive protocol **Subliminal-Free Sign**, and **Verify** below. Based on a subliminal-free signature scheme, a sender A performs an interactive protocol with a warden W. And, W generates the final signature σ and transmits it to a receiver B. Note that W is *honest-but-curious*. That is, W will honestly execute the tasks assigned by the related algorithm. However, it would like to learn secret information as much as possible.

- **Setup:** It takes as input a security parameter λ and outputs system public parameters $Params$.
- **KeyGen:** It takes as input a security parameter λ, system public parameters $Params$ and returns a signing-verification key pair (sk, pk).
- **Subliminal-Free Sign:** An interactive protocol between the sender and the warden. Given a message M, a signature σ is returned.

– **Verify:** It takes as input system public parameters $Params$, a public key pk and a signature message (M, σ). It returns 1 if and only if σ is a valid signature on message M.

3.2 Security Model

In the proposed scheme, the warden participates in the generation of a signature, hence the ability of the warden to forge a signature is enhanced. We regard the warden as the adversary. The formal definition of existential unforgeability against adaptively chosen messages attacks (EUF-CMA) is based on the following EUF-CMA game involving a simulator $\mathcal{S}$ and a forger $\mathcal{F}$:

1. **Setup:** $\mathcal{S}$ takes as input a security parameter λ, and runs the Setup algorithm. It sends the public parameters to $\mathcal{F}$.
2. **Query:** In addition to hash queries, $\mathcal{F}$ issues a polynomially bounded number of queries to the following oracles:
   – *Key generation oracle* $\mathcal{O}_{KeyGen}$: Upon receiving a key generation request, $\mathcal{S}$ returns a signing key.
   – *Signing oracle* $\mathcal{O}_{Sign}$: $\mathcal{F}$ submits a message M, and $\mathcal{S}$ gives $\mathcal{F}$ a signature σ.
3. **Forgery:** Finally, $\mathcal{F}$ attempts to output a valid forgery (M, σ) on some new message M, *i.e.*, a message on which F has not requested a signature. $\mathcal{F}$ wins the game if σ is valid.

The advantage of $\mathcal{F}$ in the EUF-CMA game, denoted by $\mathsf{Adv}(\mathcal{F})$, is defined as the probability that it wins.

Definition 1. (Existential Unforgeability) *A probabilistic algorithm $\mathcal{F}$ is said to (t, q_H, q_S, ϵ)-break a subliminal-free signature scheme if $\mathcal{F}$ achieves the advantage $\mathsf{Adv}(\mathcal{F}) \geq \epsilon$, when running in at most t steps, making at most q_H adaptive queries to the hash function oracle H, and requesting signatures on at most q_S adaptively chosen messages. A subliminal-free signature scheme is said to be (t, q_H, q_S, ϵ)-secure if no forger can (t, q_H, q_S, ϵ)-break it.*

4 Subliminal-Free Variant of Schnorr Signature

4.1 Construction

– **Setup:** Let (p, q, g) be a discrete logarithm triple associated with group $\mathbb{G}_{g,p}$. Let A be the sender of message $M \subseteq \{0,1\}^*$, B be the receiver of M and W be the warden. It chooses $t \in_R (1, q)$, returns t to W and computes $T = g^t \mod p$. Also, let H_0, H be two hash functions, where $H_0 : \{0,1\}^* \to \mathbb{G}_{g,p}$ and $H : \{0,1\}^* \times \mathbb{G}_{g,p} \to (1, q)$. Then, the public parameters are $Params = (p, q, g, H_0, H, T)$.

- **KeyGen:** It returns $x \in_R (1, q)$ as a secret key and the corresponding public key is $y = T^x \mod p$.
- **Subliminal-Free Sign**:
  1. W chooses two secret large integers c and d satisfying $cd = 1 \mod q$. Also, W chooses $k_w \in_R (1, q)$, thus $\gcd(k_w, q) = 1$. Then W computes $\alpha = g^{k_w c} \mod p$ and sends α to A.
  2. A chooses $k_a \in_R (1, q)$, thus $\gcd(k_a, q) = 1$. Then A computes $h_0 = H_0(M)$, $\beta = \alpha^{k_a h_0} \mod p$ and sends (h_0, β) to W.
  3. W computes $r = \beta^d = \alpha^{k_a h_0 d} = g^{k_a k_w h_0 cd} = g^{k_a k_w h_0} \mod p$, $v_1 = y^{k_w^{-1}} \mod p$, and sends (r, v_1) to A.
  4. A computes $e = H(M \parallel r)$, $f = e^x \mod p$ and $v_2 = g^{k_a h_0} \mod p$. Then A prepares a non-interactive zero knowledge proof that $DL_e(f) = DL_T(y)$ and sends (e, f, v_2) to W.
  5. W computes $u = k_w v_1^{-1} f^{-1} v_2^{-1} \mod p$, $\theta = u^{-1} t \mod p$ and sends θ to A.
  6. A computes s' and then sends (M, s') to W:

$$\begin{aligned} s' &= k_a h_0 + \theta \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \\ &= k_a h_0 + (u^{-1} t) \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \\ &= k_a h_0 + (v_2 f v_1 k_w^{-1} t) \cdot (v_1^{-1} f^{-1} v_2^{-1}) \cdot xe \\ &= k_a H_0(M) + k_w^{-1} xte \mod q. \end{aligned}$$

  7. *Sign:* Upon receiving (M, s'), W checks if $h_0 = H_0(M)$ and $e = H(M \parallel r)$. If not, W terminates the protocol, else W computes

$$s = k_w s' = k_a k_w H_0(M) + k_w k_w^{-1} xte = k_a k_w H_0(M) + xte \mod q.$$

  Then W sends the signature message $(M, (e, s))$ to B.
- **Verify**: After receiving the signature message $(M, (e, s))$, B computes

$$r' = g^s y^{-e} \mod p$$

and $e' = H(M \parallel r')$. B returns 1 if and only if $e = e'$.

4.2 Consistency of Our Construction

On one hand, if the signature message $(M, (e, s))$ is valid, we have $s = k_a k_w H_0(M) + xte \mod q$. Thus,

$$\begin{aligned} r' = g^s y^{-e} &= g^{k_a k_w H_0(M) + xte \mod q} y^{-e} \\ &= g^{k_a k_w H_0(M)} T^{xe} y^{-e} \\ &= g^{k_a k_w H_0(M)} y^e y^{-e} \\ &= g^{k_a k_w H_0(M)} \\ &= r \mod p, \end{aligned}$$

and then $e' = H(M \parallel r') = H(M \parallel r) = e$.

On the other hand, if $e = e'$, the signature message $(M, (e, s))$ is valid. Otherwise, we have

$$s \neq k_a k_w H_0(M) + xte \mod q$$

and then $r' \neq r$. However,

$$e' = H(M \parallel r') = H(M \parallel r) = e.$$

Thus, a collision of the hash function H is obtained, which is infeasible for a secure hash function.

5 Analysis of the Proposed Subliminal-Free Signature Scheme

5.1 Existential Unforgeability

Theorem 1. *If $\mathbb{G}_{g,p}$ is a (t', ϵ')-CDH group, then the proposed scheme is $(t, q_{H_0}, q_H,\ q_S, \epsilon)$-secure against existential forgery on adaptively chosen messages in the random oracle model, where*

$$t \geq t' - (q_H + 3.2 q_S) \cdot C_{Exp}, \tag{1}$$

$$\epsilon \leq \epsilon' + q_S \cdot (q_{H_0} + q_S) 2^{-l_M} + q_S(q_H + q_S) 2^{-l_r} + q_H 2^{-l_q}, \tag{2}$$

where C_{Exp} denotes the cost of a modular exponentiation in group $\mathbb{G}_{g,p}$.

Proof. (sketch) Let $\mathcal{F}$ be a forger that $(t, q_{H_0}, q_H, q_S, \epsilon)$-breaks our proposed scheme. We construct a "simulator" algorithm $\mathcal{S}$ which takes $((p, q, g), (g^a, g^b))$ as inputs and runs $\mathcal{F}$ as a subroutine to compute the function $DH_{g,p}(g^a, g^b) = g^{ab}$ in t' steps with probability ϵ', which satisfy the Equalities (1) and (2). $\mathcal{S}$ makes the signer's verification key $y = g^a \mod p$

public, where the signing key a is unknown to $\mathcal{S}$. Aiming to translate $\mathcal{F}$'s possible forgery $(M, (e, s))$ into an answer to the function $DH_{g,p}(g^a, g^b)$, $\mathcal{S}$ simulates a running of the proposed scheme and answers $\mathcal{F}$'s queries. S uses $\mathcal{F}$ as a subroutine. Due to space limitation, we don't present the details here. ■

5.2 Subliminal-Freeness

It can be seen from the proposed scheme that the receiver B can only obtain the signature message $(M, (e, s))$ and temporary value r in addition to the verification public key y, thus it is necessary for the sender A to use e, s or r as a carrier when transmitting subliminal information.

In the following, we demonstrate that none of e, s and r can be controlled by A. On one hand, although the parameters $(\alpha, v_1, \theta) = (g^{k_w c}, y^{k_w^{-1}}, u^{-1}t) \mod p$ can be obtained by A, the secret exponents c, d and the secret parameters t, u are unknowable to him. Thus, A cannot obtain any information about k_w and g^{k_w}. Particularly, A knows nothing of k_w and g^{k_w} in the whole process of signing, hence the value of $s = k_w s' \mod p$ cannot be controlled by A. On the other hand, although the signer A computes $e = H(M \parallel r)$, nothing of k_w and g^{k_w} is available to him. Thus, the value of $r = g^{k_a k_w H_0(M)} \mod p$ cannot be controlled by A, and hence the value of e cannot be controlled. Note that if the value r generated by the warden W is not used by A in the Step 4, W can detect this fact in the Step 7 and terminate the protocol. Furthermore, if A attempts to directly compute k_w from g^{k_w}, he has to solve the discrete logarithm problem in group $GF^*(p)$, which is infeasible according to the intractability assumption of DLP.

Hence, we realize the complete subliminal-freeness of the subliminal channels existing in the random session keys in Schnorr signature scheme.

6 Conclusions and Future work

In this paper, a subliminal-free protocol for Schnorr signature scheme is proposed. The proposed protocol completely closes the subliminal channels existing in the random session keys in Schnorr signature scheme. More strictly, it is completely subliminal-free in computational sense, and its security relies on the CDH assumption in the random oracle model. In addition, it is indispensable for the sender and the warden to cooperate with each other to sign a given message, and the warden is *honest-but-curious* and cannot forge a signature independently.

It would be interesting to construct subliminal-free signature schemes provably secure in the standard model.

Acknowledgements

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by the National Natural Science Foundation of China (No.61272457), the Nature Science Basic Research Plan in Shaanxi Province of China (No.2011JQ8042), and the Fundamental Research Funds for the Central Universities (Nos.K50511010001 and K5051201011). In particular, this work is supported by the Graduate Student Innovation Fund of Xidian University (Research on key security technologies of large-scale data sharing in cloud computing).

References

1. Gustavus J. Simmons. The prisoner' problem and the subliminal channel. In *Advances in Cryptology-Crypto 1983*, pages 51–67. Plenum Press, 1984.
2. Preeti Gupta. Cryptography based digital image watermarking algorithm to increase security of watermark data. *International Journal of Scientific & Engineering Research*, 3(9):1–4, 2012.
3. George Danezis, Markulf Kohlweiss, and Alfredo Rial. Differentially private billing with rebates. *Information Hiding*, volume 6958 of *Lecture Notes in Computer Science*, pages 148–162. Springer Berlin Heidelberg, 2011.
4. William R. Claycomb, Carly L. Huth, Lori Flynn, David M. McIntire, and Todd B. Lewellen. Chronological examination of insider threat sabotage: preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(4): 4–20, 2012.
5. Byungha Choi and Kyungsan Cho. Detection of insider attacks to the web server. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(4): 35–45, 2012.
6. Kangwon Lee, Kyungroul Lee, Jaecheon Byun, Sunghoon Lee, Hyobeom Ahn and Kangbin Yim. Extraction of platform-unique information as an identifier. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(4): 85–99, 2012.
7. Chin-Ling Chen and Jyun-Jie Liao. A fair online payment system for digital content via subliminal channel. *Electronic Commerce Research and Applications*, 10(3):279–287, 2011.
8. Xuanwu Zhou, Xiaoyuan Yang, Ping Wei, and Yupu Hu. An anonymous threshold subliminal channel scheme based on elliptic curves cryptosystem. In *Computer-Aided Industrial Design and Conceptual Design, CAIDCD '06*, pages 1–5, nov. 2006.
9. K. Kim F. Zhang, B. Lee. Exploring signature schemes with subliminal channel. In *Symposium on Cryptography and Information Security'03*, pages 245–250, 2003.
10. Tzonelih Hwang Chao-Lin Yang, Chuan-Ming Li. Subliminal channels in the identity-based threshold ring signature. *International Journal of Computer Mathematics*, 86(5):753–770, 2009.

11. Dai-Rui Lin, Chih-I Wang, Zhi-Kai Zhang, and D.J. Guan. A digital signature with multiple subliminal channels and its applications. *Computers & Mathematics with Applications*, 60(2):276–284, 2010. Advances in Cryptography, Security and Applications for Future Computer Science.
12. C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel. Pripayd: Privacy-friendly pay-as-you-drive insurance. *IEEE Transactions on Dependable and Secure Computing,* 8(5):742–755, 2011.
13. C.P. Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *Advances in Cryptology-CRYPTO'89*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer New York, 1990.
14. Y. Desmedt. Simmons' protocol is not free of subliminal channels. In *Proceedings of 9th IEEE Computer Security Foundations Workshop, 1996*, pages 170–175, 1996.
15. Gustavus J. Simmons. Subliminal communication is easy using the dsa. In Tor Helleseth, editor, *Advances in Cryptology-EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 218–232. Springer Berlin Heidelberg, 1994.
16. Xin Xiangjun and Li Qingbo. Construction of subliminal channel in id-based signatures. In *WASE International Conference on Information Engineering, 2009. ICIE'09.* , volume 2, pages 159–162, 2009.
17. Yuhua Xie, Xingming Sun, Lingyun Xiang, and Gang Luo. A security threshold subliminal channel based on elliptic curve cryptosystem. In *Processing of IIHMSP '08 International Conference on Intelligent Information Hiding and Multimedia Signal 2008*, pages 294–297, 2008.
18. Gustavus J. Simmons. The subliminal channels of the us digital signature algorithm (DSA). In *Advances in Cryptology-Cryptography-SPRC'93*, pages 15–16, 1993.
19. Gustavus J. Simmons. An introduction to the mathematics of trust in security protocols. In *Proceedings of Computer Security Foundations Workshop VI, 1993*, pages 121–127, jun 1993.
20. Gustavus J. Simmons. Results concerning the bandwidth of subliminal channels. *Selected Areas in Communications, IEEE Journal on*, 16(4):463–473, 1998.
21. Cai Qingjun and Zhang Yuli. Subliminal channels in the NTRU and the subliminal-free methods. *Wuhan University Journal of Natural Sciences*, 11:1541–1544, 2006.
22. Ying Sun, Chunxiang Xu, Yong Yu, and Bo Yang. Improvement of a proxy multi-signature scheme without random oracles. *Computer Communications*, 34(3):257–263, 2011. Special Issue of Computer Communications on Information and Future Communication Security.
23. M. V. Jadhav. Effective detection mechanism for tcp based hybrid covert channels in secure communication. In *2011 International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT)*, pages 1123–1128, 2011.
24. Naoto Yanai, Raylin Tso, Masahiro Mambo, and Eiji Okamoto. A certificateless ordered sequential aggregate signature scheme secure against super adverssaries. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(1): 30–54, 2012.
25. Naoto Yanai, Raylin Tso, Masahiro Mambo, and Eiji Okamoto. A certificateless ordered sequential aggregate signature scheme secure against super adverssaries. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(1): 30–54, 2012.
26. Gustavus J. Simmons. Subliminal channels: past and present. *European Transactions on Telecommunications*, 5(4):459–474, 1994.