Practical Secret Signature Scheme with No Randomness Saving

Byoungcheon Lee
Dept. of Information Security, Joongbu University
101, Daehak-Ro, Chubu-Myeon, Geumsan-Gun, Chungnam, Korea
sultan@joongbu.ac.kr

***Abstract*—Secret signatures, proposed by Lee *et al.* [5], [6], provide signature privacy and public provability at the same time. Using these schemes a signer can send his signature secretly to a designated receiver such that only the designated receiver can verify the signature. Moreover, if any argument occurs between them, the validity of the secret signature can be proven publicly either by the signer or the receiver. But in these schemes one of the drawback is that the signer has to keep the random number used in the signing algorithm for later use, i.e., to provide public provability. This is very impractical in the real world, since random numbers used in many cryptographic algorithms are generally used only once and they have to be removed safely for security reason.**

In this paper we amend Lee *et al.*'s secret signature scheme such that random number is replaced by a pseudo random number that can be computed only by the signer as a function of signer's private key and timestamp. With this change signer can compute the pseudo random number at any later time that he doesn't need to save it anymore, and it can be computed only by the signer. With this change we think that secret signature scheme becomes more practical and can be used as an important cryptographic primitive to achieve signature privacy in the real world.

***Keywords*-Secret signature; Signature privacy; Public provability; Randomness saving**

I. Introduction

The concept of secret signature was first introduced by Lee *et al.* in [5], [6]. In secret signature schemes signer computes a one way secret key agreement with a designated receiver and signs a message and the agreed key together, then the secret signature can be verified only by the designated receiver who can recover the secret agreed key. Signature privacy is provided since anyone except the signer and the designated receiver cannot compute the key agreement and therefore cannot verify the signature. Public provability means that the signer or the designated receiver can prove the validity of secret signature to others when there are some argument between them. It is a good combination of digital signature and key agreement technology to provide signature privacy and public provability at the same time.

Secret signature was proposed to provide signature privacy more efficiently. Consider a business scenario where both the sender (signer) and the receiver (verifier) wish to keep their exchanged signatures private. A "straightforward" approach to achieve signature privacy is to encrypt a digital signature with the receiver's public key so that only the legitimate receiver can decrypt and retrieve the original signature. This is the so-called sign-then-encrypt approach, which is widely adopted in the real world. In order to implement the signature and encryption operations in more efficient manner, signcryption [7] was proposed in 1997 by Zheng. Alternative solutions to achieve signature privacy by limiting the verifiability of the signature only to a designated entity incluse the designated verifier signature (DVS) [4] and the limited verifier signature (LVS) [1], [2]). As shown in [5] secret signature scheme provides signature privacy more efficiently than signcryption scheme.

Secret signature can be a very useful primitive to achieve business privacy in more efficient way, but in its current form it is hard to be applied in the real world. Since the random number used in the signing stage is needed in public proving stage by the signer, signer has to save it somewhere in his computer system securely. In our general security practice this kind of temporal random numbers used in signing stage have to be erased quickly and safely. Once it is exposed to others, signer's private key can be computed from the signature. Therefore, this kind of randomness saving in signature schemes cannot be used in the real world.

In this paper we modify the secret signature scheme such that the random number used in signing stage is computed by the signer as a function of signer's private key. With this change signer does not need to keep the random number, since he can recompute the same random number at any later time, but it can be computed only by the signer.

II. Modified Secret Signature Scheme

Here we show a modification of Lee et.al.'s discrete log-based implementation of secret signature [5].

1. Setup: Consider common system parameters (p, q, g) where p and q are large primes satisfying $q|p-1$ and g is an element of order q in Z_p^*. We then require a secure cryptographic hash function, $H : \{0,1\} \mapsto Z_q$. Let $\in_R$ denote uniform random selection.

2. Key Generation: A signer A has a long-term certified key pair (x_A, y_A), where $x_A \in_R Z_q^*$ and $y_A = g^{x_A}$. A receiver B has a long-term certified key pair (x_B, y_B), where $x_B \in_R Z_q^*$ and $y_B = g^{x_B}$.

3. Signing: Let m denote the message to be signed. The signer, A, generates a timestamp T and computes a pseudo random number

$$r_A = H(m, T, x_A),$$

which can be computed only by the signer. Using r_A, A computes the one-way agreed key to be shared with the verifier B as

$$W = y_B^{r_A}.$$

A now computes

$$U = g^{r_A}, V = r_A + x_A H(m, T, U, W).$$

A sends the secret signature, $\langle m, T, U, V \rangle$, to the intended receiver, B. Note that we include the timestamp T in secret signature, since it is used at later stage for public proving of secret signature.

4. Verification: The receiver, B, uses his private key, x_B, to compute the agreed key with the signer, $W = U^{x_B}$. B then verifies V by

$$g^V \stackrel{?}{=} U \cdot y_A^{H(m,T,U,W)}.$$

If V verifies correctly, then B is convinced that the message m is indeed signed by A at time T.

III. Public Proving of Secret Signature

Public proving of secret signature has two sub-algorithms; signature proving to prove the validity of secret signature and receiver proving to prove the identity of the receiver. Signature proving is used to show that the secret signature generated by the signer is valid without revealing who is the receiver. On the other hand, receiver proving is used to show that the secret signature is designated to the receiver. These public proving schemes can be executed either by the signer or by the receiver.

A. Signature Proving

Secret signature is a private transaction between a signer and a designated receiver, but if a dispute arises between them, they may want to prove the validity of secret signature to others. Signature proving is used to show that the secret signature generated by the signer is valid without revealing who is the receiver. For signature proving signer or receiver just computes and reveals the agreed key W. From the secret signature $\langle m, T, U, V \rangle$, signer A can compute $r_A = H(m, T, x_A)$ and $W = y_B^{r_A}$, and receiver B can compute $W = U^{x_B}$. Given W, anyone can verify the validity of the secret signature by checking

$$g^V \stackrel{?}{=} U \cdot y_A^{H(m,T,U,W)}.$$

B. Receiver Proving

Let's consider the following dispute scenarios; the receiver argues that he/she is not the receiver of the secret signature, or the signer argues that he/she has not sent the secret signature to the receiver. To resolve these disputes it is required to prove who is the receiver of the secret signature. Receiver proving can be used for this purpose by either the signer or the receiver. In receiver proving the agreed key W is revealed and it is proven that W is related with the designated receiver R in a special way. Its validity can be proven by the signer or the receiver either non-anonymously (using the general proof) or anonymously (using the anonymous proof).

- General Proof: In this proof method signer's proof and receiver's proof are distinguishable, thus the identity of the prover (signer or receiver) who proves the identity of the receiver is revealed.
- Anonymous Proof: In this proof method the identity of the prover who proves the identity of the receiver is not revealed. In this proof signer's proof and receiver's proof are indistinguishable. It is computationally more expensive than that of the general proof.

With the proposed modification in secret signatures, the receiver proving protocol has not changed, thus the same method shown in [5], [6] can be used.

IV. Conclusion

In this paper we pointed out the impracticality of the secret signature schemes proposed by Lee *et al.* [5], [6] in the sense that the signer has to keep the random number used in signing stage for later use. We show that keeping the random number in the signer system for long time is difficult and it can cause security problem. Thus we propose a modified secret signature scheme where the signer's random number is computed by the signer as a function of signer's private key, message and timetsamp. Since the signer can recompute the pseudo-random number at any later time, he doesn't need to keep it in his system. With the proposed modification signer has no burden to save the random number safely for long time, and the secret signature schemes become more ready to use in the real world.

References

[1] S. Araki, S. Uehara, and K. Imamura, "The Limited Verifier Signature and its Applications, IEICE Transactions,"The Institute of Electronics, Information and Communication Engineers Press, Japan, pp. 63–68, Volume E82, A(1), 1999.

[2] X. Chen, F. Zhang, K. Kim, "Limited Verifier Signature Scheme from Bilinear Pairing,"In ACNS 2004, LNCS 3089, pp. 135–148, Springer-Verlag, 2004.

[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography,"In IEEE Transactions on Information Theory, volume IT-22(6), pp. 644–654, 1976.

[4] M. Jakobsson, K. Sako, and R. Impagliazzo, “Designated Verifier Proofs and Their Applications,”EUROCRYPT 1996, LNCS 1070, pp. 321-331, Springer-Verlag, 1996.

[5] B. Lee, K. R. Choo, J. Yang, S. Yoo, “Secret Signatures: How to Achieve Business Privacy Efficiently?,”WISA 2007, LNCS 4867, pp. 30–47, Springer-Verlag, 2007.

[6] B. Lee, J. Li, and K. Kim, “Identity-Based Secret Signature Scheme,”Fourth International Conference on Computer Sciences and Convergence Information Technology (ICCIT2009), pages 1080-1085, Seoul, Korea, 24-26 November 2009.

[7] Y. Zheng, “Digital Signcryption or How to Achieve Cost (Signature Encryption) $\ll$ Cost (Signature) + Cost (Encryption),”CRYPTO 1997, pp. 165–179, LNCS 1294, Springer-Verlag, 1997.