International Journal of Computer Mathematics
Vol. 81, No. 12, December 2004, pp. 1493–1495

UNIVERSAL FORGERY ON SEKHAR'S SIGNATURE SCHEME WITH MESSAGE RECOVERY

F. LAGUILLAUMIE[a,b,*], J. TRAORÉ[a,†] and D. VERGNAUD[b,‡]

[a]*France Télécom Research & Development, 42, rue des Coutures, B.P. 6243, 14066 Caen Cedex 4, France;*
[b]*Laboratoire de Mathématiques Nicolas Oresme, Université de Caen, Campus II, B.P. 5186, 14032 Caen Cedex, France*

(Received 26 May 2004)

Owing to the abundance of electronic applications of digital signatures, many additional properties are needed. Recently, Sekhar [Sekhar, M. R. (2004). Signature scheme with message recovery and its application. *Int. J. Comput. Math.*, **81**(3), 285–289.] proposed three signature schemes with message recovery designed to protect the identity of the signer. In this setting, only a specific verifier can check the validity of a signature, and he can transmit this conviction to a third party. In this note, we show that this protocol is totally insecure, as it is universally forgeable under a no-message attack. In other words, we show that anyone can forge a valid signature of a user on an arbitrary message. The forged signatures are unconditionally indistinguishable (in an information theoretical sense) from properly formed signatures.

Keywords: Cryptography; Universal forgery; Designated verifier signatures; Message recovery

C.R. Categories: E.3; K.6.5; D.4.6; C.2.0

1 INTRODUCTION

Recently, Sekhar [1] designed a signature scheme with message recovery, which is supposed to protect the identity of the signer. The idea for this protocol is to allow only a specific verifier to check the validity of the signature, and this verifier can prove to a third party that the signature is valid. In this sense, this protocol, whose signatures are non-repudiable, is more a designated confirmer signature scheme, as introduced by Chaum [2], than a designated verifier signature protocol introduced by Jakobsson *et al.* [3] (as claimed in Ref. [1]). In fact, in a designated verifier signature scheme (formally defined in Ref. [4]), the identity of the signer is unconditionally protected, essentially because the designated verifier can perform this signature by himself. Therefore, in such a protocol, signatures are repudiable.

The protocol proposed by Sekhar is attractive because it is often necessary in electronic transactions, to minimize the total length of the original message and the appended signature, and to protect the identity of the signer, and using message recovery therefore makes it

* Corresponding author. E-mails: laguillaumie@math.unicaen.fr/fabien.laguillaumie@francetelecom.com
† E-mail: jacques.traore@francetelecom.com
‡ E-mail: vergnaud@math.unicaen.fr

ISSN 0020-7160 print; ISSN 1029-0265 online
DOI: 10.1080/0020716042000272520

possible to kill two birds with one stone. Unfortunately, this scheme suffers a serious security flaw: indeed signatures can be universally forged. In fact, we show that anyone can forge a valid signature of a user on an arbitrary message. Furthermore, the forged signatures are unconditionally indistinguishable from properly formed signatures.

2 REVIEW OF THE SCHEME

In this section, we describe Sekhar's first scheme briefly (our attack can readily be extended to the other protocols). It is designed as follows.

Let p and q be two large primes such that $q|p-1$ and α be an element of $(\mathbb{Z}/p\mathbb{Z})^*$ of order q. Let Alice's public key be $y_A = \alpha^{x_A}$, where $x_A \in (\mathbb{Z}/q\mathbb{Z})^*$ is her secret key. Bob has (x_B, y_B) as couple of private/public keys, with $y_B = \alpha^{x_B}$, $x_B \in (\mathbb{Z}/q\mathbb{Z})^*$.

Alice, who wants to send a message m to Bob proceeds as follows:

1. chooses at random $(k_1, k_2) \in (\mathbb{Z}/q\mathbb{Z}^* \times \mathbb{Z}/q\mathbb{Z})$ and computes $U = \alpha^{k_1 - k_2} \mod p$;
2. computes $r = y_B^{k_1} U m \mod p$;
3. computes $s = k_2 x_A^{-1} - r \mod q$;

the signature is $\sigma = (r, s, U)$.

Once he has received the signature, Bob recovers the message by computing

$$m = r(y_A^{(r+s)} U)^{-x_B} U^{-1} \mod p.$$

If Bob wants to prove to someone else that (r, s, U) is a valid signature from Alice, he executes some zero-knowledge protocols with this third party.

3 THE FLAW

In the paper [1], only the anonymity properties are investigated, not unforgeability. Therefore, it is not possible to point out the error in the security proof.

One can forge a signature of any message m by the following:

1. chooses at random $(t_1, t_2) \in [[1, q-1]]^2$;
2. computes $U = \alpha^{t_1} y_A^{t_2} \mod p$;
3. computes $r = mU y_B^{t_1} \mod p$;
4. computes $s = -r - t_2 \mod q$.

In fact,

$$r\left(y_A^{(r+s)} U\right)^{-x_B} U^{-1} = mU y_B^{t_1} (\alpha^{t_1})^{-x_B} U^{-1} = m.$$

Therefore, (r, s, U) is a valid signature for the message m. Besides, the forged signatures are unconditionally indistinguishable (in an information theoretical sense) from properly formed signatures.

4 CONCLUSION

The purpose of this note is to emphasize, once again, that when adapting existing protocols in a different setting, we must be very careful and investigate all the security aspects from the beginning.

In the context investigated by Sekhar [1], Saeednia *et al.* [5] proposed, in 2003, an efficient designated verifier signature scheme based on Schnorr signatures, whose unforgeability and anonymity under a chosen message attack has been proved by Laguillaumie and Vergnaud [6].

As the concept of designated confirmer (or verifier) signatures with message recovery feature seems promising in financial cryptography, designing such a secure and efficient protocol remains an interesting open problem.

References

[1] Sekhar, M. R. (2004). Signature scheme with message recovery and its application. *Int. J. Comput. Math.*, **81**(3), 285–289.

[2] Chaum, D. (1995). Designated confirmer signatures. Advances in Cryptology – EUROCRYPT '94: Workshop on the theory and application of Cryptographic Techniques, Perugia, Italy, May 1994. *Proceedings: Lecture Notes in Computer Science*, ed. A. De Santis, **950**, 86–91. Springer-Verlag, Heidelberg.

[3] Jakobsson, M., Sako, K. and Impagliazzo, R. (1996). Designated verifier proofs and their applications. Advances in Cryptology – EUROCRYPT '96, International Conference on the theory and application of Cryptographic Techniques, Saragossa, Spain, May 12–16, 1996. *Proceedings: Lecture Notes in Computer Science*, ed. Ueli M. Maurer, **1070**, 142–154. Springer-Verlag, Heidelberg.

[4] Steinfeld, R., Bull, L., Wang, H. and Pieprzyk, J. (2003). Universal designated verifier signatures. Advances in Cryptology – ASIACRYPT 2003, 9th International Conference on the theory and application of Cryptology and Information Security, Taipei, Taiwan, November 30–December 4, 2003. *Proceedings: Lecture Notes in Computer Science*, ed. Laih, Chi Sung, **2894**, 523–542.

[5] Saeednia, S., Kremer, S. and Markowitch, O. (2003). An efficient strong designated verifier signature scheme. 5th International Conference, ICICS 2003, Huhehaote, China, October 10–13, 2003. *Proceedings: Lecture Notes in Computer Science*, ed. Perner, P., Qing, S., Gollmann, D., Zhou, J. **2836**, 40–54. Springer-Verlag, Heidelberg.

[6] Laguillaumie, F. and Vergnaud, D. (2004). Designated verifier signatures: anonymity and efficient construction from *any* bilinear map. Fourth International Conference, SCN 2004, Amalfi, Italy, September 8–10. *Proceedings: Lecture Notes in Computer Science*, ed. Carlo Blundo. To appear.