High-Level Secured Signature Scheme

Nicolae Constantinescu
University of Craiova
Department of Informatics
A.I. Cuza str., no. 13, Craiova
Romania
nikyc@central.ucv.ro

Costin Boldea
University of Craiova
Department of Informatics
A.I. Cuza str., no. 13, Craiova
Romania
cboldea@inf.central.ucv.ro

Abstract: Fan and Lei proposed an user efficient blind signature scheme based on quadratic residues. The main merit of this scheme is that only a few number of arithmetic modular operations are required for a user to get a legal signature. Therefore, it is very suitable for commerce applications. However, Shao pointed out that this scheme did not achieve the unlinkability property. Furthermore, he also proposed an improved blind signature scheme to remedy this weakness and reduce the computations for requests. In this article, we presents a linking strategy to show that this improved version is also not a true blind signature scheme.

Key–Words: signature scheme, public key cryptography, blind signature.

1 Introduction

Public key cryptosystems where a great step forward. With the introduction of RSA [5] there arisen the possibility of digital signatures. This opportunity was a long awaited result since Diffie and Hellman presented their famous paper [6]. The RSA, and other criptosystems alike RSA, (Rabin [3],etc.) introduced digital signatures which could be used as a legal replacement for the classical signature. Generally these signatures assure integrity of data and unforgeability, the signature representing a direct link between the signer and the fact that he signed the document and noone else. However, for some applications this link is not a desired property. These applications might include electronic elections, electronic banking systems, etc. Thus, the identity of the signer should not be revealed, anonymity property being a must.

In 1982 David Chaum [1] proposed a blind signature scheme which not only achieves the unforgeability property but also achieves the unlinkability property. This works in the following way, a requester sends a blind message to request his signature from the signer, the signer signs the blind message and sends the result to the requester. The requester then has to perform a unblinding function in order to obtain a valid signature for his message. The signature has the property that it can be verified but the signer cannot link the blind message and the signature of the chosen message. A secure blind signature scheme must satisfy the unforgeability property and the unlinkability property.

Since users generally have less computing power than the signer, in applications which involve electronic banking, the bank would act as the signer while the customer is the requester. Considering these reasons, Fan and Lei [2] proposed a signature scheme based on quadratic residues (QR) which involves only a few modular computations in order to obtain a legal signature. This property makes the scheme of Fan and Lei appropriate for challenged systems in what concerns computation power available to the user. Despite the qualities of the scheme Shao [4] proved that the signature scheme is not truly a blind signature scheme.

2 Cryptographically approach

The fundamental problem in cryptography is the generation of a shared secret key by two parties, A and B, not sharing a secret key initially over an insecure channel which is under the control of E. The general mathematical model: is that in which A and B are connected only by a public channel and E can eavesdrop the communication. The problem can be solved with public key cryptography in which we assume that the power of computing of E is limited. Another possibility is to develop techniques that avoid the above assumption. The motivation for is two-fold: First, one avoids having to worry about the generality of a particular computational model, which is of some concern in view of the potential realizability of quantum computers. Secondly, and more importantly, no strong rigorous results on the difficulty of breaking a cryptosystem have been proved, and this problem continues to be among the most difficult ones in complex-
ity theory. The general protocol take place in a scenario where $A$, $B$ and $E$ know the correlated random variables $X$, $Y$, $Z$, respectively, distributed according to some joint probability distribution that may be under partial control of $E$ (like for the case of quantum cryptography).

We can see that the problem can be solved in the following phases:

- A and B must detect any modification or insertion of messages
- A and B establish a secret communication key

The first phase is called authentication step. This can be done with classical statistical tests. The second phase consist in three steps:

- Advantage distillation: The purpose of this step is to create a random variable about either $A$ or $B$ has more information than $E$. Advantage distillation is only needed when $W$ is not immediately available from $X$ and $Y$. $A$ and $B$ create $W$ by exchanging messages, summarized as the random variable $C$, over a public channel. A discussion on this facts can be found in Maurer [7]

- Information reconciliation. To agree on a string $T$ with very high probability, $A$ and $B$ exchange redundant error-correct information $U$, such as a sequence of parity checks. After this phase, $E$ (incomplete) information about $T$ consist of $Z$, $C$ and $U$ (Maurer [8])

- Privacy amplification. In the final phase, $A$ and $B$ agree publicly on a compression function $G$ to distill a shorter string $S$ about which $E$ has only a negligible amount of information (Bennett [9] and Cachin [10, 11]). Therefore, $S$ can be subsequently be used as a secret key. In [10] and [11] Cachin proof the connection between smooth entropy, Renyi entropy and privacy amplification phase. In this paper we study the effect of side information $U$ on the collision entropy (Renyi entropy of order 2) which is a measure of the security of the protocol

We assume that the reader is familiar with the notion of entropy and the basic concepts of information theory (Blahut [12]). In privacy amplification, a different and a non-standard entropy measure, collision entropy, is of central importance. Collision entropy is also known as Renyi entropy of order 2 (see Cachin [10]).

### 3 Overview of Shaos Improved User Efficient Blind Signature Scheme

In Shaos scheme, there are two kinds of participants, a signer and a group of requesters. Requesters request the blind signatures from the signer, and the signer issues the blind signatures to the requesters. In addition, the scheme can be divided into four phases: (1) the initialization phase, (2) the requesting phase, (3) the signing phase, and (4) the extraction phase.

**The Initialization Phase**

The signer computes $n = pq$, where $p$, $q$ are two large primes, and $p ≡ q ≡ 3$ $(mod 4)$. Furthermore, let $H$ be a one-way hash function. The signer keeps $p$ and $q$ secret, and publishes $n$ and $H$.

**The Requesting Phase**

To obtain a signature of the message $m$, the requester randomly chooses two integers $u$ and $b$, such that

$$\alpha = b^2 H(m)(u^2 + 1) \mod n. \quad (1)$$

Then the requester delivers $\alpha$ to the signer.

**The Signing Phase**

While receiving $\alpha$, the signer randomly chooses an integer $x$. Because the signer knows the factors $p$ and $q$ of $n$, and $\alpha(x^2 + 1) \mod n$ is a QR in $\mathbb{Z}_n^*$, therefore, the signer has the ability to derive $t$ from

$$t^{-2} = \alpha(x^2 + 1) \mod n. \quad (2)$$

Then, the signer delivers the pair $(t, x)$ to the requester.

**The Extraction Phase**

After receiving $(t, x)$, the requester computes

$$c = (ux - 1)(x + u)^{-1} \mod n, \quad (3)$$

and

$$s = bt(x + u) \mod n. \quad (4)$$

The pair $(c, s)$ is a signature of $m$. To verify the validity of $(c, s)$ of $m$, the verifier checks whether or not the following equation holds,

$$H(m)s^2(c^2 + 1) = 1 \mod p. \quad (5)$$

In the following, we prove that equation 5 always holds while the signature $(c, s)$ is correct. According to equation 2, we get

$$t^2\alpha(x^2 + 1) = t2t - 2 = 1 \mod n. \quad (6)$$

Hence, we have
With \( c \) and \( s \), the signer computes

\[
H(m)s^2(c^2 + 1) = (\frac{\alpha}{b^2(c^2 + 1)})((bt(x+u))^2((\frac{ux-1}{x+u})^2 + 1))
\]

\[
= (\frac{\alpha b^2}{c^2 + 1})((bt(x+u))^2((ux-1)^2 + (x+u)^2))
\]

\[
= (\alpha b^2(u^2 + 1))(bt)^2(x^2 + 1)(a^2 + 1)
\]

\[
= t^2 \alpha (x^2 + 1) = 1 \mod n.
\]

## 4 The Weakness of Shaos Improved User Efficient Blind Signature Scheme

In this section, we show that the signatures can be traced by the signer in Shaos scheme. Therefore, this scheme does not really achieve unlinkability property. We consider the follow scenario.

1. Let \( RI_i \) be the requester is identity. The signer keeps a set of records \( S = \{(RI_i, \alpha_i, t_i, x_i) \mid i = 1, 2, \ldots, z\} \) for \( z \) instances of the blind signed messages. Furthermore, the signer obtains the signature \((H(m), c, s)\) of the message \( m \) when it is revealed by a requester.

2. With \( c \) and \( s \), the signer computes

\[
cs = (ux-1)bt \mod n.
\]

Then, the signer takes out \( t \) from some tuples in the set \( S \) and computes

\[
cst^{-1} = (ux-1)bt \mod n,
\]

and

\[
(cst^{-1})^2 = (ux-1)^2b^2 = (u^2x^2 - 2ux + 1)b^2 = u^2b^2x^2 + b^2 - 2uxb^2 \mod n.
\]

3. Since

\[
\alpha = b^2H(m)(u^2 + 1) \mod n,
\]

the signer can compute

\[
\alpha H^{-1}(m) = b^2(u^2 + 1) = b^2u^2 + b^2 \mod n.
\]

4. Now, in the signing phase, if the signer chooses \( x = 1 \) for some requesters on purpose, then equation 9 can be rewritten as

\[
(cst^{-1})^2 = u^2b^2 + b^2 - 2ub^2 \mod n.
\]

From equations 10 and 11, the signer can derive

\[
(cst^{-1})^2 = \alpha H^{-1}(m) - 2ub^2 \mod n.
\]

Therefore,

\[
2ub^2 = \alpha H^{-1}(m) - (cst^{-1})^2 \mod n.
\]

That is,

\[
ub^2 = 2 - 1(\alpha H - 1(m) - (cst^{-1})^2) \mod n.
\]

5. From Equation (4), since \( s = tb + tub \mod n \), we have

\[
sb = tb^2 + tub^2 \mod n.
\]

To replace \( ub^2 \) with \( 2-1(\alpha H-1(m)-(cst-1)^2) \) from equation 12, equation 13 becomes

\[
sb = tb^2 + t(2^{-1}(\alpha H^{-1}(m)-(cst^{-1})^2)) \mod n.
\]

Since

\[
tb^2 - sb = -t(2^{-1}(\alpha H^{-1}(m)) - (cst^{-1})^2) \mod n,
\]

we have

\[
b(b - st^{-1}) = (cst^{-1})^2 - 2^{-1}\alpha H^{-1}(m) \mod n.
\]

Therefore, the signer can derive

\[
b(b - st^{-1}) = (cst^{-1})^2 - 2^{-1}\alpha H^{-1}(m) \mod n.
\]

6. The improved blind signature scheme is based on the theory of quadratic residues. The security of this scheme is based on the difficulty of finding the square roots modulo a composite number. According to Rabins public key cryptosystem [3], to encrypt the message \( M \), the encryption function is

\[
E(M) = C = M(M + a) \mod n,
\]
where \( C \) is the corresponding ciphertext and \( a \) and \( n \) are made public. The decryption function is

\[
D(C) = M = \frac{-a}{2} \pm \sqrt{(a/2)^2 + C \mod p} \tag{17}
\]

or

\[
D(C) = M = \frac{-a}{2} \pm \sqrt{(a/2)^2 + C \mod q}. \tag{18}
\]

Without knowing the factors \( p \) and \( q \) of the modulus \( n \), it is infeasible to compute the square root \( M \) from the given messages \( a \) and \( C \). Recall the computation of the square root \( b \) from equation (15). Since the signer knows the factors \( p \) and \( q \) of \( n \), \( st^{-1} \mod n \), and \((cst^{-1})^2 - 2^{-1}aH^{-1}(m)\mod n \), the parameter \( b \) in equation (15) can be easily computed from the decryption function of Rabin’s public key cryptosystem.

7. Since \( b \) can be obtained, therefore the signer can compute \( u \) from equation (12). Further, the signer can compute \( c' \) and \( s' \) from equations (3) and (4). If \((c', s')\) is equal to the received signature \((c, s)\), then the signer can get the identity of the requester from some record in the set \( S \). Obviously, by the blind signature \((H(M), c, s)\), the signer can make a linkage between it and the identity of the requester. Therefore, the scheme does not achieve the unlinkability property.

5 Conclusions

Shaos scheme is designed to be more efficient for users. Therefore, the scheme is suitable for many applications that users have low computation capabilities. However, Shaos scheme is not a true blind signature. In this article, we have presented a link strategy to show that Shaos blind signature scheme is not really blind. The future research will focus on the special signature classifications, ranking by Equivalent Linear Complexity.

Acknowledgements: The research was partial supported by CNCSIS grant no 79/2007 in the case of the first author.

References:


