A New Blind Signature for Electronic Commerce

Hua Wang *Ron Addie*

Department of Mathematics & Computing
University of Southern Queensland
Toowoomba, Australia, Q4350
E-mail: {wang, addie}@usq.edu.au

Abstract. Blind signature schemes, as important cryptographic primitives, are useful protocols that guarantee the anonymity of the participants. In this paper, a new blind signature based on the strong *RSA* assumption is presented. The new blind signature scheme is quite efficient and state-free. It does not require the signer to maintain any state and can be proven secure against adaptive chosen message attack under a reasonable tractability assumption, the so-called Strong *RSA* assumption. Moreover, a hash function can be incorporated in to the scheme in such a way that it is also secure in the random oracle model under the standard *RSA* assumption.

Keywords: Signature scheme, RSA, Security.

1. Introduction

A blind signature scheme is a protocol allowing Bob to obtain a valid signature for a message *m* from a signer Alice without her seeing the message or its signature. If Alice sees *m* and its signature later, she can verify that the signature is genuine, but she is unable to link the message-signature pair to the particular instance of the signing protocol that has led to this pair. The concept of a blind signature scheme was introduced by Chaum [2]. It allows to realize secure electronic cash systems protecting customer's privacy (e.g. [1], [3], [4], [5], [7], [8]) as well as other cryptographic protocols protecting the participant's anonymity (e.g. secure voting protocols [12]). Two proposals for blind signature scheme have been published: the first, presented in [2], is based on the *RSA* scheme, and the second is described in [6].

R. Gennaro, S. Halevi, and T. Rabin [11] recently discovered efficient, state-free signature schemes based on the strong RSA assumption. Their schemes contains several signature schemes, but the only fully proved scheme requires a "rap door" or "chameleon" collision-resistant hash function with the following very special property: its output is a prime number. Implementing such a hash function is both awkward and potentially computationally expensive.

The strong RSA assumption (*SRA*) is that the following problem is hard to solve:
Given a randomly chosen *RSA* modulus *n* and a random $z \in Z_n^*$, find $r > 1$ and $y \in Z_n^*$ such that $y^r = z$.
Note that this differs from the ordinary *RSA* assumption (*RA*), in that for *RA*, the exponent *r* is chosen independently of *z*, whereas for *SRA*, *r* may be chosen in a way that depends on *z*. The *SRA* is a potentially stronger assumption than the *RA*, but at the present time, the only known method for breaking either *RA* or *SRA* is to solve the integer factorization problem.

In this paper, we propose a new blind signature scheme. Our scheme is more efficient and state free and can solve the above the problem related to "trap door" or "chameleon" collision-resistant hash function. While the signing algorithm still has to generate a prime number, it has a great deal of flexibility in how this is done, yielding a much more efficient algorithm.

The security of our new blind signature scheme is against an adaptive chosen message attack, as defined in [10]. To prove our new scheme is secure, we need the strong RSA assumption, recently introduced by N.Baric and B.Pfitzmann [16]. We also need a collision-resistant hash function and a universal one-way hash function [12]. Our new scheme is desirable in that they are state-free, unlike other provably secure schemes [8, 9]. Of course, we achieve this at the expense of using a potentially stronger assumption than that is made in [8, 9].

We are not making use of the "random oracle" model of computation [11], in "random oracle model" (a random database for keys and users etc) where all parties have access to a public random oracle that provides a bridge between cryptographic theory and cryptographic practice, but rather, we are working in the "real world" of computation. Indeed, the standard "hash and invert" *RSA* signature is provably secure in the random oracle model under the standard *RSA* assumption. We also make the further observation that another trapdoor hash function can be incorporated in to our new scheme in such a way that they are also secure in the random oracle model under the standard *RSA* assumption. In this sense, our scheme can be made to be at least as secure as a standard *RSA* signature.

Our new scheme can be seen as an improved variation of the scheme of R. Cramer and V. Shoup [10].

This paper is organized as follows: in section 2, we introduce a basic signature scheme and then the new blind signature scheme is presented as an improvement in section 3. Conclusions are included in section 4.

2. Basic Signature Scheme

In this section we describe the basic signature scheme. The scheme is parameterized by two security parameters k and l, where $l + 1 < k$. Reasonable choices might be $k = 512$ and $l = 160$. The scheme makes use of a collision-resistant hash function H whose output can be interpreted as a positive integer less than 2^l. A reasonable choice for H might be SHA-1. For a positive integer n, we let QR_n denote the subgroup of Z_n^* of squares (i.e., the quadratic residues modulo n).

Key Generation

Two random k-bit primes p and q are chosen, where $p = 2p'+1$ and $q = 2q'+1$ with both p' and q' prime. Let $n = p\,q$ and the following are also chosen:

1. random numbers $h, x \in QR_n$
2. a random $(l + 1)$-bit prime e'

The **public key** is

$$(n, h, x, e').$$

The **private key** is

$$(p; q).$$

Signature Generation

To sign a message m (an arbitrary bit string), a random (l + 1) bit prime $e \neq e'$ and a random $y' \in QR_n$ are chosen. The equation

$$y^e = x h^{H(x')}$$

is solved for y, where x' satisfies the equation

$$y'^{e'} = x' \, h^{H(m)}.$$

Note that y can be calculated using the factorization of n in the private key. The signature is

$$(e, y, y').$$

Signature Verification

To verify a putative signature (e, y, y') on a message m, it is first checked that e is an odd $(l+1)$-bit number different from e'. Second, $x' = y'^{e'} h^{-H(m)}$ is computed. Third, it is checked that $x = y^e h^{-H(x')}$.

Lemma 1: The above signature scheme is secure against adaptive chosen message attack, assuming the strong *RSA* and assuming that H is collision resistant.

3. New Blind Signature Scheme

In this section, we design a new blind signature scheme based on the basic signature scheme, and prove that the new result is a blind signature scheme.

First we give a formal definition of the blindness for a signature scheme. Let *V* denotes Alice's complete view of an execution of the protocol, i.e. her random coin tosses and all exchanged values; and let (*m, sig(m)*) denote the message- signature pair generated in that particular execution.

Definition 2. A signature scheme is called blind if Alice's view *V* and the message-signature pair (*m, sig (m)*) is statistically independent.

The following protocol is a blind version of the modification of strong *RSA* described in Section 2. Suppose $x = \mathrm{h}^{\alpha} \pmod{\mathrm{n}}$.

Step 1. Alice randomly chooses $y' \in QR_n$ and computes $\tilde{R} = \mathrm{x}^{y'} \pmod{n}$ and sends $y', \tilde{R}$ to Bob.

Step 2. Bob randomly chooses $\alpha, \beta \in QR_n$ and computes

$$x' = \alpha\, m + \beta\, \tilde{R} \pmod{\mathrm{n}}, \quad \tilde{m} = \beta H(x') \pmod{n}$$

$$R = \tilde{R}^{\alpha}\, \mathrm{h}^{\beta H(x')} \pmod{n}, u = \alpha a y' + \tilde{m} \pmod{n}$$

and sends *u* to Alice.

Step 3. Alice computes $b = du \pmod{p'q'}$, $y = h^b \pmod{n}$ and sends y to Bob. Where e is a random odd integer in QR_n and $ed = 1 \pmod{p'q'}$.

Step 4. Bob verifies $y^e \stackrel{?}{=} R \pmod{n}$.

Note: Alice is trusted only if the verification $y^e \stackrel{?}{=} R \pmod{n}$ is passed or not.

We describe the blind signature scheme as follows for blind proof:

Alice		Bob
$y' \in QR_n$, $\tilde{R} = x^{y'} \pmod{n}$	$\xrightarrow{y', \tilde{R}}$	$\alpha, \beta \in QR_n$
		$x' = \alpha m + \beta \tilde{R}$
		$R = \tilde{R}^{\alpha}\, \mathrm{h}^{\beta H(x')} \pmod{\mathrm{n}}$
	$\xleftarrow{u}$	$u = \alpha a y' + \tilde{m} \pmod{n}$
$b = du \pmod{p'q'}$, $y = h^b \pmod{n}$	$\xrightarrow{y}$	Verify $y^e \stackrel{?}{=} R \pmod{n}$

Theorem 3: The pair (e, y, y') is a valid signature of message *m* for the modification of strong *RSA* presented in Section 2 and the above protocol is a blind signature scheme.

Proof: The validity of the signature (e, y, y') can easily be shown as follows.

$$eb = edu = u = \alpha a y' + \tilde{m} \pmod{p'q'}$$

hence

$$y^e = h^{eb} = h^u = h^{\alpha a y' + \tilde{m}} = x^{\alpha y'} h^{\tilde{m}} = \tilde{R}^{\alpha}\, \mathrm{h}^{\beta H(x')} = R \pmod{n}$$

which means that (e, y, y') is a valid signature of *m* .

In order to prove the blindness of the protocol, we show that given any view V and any valid message signature pair $(m, (e, y, y'))$, there exists a unique pair of blinding factors α and β. Because Bob chooses the blinding factors α and β at random, the blindness of the signature scheme follows.

If the signature (e, y, y') of m has been generated during an execution of the protocol with view V consisting of y' (public), $\tilde{R} = x^{y'} (\mathrm{mod} n)$, $b = du (\mathrm{mod}\ p'q')$, $y = h^b (\mathrm{mod}\ n)$, then the following equations must hold for α and β:

$$x' = \alpha m + \beta \tilde{R} (\mathrm{mod}\ n)$$
$$u = \alpha a y' + \beta H(x') (\mathrm{mod} n)$$
$$R = \tilde{R}^{\alpha}\ \mathrm{h}^{\beta \mathrm{H}(x')} (\mathrm{mod}\ n)$$

By the strong *RSA* assumption , the blinding factors α and β are uniquely determined by the first two equations:

$$\beta = \frac{(ay'x' - mu)}{(\tilde{R}ay' - mH(x'))} (\mathrm{mod}\ n),$$
$$\alpha = \frac{(x'H(x') - u\tilde{R})}{(mH(x') - ay'\tilde{R})} (\mathrm{mod} n)$$

Because $ed = 1 (\mathrm{mod}\ p'q')$, we obtain:

$$eb = edu = u = \alpha a y' + \tilde{m} = \alpha a y' + \beta H(x') (\mathrm{mod}\ p'q')$$

therefore:

$$y^e = R (\mathrm{mod}\ n).$$

The proof of the security of the new blind scheme is omitted here, as it can be shown in a similar way to that in [10].

Notes that the signature verification algorithm does not need to verify that e is prime. This is better than R. Gennaro, S. Halevi and T. Rabin's scheme [11]. We need a collision-resistant hash function but a universal one-way hash function [12] is sufficient. Our new scheme is state-free, unlike other provably secure schemes in [8, 9].

4. Conclusion

In this paper, we have developed a new blind signature scheme based on strong RSA assumption. The security of our scheme is guaranteed by Lemma 1. The new blind scheme is state free and much more efficient and it does not require the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable tractability assumption, the so-called Strong *RSA* assumption. Moreover, a hash function can be incorporated in to the scheme in such a way that it is also secure under the standard *RSA* assumption.

References

[1] D. Chaum: Blind Signature Systems, Advances in Cryptology , Crypto '83 , Plenum, pp: 147-153.

[2] Jan Camenisch and Markus Michels, Separability and Efficiency for Generic Group Signature Schemes in Advances in Cryptology – CRYPTO '99., Springer Verlag, pages 106-121.

[6] D. Chaum, T. Pedersen: Wallet databases with observers, Advances in Cryptology, Crypt '92, LNCS 740, Springer Verlag, pp. 89-105.

[8] R. Cramer and I. Damgard. New generation of secure and practical RSA-based signatures. Advances Cryptology, Crypto '96, pages 173-185, 1996.

[9] C. Dwork and M. Naor. An efficient existentially unforegeable signature scheme and its applications. In Advances in Cryptology-Crypto '94, pages 218-238, 1994.

[10] R. Cramer, V. Shoup. Signature schemes based on the Strong RSA assumption, 6th ACM Conference on Computer and Communication Security, Singapore, ACM Press, November 1999.

[11] R. Gennaro, S. Halevi, and T. Rabin. Secure signatures, without trees or random oracles. Advances in Cryptology-Eurocrypto '99 , pages 123- 139, 1999.

[12] M. Naor and M.Yung. Universal one-way hash functions and their cryptographic applications, In 21st annual ACM Symposium on Theory of Computing, 1989

[13] M. Bellare and P . Roga way . Random oracles are practical: a paradigm for designing efficient protocols. In First ACM Conference on Computer and Communications Security , pages 62-73, 1993.

[14] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21,2 (Feb. 1978), 120--126.

[15] H. Wang, Y. Zhang, J. Cao, V. Varadharajan, Achieving Secure and Flexible M-Services Through Tickets, IEEE Transactions Special issue on M-Services. IEEE Transactions on Systems, Man, and Sybernetics. Part A, Vol. 33, Issue: 6, pages: 697- 708, Nov. 2003.

[16] N. Baric and B. Pfitzmann ,collision-free accumulators and fail-stop signature schemes without trees, Advances in Cryptology-Eurocrypto '97 , pages 480-494, 1997.