A Simple Secure Signature Scheme Based on the Strong RSA Assumption without Random Oracle Model

Akram Naji **and** **Yahya Abu Hasan**,

School of Mathematical Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia.

Summary
In this paper, we present a simple secure signature scheme which is based on the Strong RSA Assumption without random oracle model. This scheme is derived from the Cremer and Shoup strong RSA signature scheme. In contrast, the public key and signature sizes in our proposed scheme are smaller. Consequently, our scheme is somewhat more efficient.

Key words:
Cryptography, public key cryptosystem, digital signature, RSA

1. Introduction

The paper based workflow systems are rapidly being replaced by the electronic based media systems, in which all forms, messages and data are digitally processed; examples as in e-government and e-commerce. In these systems, it is very important to preserve the original contents from any malicious interference. This is a problem of security.

Digital signature techniques, which allow transferring message and user identity authentication, begin to play a very important role in the network communication. Even in a small organization, it is desirable to authenticate all messages from one employee to the other.

Many signature schemes were proposed since the 90's. It is known that a signature scheme that produces signatures of length l can have some security of at most 2^l, which means that given the public key, it is possible to forge a signature on any message in $O(2^l)$ time.

A natural question is how we can construct a signature scheme that can provide the same security while at the same time use a shorter signature length.

In 1988, Goldwasser, Micali and Rivest formally introduced the standard security model for the digital signature, namely "existential unforgeability under an adaptive chosen message attack"[7]. In their paper, they proposed the first provably secure signature scheme under the standard model; however, their scheme was impractical. Later, in 1999, Gennaro, Halevi and Rabin proposed the efficient, state-free signature scheme based on the strong RSA assumption which is provably secure under the standard model [6]. The Gennaro scheme required a trapdoor collision-resistance hash function with very special property: its output is a prime. This property made The Gennaro scheme more computationally expensive. In 1999, Cremere and Shoup constructed a practical and secure signature scheme under the strong RSA assumption in the standard model without random oracle [3] which sidesteps that problem. The Cremere and Shoup received many considerations which introduced the variants schemes; Camensisch and Lysyanskaya [3], Popescu [10], Fischlin [5], Tan et al. [13], and Tan [12]. The last three schemes are more efficient than the original scheme and Camensisch and Lysyanskaya which is less efficient then the original scheme.

In this paper, we proposed a simple secure signature scheme which is derived form the Cremer and Shoup strong RSA signature scheme [3]. Our scheme is provably secure against adaptive chosen message attack which meets the definition of the standard security, as define in [7]. The proposed scheme compares well with the original scheme and its variants; it has the smaller public key and signature size, thus enhancing the scheme efficiency.

2. Theoretical Assumption

We first describe the two assumption of RSA to be used in our scheme.

Definition 1. Ordinary RSA Assumption (ORSA). Let $n = p.q$ be the product of two large primes, an element $z \in Z_n^*$, and $e \in Z_n^*$ such that $gcd(e,(p-1)(q-1)) = 1$, the ordinary RSA Assumption states that it is hard, given $n, z, e \in Z_n^*$, to find $y \in Z_n^*$ such that $y^e = z\,(mod \quad n)$.

Definition 2. Strong RSA Problem (SRSA). *Let* $n = p.q$ be the product of two large primes, and an element

Manuscript received November 5, 2007
Manuscript revised November 20, 2007

$z \in Z_n^*$. The Strong RSA Problem (SRSA) states that it is hard to find values $e \in Z_n^*$ such that $gcd(e,(p-1)(q-1)) = 1$, and $y \in Z_n^*$ such that $y^e = z\,(mod \;\; n)$.

The security of our digital signature scheme is based on the Strong RSA Assumption.

3. The Signature Scheme

Our scheme resembles somewhat the scheme of Cremer and Shoup [3]. The scheme is parameterized by two security parameters l and l' where $l+1 < l'$. In our scheme, reasonable choice might be $l = 256$ and $l' = 512$. We suggest modifying the parameter l because the Cremer and Shoup signature used SHA-1 [9] in their scheme which it output less than 2^l. Unfortunately, SHA-1 has been broken [14]. The attacks can find collisions in the full version of SHA-1, requiring fewer than 2^{69} operations. Therefore, we incorporate SHA-256 as a collision resistant hash function *H* in our scheme to output a positive integer less than 2^l.

3.1. KEY GENERATION

A signer now chooses the following values to generate his public and private key.

1. select two random l'-bit primes p & q such that $p = 2p'+1$ and $q = 2q'+1$, with both p' & q' prime.
2. set RSA modulus $n = p.q$
3. choose two random $h, x \in QR_n$; (for a positive integer *n*, QR_n donate the quadratic residues modulo *n*)
4. The public key $PK = (n, h, x)$
5. The corresponding secret key $SK = (p, q)$

3.2. Signature Generation

To sign a message $m \in \{0,1\}^*$ the signer achieves the following steps:

1. choose at random *(l + 1)*-bit prime e
2. solve the following equation for y
$$y = (x h^{H(m)})^{-e}\,(mod\, n)$$
3. A valid signature on m is given by *(e , y)*.

Note that, signer can calculate y easily since he/she knows the factorization of n in the private key.

3.3. Signature Verification

To verify that a putative signature (*e , y)* on a message $m \in \{0,1\}^*$ is a valid signature (with respect the public key of the signer) the following steps are checked correctly:

1. check that e is an *(l + 1)*-bit prime
2. check that $x = y^e \, h^{-H(m)}\,(mod\, n)$

4. Security Proof Analysis

We now show that our signature scheme is secure against an adaptive chosen message attack, similar to [2].

Theorem 1. The signature scheme presented above is secure against adaptive chosen messages attack under SRSA Assumption and the further assumption that there exists a family of hash functions *H* are collision-resistant.

Proof: To prove this theorem, let us consider a forging algorithm that allows the adversary as an oracle to makes *t* signing queries. Let m_i (where $1 \le i \le t$) be the *i*th message signed, its output signature is (e_i, y_i). Let (e, y) be the forgery signature on message *m*, where *m* is not queried for all signing queries.
Now, we assume that all e_i chosen by the signer during an attack are distinct and $H(m) = H(m_i)$ for all *i*. The forged signature must satisfy one of the following.

There two types of forgers as the following:
Type II: For some $1 \le j \le t$, $e = e_j$
Type III: For all $1 \le i \le t$, $e \ne e_i$

Comparing this forging algorithm with forging algorithm of Cremer & Shoup [2], in our algorithm the Type I Forger disappear due to our modification. We show how can use Type II forger and III forger to break the ORSA and SRSA respectively.

4.1 Type II Forger

Suppose we have a Type II Forger success with non-negligible probability. We can use this Type to break the Original RSA assumption. We are given n, a random $z \in Z_n^*$, and a random *(l+1)-bit* prime *r,* must find an $z^{1/r}$. For doing this, we invoke Type II Forger on creating the public key and generate signature. Set $e_j = r$ and for all $i \ne j$, choose a random *(l+1)*-bit prime e_i.

Let $$h = z^{2 \cdot \prod_{i \ne j} e_i}$$

Pick $w \in Z_n^*$, and *l-bit* a randomly

Set $$x = h^{-a} \cdot w^{2 \prod_i e_i}$$

To sign the *i-th* message on behalf on the signer; $i \neq j$, $e_i \neq e_j$

$$y_i^{e_i} = z^{-2a\prod_{k\neq i} e_k} \cdot w^{2\prod_{k\neq i} e_k} \cdot z^{2\prod_{k\neq i} e_k \cdot H(m_i)}$$

$$y_i^{e_i} = w^{2\prod_{k\neq i} e_k} \cdot z^{2\prod_{k\neq i} e_k \cdot (H(m_i)-a)}$$
$$= (x \cdot h^{H(m_i)})^{-e_i}$$

For the *j-th* signature query

$$y_j^{e_j} = w^{2\prod_{k\neq j} e_k} \cdot z^{2\prod_{k\neq j} e_k \cdot (H(mj)-a)}$$
$$= (x \cdot h^{H(m_i)})^{-e_j}$$

We assume that Adv creates a Type II Forger (e,y) on a message *m*, where $e = e_j = r \ \& H(m) \neq H(m_j)$, so that we get

$$y = (x \cdot h^{H(m)})^{-e}$$
$$y_j = (x \cdot h^{H(m_j)})^{-e_j}$$

The output of Adv produces another representation of *x* with respect to *h and* $e = e_j = r$, that is

$$y_j^{e_j} \cdot h^{-H(m_j)} = x = y^e \cdot h^{-H(m)}$$

We then obtain $(\frac{y}{y_j}) = h^{H(m)-H(m_j)}$

By letting $w = \frac{y}{y_j}$ and $c = H(m) - H(m_j)$,

we have

$$w^r = z^{2c\prod_{i=1}^{t} e_i}$$

If $gcd(2c\prod_{i=1}^{t} e_i, r) \neq 1$ for all $1 \leq i \leq t$, output fails and stops. Otherwise, we assume $gcd(2c\prod_{i=1}^{t} e_i, r) = 1$,

let $e' = 2c\prod_{i=1}^{t} e_i$, so $gcd(e', r) = 1$. By the extended Euclidean algorithm, we can find two other integers $\bar{e} \ \& \ \bar{r} \in Z$ such that $\bar{e}e' = 1 + \bar{r}r$. It follows that

$$(w^{\bar{e}} \cdot z^{\bar{r}}) = z$$

4.2. Type III Forger

We demonstrate how to use this case to break the SRSA assumption. That is, we are given *n* and $z \in Z_n^*$, find $r > 1$ and an *r-th* root of *z*.

We invoke Type III Forger on creating the public key and generate signature, as following. We choose a random *(l+1)*-bit primes $e', e_1, ..., e_t$. We then let

$$h = z^{2e' \cdot \prod_i e_i}$$

$x = h^a$, such that a random $a \in \{1, ..., n^2\}$

Now, as QR_n is a cyclic group of order $p'q'$. We assume that *h* is a generator QR_n with high probability. Now let $a = b\,p'q' + c$, where $0 \leq c \leq p'q'$, due to choosing *a* randomly at a suitable large interval, as follows in [2], *c* and *b* are essentially independent.

Since we know all the relevant roots of *x* and *h*, we can easily sign all message. Now let Adv create the Type III Forger, e,y . Then we have

$$y = (x \cdot h^{H(m)})^{-e} = z^{2e'\prod_i e_i \cdot (a + H(m_i))} = z^m$$

Where $m = 2e'\prod_i e_i \cdot (a + H(m_i))$

The fact that $e \nmid m$ with non-negligible probability, let $d = gcd(e, m))$, and then we can compute a non-trivial *(e/d)th* root of z. By letting, *r* to be a prime dividing *e* and follows the same argument in [2], we can find *rth* root of *z*.

5. Efficiency Performance Analysis

In this section, we consider the efficiency performance of our scheme. We compare the computation complexity of our proposed scheme with the Cremer & Shoup scheme and its variants in terms of the signature size, public keys size and the signing time. In literature, Tan made a good comparison between his scheme with the Cremer-Shoup scheme (CS), Camensisch-Lysyanskaya scheme (CL), Fischlin scheme (F), and Tan et al. scheme (TYS) under same security parameters, refer to [12]. Continuously, we make comparing with the CS scheme, the Popescu scheme (P), and the Tan scheme (T) under same conditions in Table 1:

Table 1 Computational Complexity Comparison

	CS Scheme	*P Scheme.*	*T Scheme*	*Proposed Scheme.*
PK	$3n+l+1$	$3n$	$3n$	$3n$
Sg. S	$2n+l+1$	$2n+l+1$	$n+2l+2$	$n+l+1$
Sg. T	$3l$	$2l$	$2l$	$2l$

Note: PK is the public size. Sg. S is the signature size. Sg. T is the signing time.

Referring to the table above, the signing size of our proposed scheme is shorter than that of Cremer-Shoup scheme, the Popescu scheme, and the Tan scheme. The public key size of our proposed scheme is shorter than that of Cremer-Shoup scheme, and almost same as that of the Popescu scheme, and the Tan scheme.

Secondly, The cost and times of signature generation algorithm in our scheme can be broken down into the following components; generation of a random *(l + 1)-bit* prime e, and computation of *y* which needs two exponentiations: one full with $e^{@1}$, and one small with *H(m).* From the above table, the time and the cost signature generation of proposed is more efficient than the

Cremer-Shoup scheme and somewhat better than Tan scheme.

We can improve the efficiency of our scheme by reducing the cost of computation of y by making some alteration to the key generation algorithm to generate x as a power of h , *for a random a mod* $p'q'$, and compute $x = h^a$. The value of a would become a part of a private key. This modification reduces the cost by perform only one full exponentiation with $(a + H(m))\ e^{@1}$. For speeding up modular exponentiation, we can use any method such as the Chinese Remainder Theorem, or pre-computation technique [8].

However, the cost and exponentiation times require in our scheme to generate signature is less than the cost of the Cremer and Shoup scheme.

6. Conclusion

In this paper, we proposed a simple secure simple signature scheme based on the strong RSA assumption. The proposed scheme is derived from the Cremer and Shoup strong RSA signature scheme. We show that our scheme is provable secure against adaptive chosen messages attack without using random oracle model. Besides, our scheme has a smaller public key and signature size than the original scheme. Finally, we show that the cost and time of our scheme are lees than the original scheme. Therefore, our scheme is more efficient.

Acknowledgment

The authors would like to express their cordial thanks to The Universiti Sains Malaysia (USM) Fundamental Research Grant Scheme (FRGS) grant for supporting this study.

References

[1] Cramer, R. & Damgaard, I., "New generation of secure and practical RSA-based signatures," In Advances in Cryptology-Crypto'96. pp. 173-185, 1996.

[2] Camenisch, J. and Lysyanskaya, A.'A signature scheme with efficient protocols', Proceedings of Third Conference on Security in Communication Networks – SCN'02, Amalfi, Italy, pp.274–295, 2003.

[3] Cramer, R. & Shoup, V., "Signature Schemes Based on the Strong RSA Assumption," IBM Research Report RZ 3083, 1999.

[4] Diffie, W. & Hellman, M., "New Directions in Cryptography," IEEE Transaction Information Theory. IT-22, 6, pp. 644-654, 1976.

[5] Fischlin, M.,'The Cramer-Shoup strong-RSA signature scheme revisited', Proceedings of Workshop in Public Key Cryptography – PKC 2003, Miami, FL, pp.116–129, 2003.

[6] Gennaro, R., Halevi, S. and Rabin, T.,'Secure hash-and-sign signature without the random oracle', Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt'99), Prague, Czech Republic, pp.123–139, 1999.

[7] Goldwasser, S. Micali, & S. Rivest. R. "A digital signature scheme secure against adaptive chosen-message attacks," SIAM Journal on Computing. 17(2), pp. 281-308, 1988.

[8] LIM, C. H. & LEE, P. J. () More Flexible Exponentiation with Precomputation. Advances in Cryptology - CRYPTO '94, 95-107, 1994.

[9] National Institute of Standards and Technology. "Secure Hash Standard (SHS) ," FIPS Publication 180-1, 1995.

[10] Popescu, C., " A Modification of the Cramer-Shoup Digital Signature Scheme" , Studia Univ. "Babeş-Bolyai" Informatica, vol. XLVII, nr. 1, pp. 27-36, 2002.

[11] Rivest, R. Shamir, A. & Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, 21, pp. 120-126, 1978.

[12] Tan, C.H.,'A new signature scheme without random oracles', International Journal of Security and Networks - Vol. 1, No.3/4 pp. 237 - 242, 2006.

[13] Tan, C.H., Yi, X. and Siew, C.K.'A new provably secure signature scheme', IEICE Transactions on Fundamentals of Electronic, Communications and Computer Sciences, Vol. E86-A, No. 10, pp.2633–2635. 2003

[14] Wang, X. Yin, Y. & Yu, H., "Finding collisions in the full SHA-1," Lecture Notes in Computer Science. 3621,17–36. 36, 2005

Akram Naji received the B.Sc. in Mathematical Sciences from Depart. of Math. Sana'a Univ., Yemen, in 1997. He received the M.Sc. degree in IT from School of Computer Sciences, USM, Malaysia, in 2005. After, he worked as a demonstrator in Depart. of Math. Al-Mahweet Collage, Sana'a Univ., (1997-2001). He is working towards Ph.D in Cryptography at the School of Mathematical Sciences, University Sains Malaysia. His current research interest is in the digital signature schemes.

Yahya Abu Hasan is a lecturer in the School of Mathematical Sciences, Universiti Sains Malaysia. His research interests are: data security (digital signature), data mining (microarray) and mathematical modeling (epidemiology).