

New signature scheme based on two cryptographic assumptions

Zheng Minghui^{1,2} Cui Guohua¹

(¹College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

(²Department of Computer Science, Hubei Institute for Nationalities, Enshi 445000, China)

Abstract: In order to improve the security of the signature scheme, a digital signature based on two hard-solved problems is proposed. The discrete logarithm problem and the factoring problem are two well known hard-solved mathematical problems. Combining the ElGamal scheme based on the discrete logarithm problem and the OSS scheme based on the factoring problem, a digital signature scheme based on these two cryptographic assumptions is proposed. The security of the proposed scheme is based on the difficulties of simultaneously solving the factoring problem and the discrete logarithm problem. So the signature scheme will be still secure under the situation that any one of the two hard-problems is solved. Compared with previous schemes, the proposed scheme is more efficient in terms of space storage, signature length and computation complexities.

Key words: digital signature; security; factoring problem; discrete logarithm problem

Digital signatures play an important role in the security of e-government, e-commerce and other web applications by assuring the integrity, authenticity and non-repudiation of web data both when exchanged and retrieved from storage. Since Diffie and Hellman^[1] first proposed the concept of the digital signature, some different kinds of digital signature schemes have been proposed, but the security of most are based on either the factoring problem (FAC) or the discrete logarithm problem (DLP). The ElGamal signature scheme^[2] is one of the most well-known and representative schemes in existing digital signature schemes which are based on the DLP. The modified OSS signature scheme^[3] proposed by Naccache is one of the most well-known and representative schemes in existing signature schemes which are based on the FAC. The ElGamal scheme and the modified OSS scheme have remained secure till now.

So far, the FAC and the DLP are still the security bases of many cryptographies and digital signature systems. Therefore, the digital signature schemes based on the factoring problem will become insecure if one day the factoring problem can be solved by a developed efficient algorithm. On the other hand, the digital signature schemes based on the discrete logarithm problem will become insecure if the discrete logarithm problem

can be efficiently broken. Assume that there is a signature scheme of which security is based on both the FAC and the DLP. The scheme will be still secure if any one of the FAC and the DLP is solved. Harn first proposed a digital signature scheme based on the factoring problem and the discrete logarithm problem^[4]. Unfortunately, Lee and Hwang pointed out that the adversary could forge the signatures of Harn's scheme with high probability^[5], if the adversary can solve the discrete logarithm problem. Lai et al. proposed a new digital signature scheme based on two hard problems^[6]. This signature scheme is currently still secure till now. Ref. [7] proposed a digital signature scheme based on two cryptographic assumptions. However, Ou et al. indicated that the scheme is based on only the discrete logarithm problem^[8].

This paper proposes a new signature scheme based on both the factoring problem and the discrete logarithm problem. The security of the proposed scheme is equivalent to the security of the ElGamal scheme if the factoring problem can be solved, and the security of the proposed scheme is equivalent to the security of the modified OSS scheme if the discrete logarithm problem can be solved.

1 Proposed Signature Scheme

In this section, we present a new signature scheme based on two cryptographic assumptions. The scheme consists of three phases: the parameters and keys generation phase, the signature generation phase, and the signature verification phase. We describe the three phases

Received 2007-05-18.

Foundation items: The National Natural Science Foundation of China (No. 60402019), the Science Research Program of Education Bureau of Hubei Province (No. Q200629001).

Biography: Zheng Minghui (1972—), male, graduate, associate professor, mhzheng@smail.hust.edu.cn.

in details as follows.

1.1 Parameters and keys generation phase

A signer or a system firstly chooses several parameters and generates appropriate keys over the finite field $\text{GF}(p)$.

① Let p be a large prime such that $p = 4p_1q_1 + 1$, where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are distinguished large primes.

② Let $n = p_1q_1$ and $g \in \mathbb{Z}_p^*$ such that $g^n \equiv 1 \pmod{p}$, $g^{p_1} \not\equiv 1 \pmod{p}$ and $g^{q_1} \not\equiv 1 \pmod{p}$.

③ Randomly choose x such that $1 < x < n$ and $\gcd(x, p-1) = 1$.

④ Compute $y = g^{x^2} \pmod{p}$.

⑤ Signer publishes y, n, p, q , and keeps x, p_1 and q_1 in secret.

1.2 Signature generation phase

Without loss of generality, m is the message to be signed. In the signature generation phase, the signer performs the following tasks.

① The signer randomly chooses an integer k such that $1 < k < n$ and $\gcd(k, n) = 1$.

② Compute $r \equiv g^k \pmod{p}$.

③ Find t such that $m \equiv x^2 r^2 + kt \pmod{n}$.

④ If $t \in \text{QR}_n$, compute s such that $s^2 \equiv t \pmod{n}$.

⑤ If $t \in \text{QNR}_n$, go to step ①.

Then (r, s) is the signature of the message m .

1.3 Signature verification phase

Any verifier can use public key y to verify the validity of the signature (r, s) for the message m by checking the equation $g^m \equiv y^{r^2} r^{s^2} \pmod{p}$. If the equation holds, the signature (r, s) is valid.

Proof In the signature generation phase, the signature (r, s) of the message m satisfies the equation

$$m \equiv x^2 r^2 + ks^2 \pmod{n}$$

Since $r \equiv g^k \pmod{p}$ and $y = g^{x^2} \pmod{p}$, then

$$g^m \equiv g^{x^2 r^2 + ks^2} \equiv y^{r^2} g^{ks^2} \equiv y^{r^2} r^{s^2} \pmod{p}$$

2 Security Analysis of Proposed Scheme

In this section, we indicate that the security of the proposed signature scheme is equivalent to both the ElGamal signature scheme and the modified OSS signature scheme. We have known that the security of the ElGamal scheme is based on the DLP, and the security of the modified OSS scheme is based on the FAC. In other words, the security of our proposed scheme is based on both the DLP and the FAC. If one day the DLP is broken, the security of our scheme can be transformed into the modified OSS scheme. On the other hand, if one day the FAC is broken, the security of our

scheme can be mapped into the ElGamal digital signature scheme.

First, we claim the proposed scheme is secure and at least based on the factoring problem. If the discrete logarithm problem can be solved, the security of proposed scheme is equivalent to the security of the modified OSS scheme.

We assume the discrete logarithm problem can be solved, and then we can obtain the value x^2 from the public key $y = g^{x^2} \pmod{p}$. Let f be a function to solve the discrete logarithm problem (i. e. $a \equiv g^{f(a)} \pmod{p}$). Thus, $x^2 = f(y)$ and $k = f(r)$. Since $s^2 \equiv t \pmod{n}$, the equation $m \equiv x^2 r^2 + kt \pmod{n}$ can be rewritten as $x^2 r^2 + ks^2 \equiv m^2 \pmod{n}$. By using the function f , we can obtain k from $f(r)$ and it becomes $x^2 r^2 + f(r) s^2 \equiv m^2 \pmod{n}$. To divide by x^2 , we can obtain $r^2 + (f(r)/x^2) s^2 \equiv m^2/x^2 \pmod{n}$. Let $m' = m^2/x^2$ and e be a function such that $e(r) = f(r)/x^2$. The equation then becomes $r^2 + e(r) s^2 \equiv m' \pmod{n}$, where (r, s) is the signature of the message m and m' can be obtained by m if the discrete logarithm problem can be solved. Thus, the verification equation of the proposed signature scheme is just like one in the modified OSS scheme (Note that in the modified OSS scheme, the verification equation is $x^2 + k(x)y^2 \equiv m \pmod{n}$, where (x, y) is the signature of the message m). Therefore, a conclusion can be drawn: if the discrete logarithm problem can be solved, the security of the proposed scheme is equivalent to the security of the modified OSS scheme, of which the security is based on the factoring problem.

Secondly, we claim that the proposed signature scheme is secure and at least based on the discrete logarithm problem. If the factoring problem can be solved, the security of our scheme is equivalent to the security of the modified ElGamal signature scheme.

We assume the factoring problem can be solved, then we can obtain the value p_1, p_2, q_1, q_2 from $n = p_1q_1$ and $p_1 = 2p_2 + 1, q_1 = 2q_2 + 1$, where $n = (p-1)/4$. (Note that we can obtain the value b from $b^2 \equiv a \pmod{n}$ if $a \in \text{QR}_n$ is known and the factoring problem can be solved.) Let $X \equiv x^2 \pmod{n}, M \equiv m^2 \pmod{n}, R \equiv r^2 \pmod{n}$ and $R' = r^2$, where $|R'| = 2|R|, |R'|$ and $|r|$ represent the bit length of R and r . Thus our proposed scheme can be rewritten as follows.

2.1 Parameters and keys generation phase

① Let p be a large prime such that $p = 4p_1q_1 + 1$, where $p_1 = 2p_2 + 1, q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are distinguished large primes.

② Let $n = p_1 q_1$ and $g \in Z_p^*$ such that $g^n \equiv 1 \pmod p$, $g^{p_1} \not\equiv 1 \pmod p$ and $g^{q_1} \not\equiv 1 \pmod p$.

③ Randomly choose X such that $1 < X < n$ and $\gcd(X, p-1) = 1$.

④ Compute $y = g^X \pmod p$.

⑤ Signer publishes y, p , and keeps X in secret.

2.2 Signature generation phase

Without loss of generality, m is the message to be signed. The signer performs the following steps.

① The signer randomly chooses an integer k such that $1 < k < n$ and $\gcd(k, n) = 1$.

② Compute $r \equiv g^k \pmod p$.

③ Find s' such that $M \equiv XR + ks' \pmod{(p-1)}$.

④ If $s' \in \text{QNR}_n$, go to step ①.

Then (r, s') is the signature of the message m .

2.3 Signature verification phase

Any verifier can use public key y to verify the validity of the signature (r, s') for the message m by checking the equation $g^M \equiv y^{r'} R'^\beta \pmod p$, where $\beta \equiv 2^{-1} s'^2 \pmod n$. If it holds, (r, s') is a valid signature of the message m .

After being rewritten, it can be seen that our proposed scheme becomes the ElGamal scheme of which security is based on the discrete logarithm problem. So we can deduce that the security of the proposed scheme is equivalent to the security of the ElGamal scheme if the factoring problem can be solved.

As discussed above, we can deduce indirectly that the security of our proposed scheme is based on two well-known cryptographic assumptions, namely, the discrete logarithm problem and the factoring problem.

3 Performance Evaluation

In this section, we make some comparisons between the proposed scheme and Laih's scheme. Up to now, Laih's scheme has remained secure and more efficient than other existing signature schemes on which security is based on both the factoring problem and the discrete logarithm problem. This is the reason we compare it with our proposed scheme. The following notations are used to facilitate the following comparison.

E_n is the exponentiation computation under the modular n ; I_n is the inverse computation under the modular n ; M_n is the multiplication computation under the modular n ; S_n is the square computation under the modular n ; A_n is the addition computation under the modular n ; H_t is the Hash function $\{0, 1\}^* \rightarrow \{0, 1\}^t$ that has arbitrary length input and t -bit output; $C_{p_1 \times p_2}$

is the Chinese remainder theorem computation under the modular $p_1 \times p_2$; and $|x|$ is the bit-length of an integer x .

The proposed scheme is simpler than other existing schemes based on both the factoring problem and the discrete logarithm problem. We list the comparison results in Tab. 1 and the compared items are the security bases, the needed memory size (bits), the signature bit-length, the computation complexity of the signature generation phase and the computation complexity of the signature verification phase. It can be seen that our proposed scheme outperforms Laih's scheme.

Tab. 1 Comparison between the proposed scheme and Laih's scheme

Items	Laih's scheme	Proposed scheme
Security basis	FAC and DLP	FAC and DLP
Memory size	Public	$3 p + n $
	Private	$2 n $
Signature length	$2 p + 2 n $	$ p + n $
Signature generation		$E_p \times 4$
		$E_p \times 2$
		$I_n \times 4$
		$M_n \times 8$
	$M_n \times (t+8)$	$S_n \times 4$
	$S_n \times 3$	$A_n \times 4$
	$A_n \times 3$	$E_{p_1} \times 5$
	$H_t \times 2$	$E_{q_1} \times 3$
		$C_{p_1 \times p_2} \times 1$
		$E_p \times 4$
Signature verification		$E_n \times t$
	$M_p \times 2$	$E_p \times 3$
	$M_n \times (t+1)$	$M_p \times 1$
	$S_n \times 5$	$S_{p-1} \times 2$
	$H_t \times 2$	

4 Conclusion

This paper proposes a new digital signature scheme on which security is based on two cryptographic assumptions. By security analysis, we can draw a conclusion that the security of the proposed signature scheme combines both the ElGamal signature scheme whose security is based on the discrete logarithm problem and the modified OSS scheme whose security is based on the factoring problem. Compared with previous work based on two cryptographic assumptions, our scheme gains more efficiency in terms of space storage, signature length, and computation complexities.

References

- [1] Diffie W, Hellman M. New directions in cryptography [J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644

- 654.

[2] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. *IEEE Transactions on Information Theory*, 1985, **31**(4): 469 – 472.

[3] Naccache D. Can O. S. S be repaired? Proposal for a new practical signature scheme [C]//*Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*. Heidelberg: Springer-Verlag, 1994: 233 – 239.

[4] Harn L. Public-key cryptosystem design based on factoring and discrete logarithms [J]. *IEE Proceedings on Computers and Digital Techniques*, 1994, **141**(3): 193 – 195.

[5] Lee N Y, Hwang T. Modified Harn signature scheme based on factoring and discrete logarithm [J]. *IEE Proceedings on Computers and Digital Techniques*, 1996, **143** (3): 196 – 198.

[6] Laih C S, Kuo W C. New signature schemes based on factoring and discrete logarithms [J]. *IEICE Transactions on Fundamentals*, 2000, **E80-A**(1): 46 – 53.

[7] He W H. Digital signature scheme based on factoring and discrete logarithms [J]. *Electronics Letters*, 2002, **37** (4): 220 – 222.

[8] Ou Haiwen, Ye Dingfeng, Yang Junhui, et al. On the digital signature schemes whose security based on solving discrete logarithms problem and factoring problem simultaneously [J]. *Journal on Communications*, 2004, **25**(10): 143 – 147. (in Chinese)

一种基于 2 个密码学假定的数字签名方案

郑明辉^{1,2} 崔国华¹

(¹ 华中科技大学计算机科学与技术学院, 武汉 430074)
(² 湖北民族学院计算机科学与技术系, 恩施 445000)

摘要: 为了提高数字签名方案的安全强度, 设计了一个同时基于 2 个难解问题的数字签名方案. 离散对数问题和因式分解问题是密码学中 2 个著名的难解问题, 融合基于离散对数难题的 ElGamal 数字签名方案和基于因式分解难题的 OSS 数字签名方案, 提出了一种安全性同时基于离散对数问题和因式分解问题的数字签名方案. 安全分析得出在一个难题被解的情况下该方案仍然是安全的. 与已有的类似方案比较, 所提出的签名方案具有更短的签名长度, 更低的存储开销和计算开销.

关键词: 数字签名; 安全性; 因式分解问题; 离散对数问题

中图分类号: TP393