Research Article

A New Signature Scheme Based on Multiple Hard Number Theoretic Problems

E. S. Ismail¹ and N. M. F. Tahat²

¹ School of Mathematical Sciences, Faculty of Science and Technology, National University of Malaysia, 43600 Bangi, Selangor, Malaysia

² Department of Mathematics, Faculty of Sciences, The Hashemite University, Zarqa 13133, Jordan

Correspondence should be addressed to E. S. Ismail, esbi75@gmail.com

Received 23 March 2011; Accepted 4 May 2011

Academic Editor: R. Pérez Jiménez

Copyright © 2011 E. S. Ismail and N. M. F. Tahat. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The past years have seen many attempts to construct digital signature schemes based on a single hard problem, like factoring or discrete logarithm. But in the near future, those systems will no longer be secure if the solution of factoring or discrete logarithms problems is discovered. In this paper, we propose a new signature scheme based on two hard number theoretic problems, factoring and discrete logarithms. The major advantage of our scheme is that it is very unlikely that factoring and discrete logarithms can be efficiently solved simultaneously, and; therefore, the security of our scheme is longer or higher than that of any scheme based on a single hard number theoretic problem. We also show that the performance of the scheme requires only minimal operation both in signing and verifying logarithms and is resistant to attack.

1. Introduction

A digital signature scheme is used to authenticate the contents of a digital message, and a valid digital signature tells that the message was generated by a legal/known sender and was not altered during the transmission. Digital signatures are commonly applicable for software distribution, internet-based transactions, forgery detection or tampering. Most digital signature schemes have the common feature that they are based on a single cryptographic assumption [1], like discrete logarithms (DL) [2] or factoring a large composite number problem (FAC) [3]. Although such problems remain difficult to solve today, it is almost inevitable that one day the FAC and DL problems could be solved. As soon as this happens, signatures based on such problems will no longer be secure. This has led researchers to propose digital signature schemes based on multiple hard number theoretic problems [4–9].

The major motivation for this research is that such schemes are more secure than the schemes based on a single hard problem. However, many such schemes have been shown to be insecure [10, 11] due to the use of inappropriate algorithms and weak analysis of security. (See Qian et al. [12]

for details of an example of an insecure signature scheme.) In this paper, we develop a new signature scheme based on a combination of factoring and discrete logarithm problems. We show that the performance of the new scheme is very efficient since it requires acceptable numbers of operations in both signature generation and signature verification.

In the following, Section 2 presents the proposed signature scheme. Section 3 analyzes the resultant security and efficiency from the new scheme, and finally, Section 4 gives our conclusions.

2. The Proposed Signature Scheme

The main purpose of proposing a signature scheme based on two hard problems is to enhance the security of the scheme. The difficulty of simultaneously solving two hard problems is harder than solving a single hard problem. The proposed scheme remains secure even if one can find a solution to one of the underlying problems.

The proposed signature scheme involves the one-to-one interactions between a signer and a verifier to execute the system initialization phase, the key generation phase,

the signature generation phase, and the signature verification phase, described as follows.

2.1. System Initialization Phase. The system initialization phase proceeds with the following commonly required parameters over the defined multiplicative groups. A one-way hash function is applied in the scheme with standard cryptographic characteristics, and to prevent the chosen message attack as defined by ElGamal [2] and Harn [13], the length of the signed message is reducible:

- (1) a cryptographic hash function $h(\cdot)$ whose output is a t -bitlength. In practice, we take $t = 128$;
- (2) a large prime p , and n is a factor of $p - 1$ and also the product of two safe primes, T and L , where $n = TL$. A function defined by $\phi(n) = (T - 1)(L - 1)$ is the phi-Euler function;
- (3) an integer g is a primitive element in $\mathbb{Z}_p^* = \{1, 2, 3, \dots, p - 1\}$ with order n such that $g^n \equiv 1 \pmod{p}$;
- (4) an integer $\alpha \in \mathbb{Z}_n^* = \{v : 1 \leq v \leq n - 1 \text{ and } \gcd(v, n) = 1\}$ is a square modulo n if there exists an $\beta \in \mathbb{Z}_n^*$ such that $\alpha \equiv \beta^2 \pmod{n}$, where $\gcd(a, b)$ denotes the greatest common divisor of a and b .

2.2. Key Generation Phase. In this phase, we do the following steps.

- (1) Pick randomly an integer e from $\mathbb{Z}_{\phi(n)}^*$.
- (2) Calculate the secret number d such that $ed \equiv 1 \pmod{\phi(n)}$.
- (3) Select at random an integer $x \in \mathbb{Z}_p^*$.
- (4) Compute the public number $y \equiv g^x \pmod{p}$.

The public and secret keys of the signature scheme are now, respectively, given by the pairs of (e, y) and (d, x) .

2.3. Signature Generation Phase. To create a signature for the message M , $1 < M < n$, the signer first hashes the message to obtain $h(M)$. Next, the signer randomly chooses a secret integer, r , $1 < r < n$ such that $\gcd(r, n) = 1$ and then computes $K \equiv g^r \pmod{p}$. The signer does the following steps.

- (1) Solve $Kr \equiv y^2 \pmod{n}$ and $x \equiv \xi^2 \pmod{n}$ for γ and ξ .
- (2) Compute $s_1 \equiv (\gamma - \xi h(M))^d \pmod{n}$ and $s_2 \equiv (\gamma + \xi h(M))^d \pmod{n}$.
- (3) Calculate $v \equiv s_1 s_2 \pmod{n}$.

Then the original signer publishes (K, v) as the signature of the message M .

2.4. Signature Verification Phase. The verifier confirms the validity of the signature (K, v) for M as follows.

- (1) Compute $\lambda \equiv v^e \pmod{n}$ and $\eta \equiv h(M)^2 \pmod{n}$.
- (2) Check the equality $g^\lambda \equiv K^K y^{-\eta} \pmod{p}$.

- (3) If the equality in (2) holds, then validates the signature otherwise rejects it.

Theorem 1. *Following the applied protocol, then the verification in the Signature Verification Phase is correct.*

Proof. The equation in (2) in Signature Verification Phase is true for valid signatures since

$$g^\lambda \equiv g^{v^e} \equiv g^{(s_1 s_2)^e} \equiv g^{(y^2 - \xi^2 (h(M))^2)^e} \equiv g^{Kr - x\eta} \equiv K^K y^{-\eta} \pmod{p}. \quad (1)$$

□

3. Security and Performance Analyses

3.1. Security Considerations. Now we will show some possible attacks by which an adversary (Adv) may try to take down the proposed signature scheme. We define each attack and provide an analysis of why each attack would fail.

3.1.1. Attack 1. Adv wishes to obtain all secret keys using all information that is available from the system. In this case, Adv needs to solve FAC and DL problems, which is clearly infeasible.

3.1.2. Attack 2. Adv tries to forge (K, v) via the equation $g^{v^e} \equiv K^K y^{-(h(M))^2} \pmod{p}$, and Adv has to ways two do this. First, he or she fixes the number K , computes $\alpha \equiv K^K y^{-(h(M))^2} \pmod{p}$ and finally solves $g^{v^e} \equiv \alpha \pmod{p}$, for v . Second, he or she fixes the number v , computes $\beta \equiv g^{v^e} y^{(h(M))^2} \pmod{p}$, and solves $K^K \equiv \beta \pmod{p}$ for K . In both scenarios, solving for such numbers is hard due to the difficulty of FAC and DL problems, only successful if Adv can solve the two problems simultaneously.

3.1.3. Attack 3. Adv may also try collecting t valid signatures (K_j, v_j) on message M_j to find the valuable secret keys. In this case, Adv has t equations as follows:

$$v_j^e \equiv K_j r_j - x (h(M_j))^2 \pmod{n}, \quad (2)$$

where $j = 1, 2, \dots, t$. Note that, the above t equations have $(t + 1)$ variables, that is, x and r_j . These secret variables are hard to find because Adv can generate infinite solutions of the above system of equations but cannot figure out which one is correct.

3.1.4. Attack 4. Let us assume that Adv is able to solve the DL problem meaning that, Adv knows the secret integer x . Unfortunately for his efforts, he still does not know d and hence cannot compute the two components s_1 and s_2 , thereby failing to calculate the integer v .

3.1.5. Attack 5. Let us assume that Adv is able to solve the FAC problem, that is, he or she knows the prime factorization of modulus n and can find the number d . However, he cannot compute s_1 and s_2 since no information is known for ξ and thus fails to compute v .

TABLE 1: Definition of given notations.

Notations	Definition
T_{MUL}	Time complexity for executing the modular multiplication
T_{EXP}	Time complexity for executing the modular exponentiation
T_{SRT}	Time complexity for executing the modular square root computation
T_{INV}	Time complexity for executing the modular inverse computation
T_{HAS}	Time complexity for performing hash function

TABLE 2: Time complexity in unit of T_{MUL} for our scheme.

Items	Time complexity	Complexity in T_{MUL}
Key generation	$T_{\text{EXP}} + T_{\text{INV}}$	$240T_{\text{MUL}} + T_{\text{INV}}$
Signature generation	$3T_{\text{EXP}} + 3T_{\text{MUL}} + 2T_{\text{SRT}} + T_{\text{HAS}}$	$963T_{\text{MUL}} + 2T_{\text{SRT}} + T_{\text{HAS}}$
Signature verification	$4T_{\text{EXP}} + 2T_{\text{MUL}} + T_{\text{HAS}}$	$962T_{\text{MUL}} + T_{\text{HAS}}$

3.2. Performance. The performance of our scheme is described in terms of number of keys, computational complexity, and communication costs. We use the following notations (Table 1) to analyze the performance of our scheme.

We ignore the negligible time performing for modular addition. The performance of our proposed signature scheme is summarized as follows: The number of secret keys (SK) and public keys (PK) of the scheme are respectively given by $\text{SK} = 2$ and $\text{PK} = 2$. The computational complexity for the key generation and signing generation and verification is given by the following Table 2, and the last column converts various operation units to T_{MUL} , where $T_{\text{EXP}} = 240T_{\text{MUL}}$ given by Koblitiz et al. [14].

Finally, the communication costs or size of parameters of the scheme (both signature generation and verification) is $7|n| + 2|p|$, where $|a|$ denotes the bitlength of a .

4. Conclusion

In this paper, we have proposed a new signature scheme based on two hard problems; factoring and discrete logarithms. The scheme offers a longer/higher level of security than that of scheme based on a single hard problem. Furthermore, the proposed scheme requires only $963T_{\text{MUL}} + 2T_{\text{SRT}} + T_{\text{HAS}}$ and $962T_{\text{MUL}} + T_{\text{HAS}}$, respectively, for both signature generation and verification. We considered some possible attacks and demonstrated that the proposed scheme would be secure against those attacks.

Acknowledgments

The first author acknowledges the financial support received from the Malaysian Fundamental Research Grant Scheme (FRGS) UKM-ST-07-FRGS0008-2009 and also an anonymous reviewer for their valuable comments.

References

- [1] W. Diffie and M. E. Hellman, "New direction in cryptography," *IEEE Transaction on Information Networking and Application*, pp. 557–560, 1975.
- [2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transaction on Information Theory*, vol. IT-31, no. 4, pp. 469–472, 1985.
- [3] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystem," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [4] W. He, "Digital signature scheme based on factoring and discrete logarithms," *Electronics Letters*, vol. 37, no. 4, pp. 220–222, 2001.
- [5] C. S. Lai and W. C. Kuo, "New signature scheme based on factoring and discrete logarithms," *IEICE Transactions on Fundamentals on Cryptography and Information Security*, vol. 80, no. 1, pp. 46–53, 1997.
- [6] N. Y. Lee and T. Hwang, "Modified Harn signature scheme based on factorising and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques*, vol. 143, no. 3, pp. 196–198, 1996.
- [7] Z. Shao, "Digital signature schemes based on factoring and discrete logarithms," *Electronics Letters*, vol. 38, no. 24, pp. 1518–1519, 2002.
- [8] Z. Shao, "Signature schemes based on factoring and discrete logarithms," *IEE Proceedings Computers and Digital Techniques*, vol. 142, no. 5, pp. 370–372, 1998.
- [9] C. T. Wang and C. C. Chang, "Signature scheme based on two hard problems simultaneously," in *Proceedings of the 17th International Conference on Advanced Information Networking and Application (AINA '03)*, pp. 557–560, Xi'an, China, March 2003.
- [10] M. S. Hwang, C. C. Yang, and S. F. Tzeng, "Improved digital signature scheme based on factoring and discrete logarithms," *Journal of Discrete Mathematical Sciences Cryptography*, vol. 5, no. 2, pp. 152–155, 2002.
- [11] L.-H. Li, S. F. Tzeng, and M. S. Hwang, "Improvement of signature scheme based on factoring and discrete logarithms," *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 49–54, 2005.
- [12] H. Qian, Z. Cao, and H. Bao, "Cryptanalysis of Li-Tzeng-Hwang's improved signature schemes based on factoring and discrete logarithms," *Applied Mathematics and Computation*, vol. 166, no. 3, pp. 501–505, 2005.
- [13] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings: Computers and Digital Techniques*, vol. 141, no. 5, pp. 307–313, 1994.
- [14] N. Koblitiz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes, and Cryptography*, vol. 19, no. 2-3, pp. 173–193, 2000.