Journal of Mathematics and Statistics 4 (4): 222-225, 2008
ISSN 1549-3644

A New Digital Signature Scheme Based on Factoring and Discrete Logarithms

Ismail E.S, N.M.F. Tahat and R.R Ahmad
School of Mathematical Sciences, University Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia

Abstract: Problem statement: A digital signature scheme allows one to sign an electronic message and later the produced signature can be validated by the owner of the message or by any verifier. Most of the existing digital signature schemes were developed based on a single hard problem like factoring, discrete logarithm, residuosity or elliptic curve discrete logarithm problems. Although these schemes appear secure, one day in a near future they may be exploded if one finds a solution of the single hard problem. **Approach:** To overcome this problem, in this study, we proposed a new signature scheme based on multiple hard problems namely factoring and discrete logarithms. We combined the two problems into both signing and verifying equations such that the former depends on two secret keys whereas the latter depends on two corresponding public keys. **Results:** The new scheme was shown to be secure against the most five considering attacks for signature schemes. The efficiency performance of our scheme only requires $1203T_{mul}+T_h$ time complexity for signature generation and $1202T_{mul}+T_h$ time complexity for verification generation and this magnitude of complexity is considered minimal for multiple hard problems-like signature schemes. **Conclusions:** The new signature scheme based on multiple hard problems provides longer and higher security level than that scheme based on one problem. This is because no enemy can solve multiple hard problems simultaneously.

Key words: Cryptology, cryptography, digital signature, factoring, discrete logarithms

INTRODUCTION

In modern cryptography[9], the security of developed signature schemes are based on the hardness of solving some hard number theoretical problems. The schemes stay secure as long as the problem underlies the scheme stay unsolvable. The most used hard problems for someone designing a signature scheme are factoring (FAC)[7] and Discrete Logarithms(DL)[8] problems.

However, it is understood that one day in the future the FAC and DL problems could be solved and when it happens, all signature schemes that depend on one of these problems will no longer be secure. One of the strategies to surmount this situation is by designing a signature scheme based on multiple hard problems. Undoubtedly, the security of such schemes is longer than schemes based on a single problem. This is due to unlikely solving two hard problems simultaneously. Many digital signature scheme have been designed based on both FAC and DL[4,6,11,12] but to design such schemes is not an easy task since many of them have been shown insecure[1-3,5,10]. In this study, we developed a new signature scheme based on the multiple hard problems namely factoring and discrete logarithms.

Some notations: The following parameters and notations will be used throughout this paper unless otherwise specified:

- h (.) cryptographic hash function whose output is a t-bit length. We assume here that t = 128.
- p is a large prime and n is a factor of p-1 that is the product of two safe prime p′ and q′ i.e., n = p′q′.
- An additive group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
- $\phi(n) = (p'-1)(q'-1)$ is a phi-Euler function.
- g is a primitive element in {0,1,2,…,p-1} i.e., the order of g is n which satisfies $g^n \equiv 1 \pmod p$.
- gcd (a,b) is the greatest common divisor of a and b.

MATERIALS AND METHODS

We propose the new digital signature scheme based on factoring and discrete logarithms. The proposed new signature scheme consists of three phases or algorithms: (1) initialization-generating parameters and keys, (2) signing messages, and (3) verifying signature. The

Corresponding Author: Ismail, E.S., School of Mathematical Sciences, University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

signer initializes the scheme by first generating two modulus; a prime p and a composite n = p′q′. The signer next computes public and secret keys of the scheme and publishes the public keys in a public directory and keeps secret keys secretly. In signing phase, the signer signs a message using his secret keys and sends the produced signature to a verifier. Finally, the verifier tests the validity of the signature by using singer's public key which can be accessed from the public directory.

Initialization-generating parameters and keys:

Step 1: Pick randomly an integer e from $\mathbb{Z}_n$ such that gcd (e, n) = 1.
Step 2: Calculate a secret d such that ed ≡ 1 mod ϕ(n).
Step 3: Select at random an integer x from 0 < x < n.
Step 4: Calculate a public key $y \equiv g^x \pmod p$.

Thus the public and secret keys of the system are respectively given by (y, e) and (x, d).

Algorithm for signing messages: Suppose the verifier wants the signer's signature on his message m. The singer then:

Step 1: Select two integer r and u such that r, u < n.
Step 2: Compute $K \equiv g^{h(m)^u} \pmod p$ and $R \equiv g^{h(m)^r} \pmod p$.
Step 3: Calculate $s \equiv (xh(m)+Rh(m)^u+Kh(m)^r)^d \pmod p$.

The original signer then produces (K, R, s) as a signature of message m.

Algorithm for verifying signature: Verifier confirms the validity of the signature (K, R, s) by testing the following equation whether it is holds:

$$g^{s^e} \equiv y^{h(m)} K^R R^K \pmod p \qquad (1)$$

Theorem: If the algorithms of generating parameters and keys and signing messages run smoothly then the validation of signature in verifying signature algorithm is correct.

Proof: The Eq. (1) above is true for valid signature since:

$$g^{s^e} \equiv g^{xh(m)+Rh(m)^u+Kh(m)^r} \equiv g^{xh(m)} g^{Rh(m)^u} g^{Kh(m)^r}$$
$$\equiv g^{xh(m)} \left(g^{h(m)^u}\right)^R \left(g^{h(m)^r}\right)^K \equiv y^{h(m)} K^R R^K \pmod p.$$

RESULTS

In this study, we give our results in terms of security analysis and efficiency performance of our proposed signature scheme based on multiple hard problems.

Security analysis: Now we shall show some possible attacks by which an adversary (Adv) may try to take down the new developed signature scheme. For every attack, we define the attack and give reason why this attack would fail.

Attack 1: Adv wishes to obtain secret keys (x, d) using all information that is available from the system. In this case, Adv needs to solve ed ≡ 1 mod ϕ (n) and $y \equiv g^x \pmod p$ respectively for d and x which are clearly infeasible because the difficulty of solving FAC and DL. Moreover, all secret integers like (p′, q′) will also hard to find.

Attack 2: Adv tries to derive the signature (K, R, s) for a given message M by letting two integers fixed and finding the other one. In this case, Adv randomly select (K, R) or (R, s) or (K, s) and find s or K or R respectively such that the Eq. 1 satisfied. For example, say Adv fixes the values (K, R) and tries to figure out the value of s. Adv starts by computing $\alpha \equiv y^{h(m)} K^R R^K \pmod p$ and solve $g^{s^e} \equiv \alpha \pmod p$ for s. Unfortunately, s can only be found if both FAC and DL are breakable.

Say that DL is breakable, then Adv knows s^e but still cannot figure out the value of s since he or she learns nothing about d. In this case too, the breakable of FAC does not help the Adv at all. The rest of two cases go similarly.

Attack 3: Adv may also try collecting w valid signature (K_j, R_j, s_j) on message m_j where j = 1, 2, …, w and attempts to find secret keys and number of the signature scheme. In this case, Adv has w equations as follows:

$$s_1^e \equiv xh(m_1) + R_1 h(m_1)^{u_1} + K_1 h(m_1)^{r_1} \pmod n$$
$$s_2^e \equiv xh(m_2) + R_2 h(m_2)^{u_2} + K_2 h(m_2)^{r_2} \pmod n$$
$$\vdots$$
$$s_w^e \equiv xh(m_w) + R_w h(m_w)^{u_w} + K_w h(m_w)^{r_w} \pmod n.$$

In the above w equations, there are (2w+1) variables namely x, u_j and r_j where j = 1, 2, …, w which are not known by the Adv. Hence, x stays hard to detect

because Adv can generate infinite solutions of the above system of equations but cannot figure out which one is correct.

Attack 4: It is assumed that Adv is able to solve DL problem. In this case, Adv knows x but cannot compute s because he does not know d (difficulty of breaking FAC).

Attack 5: It is assumed that Adv is able to solve FAC problem. Thus, he knows the prime factorization of n. In this case, Adv knows d but still cannot calculate the third component signature, s because he or she does not know the value of x due to the difficulty of breaking DL.

Performance evaluation: Next, we investigate and discuss the performance of our scheme in terms of number of keys, computational complexity and communication cost. The following notations are used to analyse the performance of the scheme.

- SK and PK are the number of secret and keys respectively,
- T_{exp} is the time complexity for modular exponentiation,
- T_{mul} is the time complexity for modular multiplication,
- T_{inv} is the time complexity for a modular inverse computation,
- T_h is the time complexity for performing a one-way hash h (.),
- |x| denotes the bit length of x.

In this evaluation, we ignore the time for performing modular addition and subtraction computations and the probability of the bit being 0 or 1 is 1/2. The Table 1 shows the efficiency of our scheme. From the Table 1, the signer performs only $1203T_{mul}+T_h$ time complexity to issue a signature and the verifier needs only $1202T_{mul}+T_h$ time complexity to validate the received signature using the conversion $T_{exp} = 240T_{mul}$.

Table 1: The performance of the new signature scheme

		Our new signature scheme
The number of keys	SK	2
	PK	2
Computational complexity	Signing	$5T_{exp}+3T_{mul}+T_h$
	Verifying	$5T_{exp}+2T_{mul}+T_h$
Communication cost		$3\|n\|+4\|p\|$

DISCUSSION

Most of the designated signature schemes are based on a single hard problem. Although these schemes secure but in a near future if an adversary manages to solve this problem, he then can recover all secret information including secret keys and parameters of the scheme. These include the schemes of Rivest *et al.*[7] and ElGamal[8].

Our scheme is prevented from this type of problem. This is because, the scheme is designed on two hard problems namely factoring and discrete logarithm problems. To break the scheme, the enemy has to solve the two problems simultaneously, which is impossible. Next, our scheme is protected from five attacks and these attacks are the most common considering attacks for signature schemes. The performance analysis of the scheme reveals that the signature process needs $1203T_{mul}+T_h$ time complexity whereas the verification process requires $1202T_{mul}+T_h$. The higher time complexity is contributed by the use of two hard problems but yet the scheme provides longer security than schemes on a single problem.

CONCLUSION

In this study, we presented a new digital signature scheme based on factoring and discrete logarithms. The proposed scheme requires less than $1203T_{mul} + T_h$ time complexities in both signing and verifying algorithms. Some possible attacks have also been considered and we have shown that our scheme secure from those attacks.

ACKNOWLEDGMENT

The first author acknowledges the financial support received from the Universiti Kebangsaan Malaysia through the OUP grant UKM-OUP-NBT-29-153/2008.

REFERENCES

1. Laih, C.S. and W.C. Kuo, 1997. New signature scheme based on factoring and discrete logarithms. IEICE Trans. Fundamentals Cryptography Inform. Sec., 80: 46-53.
2. Wang, C.T., C.H. Lin and C.C. Chang, 2003. Signature scheme based on two hard problems simultaneously. Proceedings of the 17th International Conference on Advanced Information Networking and Application, Mar. 27-29, IEEE Computer Society, Washington, DC, USA., pp: 557. http://portal.acm.org/citation.cfm?id=784562

3. Qian, H., Z. Cao and H. Bao, 2005. Cryptography of Li-Tzeng-Hwang's improved signature schemes based on factoring and discrete logarithms. Applied Math. Comput. 166: 501-505. http://cat.inist.fr/?aModele=afficheN&cpsidt=16902836.
4. Harn, L., 1994. Public key cryptosystem design based on factoring and discrete logarithms. IEE Proceeding of Computers Digital Techniques, May, 1994, IEEE Xplore, USA., pp: 193-195. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=287062&isnumber=7148.
5. Hwang, M.S., C.C. Yang and S.F. Tzeng, 2002. Improved digital signature scheme based on factoring and discrete logarithms. J. Discrete Math. Sci. Cryptograph., 5: 152-155.
6. Lee, N.Y. and T. Hwang, 1996. Modified Harn signature scheme based on factoring and discrete logarithms. IEE Proceeding of Computers Digital Techniques, May, 1996, IEEE Xplore, USA., pp: 196-198. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=503291&isnumber=11071.
7. Rivest, R., A. Shamir and L. Adleman, 1978. A method for obtaining digital signature and public-key cryptosystem. Commun. ACM., 21: 120-126. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.5588.
8. ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans. Inform. Theory IT, 31: 469-472. http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C84/10.PDF.
9. Diffie, W. and M.E. Hellman, 1976. New direction in cryptography. IEEE Trans. Inform. Theory IT, 22: 644-654. http://citeseer.ist.psu.edu/old/diffie76new.html.
10. He, W.H., 2001. Digital signature scheme based on factoring and discrete logarithms. Electronic Lett., 37: 220-222. DOI: 10.1049/el:20010149.
11. Shao, Z., 1998. Signature schemes based on factoring and discrete logarithms. IEE Proceeding of Computers Digital Techniques, Jan. 1998, Institution of Electrical Engineers, Great Britain, pp: 33-36. http://direct.bl.uk/bld/PlaceOrder.do?UIN=039375114&ETOC=RN&from=searchengine.
12. Shao, Z., 2002. Digital signature schemes based on factoring and discrete logarithms. Electronic Lett., 38: 1518-1519. DOI: 10.1049/el:20021093.