International Journal of Cryptology Research 4(1): 32 - 41 (2013)

Threshold Signature with Hybrid Problems

[1]Mohd Saiful Adli Mohamad and [2]Eddie Shahril Ismail

School of Mathematical Sciences,
Faculty of Science and Technology,
Universiti Kebangsaan Malaysia,
43600 Bangi, Selangor, Malaysia

E-mail: msadli@uum.edu.my and esbi@ukm.my

*Corresponding author

ABSTRACT

The digital signature schemes with hybrid problems are rapidly developed recently, since it is understood that the single-problem scheme will no longer be secure in near future. Meanwhile, the concept of group-oriented cryptography, known as threshold cryptography, gives a new dimension in development of signature scheme. In this paper, we present a new threshold signature scheme based on two hard number theoretical problems; residuosity and discrete logarithm. The advantage of our scheme is based on the assumption that it is very unlikely to solve two hard number theoretical problems simultaneously. We also show that our scheme is secure against some cryptographic attacks and also significantly efficient compare with threshold signature scheme based on single problem.

Keywords: digital signature schemes, group-oriented cryptography, theoretical problems; residuosity and discrete logarithm.

1. INTRODUCTION

A digital signature scheme is a mathematical scheme that being used to authenticate the contents of an online message or document. Digital signatures are widely used for software distribution, internet-based transactions, electronic commerce, online file movement system, etc. In general, a digital signature scheme must satisfy the following properties: i) authentic, ii) not forgeable, iii) not reusable, iv) unalterable, and v) non-repudiated.

After Diffie and Hellman (1976) introduced the concept of public-key cryptography, many digital signature schemes have being developed based on various number theory problems such as factoring (Rivest *et. al.* (1978)), residuosity (Rabin (1979)), discrete logarithm (ElGamal (1985)), and elliptic curve (Koblitz (1987); Miller (1985)). Although the single-

problem schemes remain unsolved today, but it is understood that in the future, the problems could be solved. When it happens, the single-problem schemes will no longer be secure. That's the reason why recent digital signature schemes were developed based on hybrid problems (Lee and Hwang (1996); Laih and Kuo (1997); He (2001); Wang *et. al.* (2003); Ismail *et. al.* (2009)).

Nowadays, many electronic documents need to be signed by more than one person. This problem brings the idea of society-oriented cryptography, which is known as threshold cryptography (Desmedt (1988)). The development of threshold cryptosystem (Desmedt and Frankel (1989)) use the concept of Shamir's secret sharing (Shamir (1979)), which is based on Lagrange interpolation technique. Then, in 1991, Desmedt and Frankel proposed the first (t, n) threshold digital signature scheme based on the RSA assumption (Desmedt and Frankel (1991)), while Harn proposed another (t, n) threshold digital signature scheme from modified ElGamal scheme (Harn (1994)).

In (t, n) threshold digital signature schemes (Desmedt and Frankel, (1991); Harn (1994); Wang *et. al.* (1998); Lee and Chang (1999)), any t out of n signers is required to sign an online message or document, while a single verifier can validate the group signature with the signers' group public key. Apart from such schemes, there were also schemes with single signer and (k, l) verifiers (Harn (1993); Hoster *et. al.* (1995)) and schemes that integrate both ideas (Wang *et. al.* (2000); Hsu *et. al.* (2002)).

2. PROPOSED THRESHOLD SIGNATURE SCHEME

In this paper, we propose a new threshold signature scheme based on two hard number theoretical problems; residuosity and discrete logarithm. The security of our scheme is based on the assumption that it is difficult to solve both problems simultaneously. In our scheme, t out of n signers can collaboratively sign the message on behalf of the group, while a single verifier can validate the group signature.

In this scheme, a trusted dealer (TD) is required to generate the parameters and keys for the signers' group and verifier. Before generates the secret and public keys, TD sets the following parameters that will be used throughout this scheme:

(i) $h(m)$ - the one-way hash function for the message m.
(ii) p - a 1024-bits prime number.
(iii) $N = PQ$ - a factor of $p - 1$, where P and Q are two safe primes.
(iv) g - a generator of order N, satisfying $g^N \equiv 1 \pmod{p}$.

Step 1: Generating Keys

In this phase, TD performs the following actions to generate the secret and public keys of the scheme:

1. Picks randomly $e \in \mathbb{Z}_N^*$ such that $\gcd(e^2, N) = 1$.
2. Calculates $w \equiv g^{e^2} \pmod{p}$.
3. After that, constructs a (t, n) threshold function,

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{N},$$

where a_i are random integers between 1 and $N - 1$, and $i = 0,1,2, \ldots, t - 1$.
4. Sets the group secret key, $P(0) = a_0$, and calculates the corresponding group public key, $V \equiv g^{P(0)} \pmod{p}$.
5. Sets a pair $(x_i, P(x_i))$ for each signer, where x_i is the public identity and $P(x_i)$ is the secret key for each signer.
6. Computes the corresponding individual public key $y_i \equiv g^{P(x_i)} \pmod{p}$ for each signer.

The public and secret keys for individual and group for the scheme are shown in Table 1.

TABLE 1: The public and secret keys of the scheme.

	Public key	Secret key
Individual	y_i	$P(x_i)$
Group	w, V	$e, P(0)$

Step 2: Signing message

Let $U = \{u_1, u_2, \ldots, u_n\}$ denoted as the n-signer group. Any t out of n signers can represent the group to sign the message. Before they collaboratively sign the message, they appoint one of them as a clerk to verify the partial signature. Here, the steps of signing the message are described.

1. Each signer selects r_i such that $0 < r_i < N$ and $\gcd(r_i, N) = 1$.
2. Computes $k_i \equiv g^{r_i} \pmod{p}$.
3. Broadcasts k_i to other signers via secure channel. After all k_i are received, each of them calculates $K \equiv \prod_{i=1}^{t} k_i \pmod{p}$.
4. By using the information of the public identity x_i of other participating signers, each of them calculates $v_i \equiv \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-x_j}{x_i - x_j} \pmod{N}$.
5. Calculates $s_i \equiv K \cdot r_i + h(m) \cdot P(x_i) \cdot v_i \pmod{N}$.
6. Sends K and v_i along with (k_i, s_i) as the partial signature for the hash-function message $h(m)$ to the clerk. Then, the clerk checks the validity of the partial signature by showing that the following equality holds:

$$g^{s_i} \equiv {k_i}^{K} \cdot {y_i}^{v_i \cdot h(m)} \pmod{p}.$$

7. After the clerk shows that all partial signatures are valid, then he solves $S^2 \equiv e^{-2} \sum_{i=1}^{t} s_i \pmod{N}$ for S. He produces (K, S) as the group signature for the hash-function message $h(m)$.

Step 3: Verifying signature

Any outsider can verify the signature, as long as he has access to the public key. After he receives the group signature (K, S), he checks

$$w^{S^2} \equiv K^K \cdot V^{h(m)} \pmod{p}.$$

If the equation holds, then the group signature is valid.

Theorem 1. *Following the applied protocol, then the verification in the signature verification phase is true.*

Proof:

The equation in signature verification phase is true for valid signature since,

$$\begin{aligned} w^{S^2} &\equiv \left(g^{e^2}\right)^{e^{-2} \sum_{i=1}^{t} s_i} && \pmod{p} \\ &\equiv g^{\sum_{i=1}^{t} s_i} && \pmod{p} \\ &\equiv g^{\sum_{i=1}^{t} K \cdot r_i + \sum_{i=1}^{t} h(m) \cdot P(x_i) \cdot v_i} && \pmod{p} \\ &\equiv \left(g^{\sum_{i=1}^{t} r_i}\right)^{K} \left(g^{\sum_{i=1}^{t} P(x_i) v_i}\right)^{h(m)} && \pmod{p} \end{aligned}$$

$$\equiv \left(\prod_{i=1}^{t} k_i\right)^{K} (g^{a_0})^{h(m)} \pmod{p}$$
$$\equiv K^K \cdot V^{h(m)} \pmod{p}$$

3. SECURITY ANALYSIS

It is important to make sure that a signature scheme that has being developed is secure against some cryptographic attacks. To show the security, we will test our threshold signature scheme with some security attacks and show that the scheme is heuristically secure. In general, we consider the following attacks:

Attack 1 (The key-only attack)

(i) Adversary (Adv) wishes to obtain group secret keys e and $P(0)$ by using all information from the system. In this case, Adv needs to solve $w \equiv g^{e^2} \pmod{p}$ and $V \equiv g^{a_0} \pmod{p}$, which are clearly infeasible due to the difficulty of solving residuosity and discrete logarithm problems simultaneously.

(ii) Adv also cannot derive the individual secret key, $P(x_i)$ from the equation $y_i \equiv g^{P(x_i)} \pmod{p}$ due to the difficulty of solving DLP.

Attack 2 (The feed attack)

Adv might try to derive their own group signature (K, S) from the verifying equation $w^{S^2} \equiv K^K \cdot V^{h(m)} \pmod{p}$ for a given message m by letting one integer fixed and finding the other one. We can divide this attack into two cases:

(i) Adv selects K and tries to figure out the value of S. In this case, Adv calculates $\lambda \equiv K^K \cdot V^{h(m)} \pmod{p}$. Then, he has to solve $\lambda \equiv w^{S^2} \pmod{p}$. Unfortunately, he cannot find S from this equation due to the difficulty of solving residuosity and discrete logarithm problems simultaneously.

(ii) Adv also might try to fix S and find K. In this case, he calculates $\gamma \equiv w^{S^2} \cdot V^{-h(m)} \pmod{p}$ and tries to solve $\gamma \equiv K^K \pmod{p}$. This is worse scenario because even both residuosity and discrete logarithm problems are solvable, the value of K still hard to find except by try and error, but it is time consuming.

Attack 3 (The chosen message-signature attack)

Adv may also try collecting t pairs of message-signature (k_{ij}, s_{ij}) and m_j, where $j = 1, 2, \dots, t$ and attempts to find the individual secret key $P(x_i)$. In this case, Adv has t equations as follows:

$$\begin{aligned} s_{i1} &\equiv K_1 \cdot r_{i1} + h(m_1) \cdot P(x_i) \cdot v_i \pmod N \\ s_{i2} &\equiv K_2 \cdot r_{i2} + h(m_2) \cdot P(x_i) \cdot v_i \pmod N \\ &\vdots \\ s_{it} &\equiv K_1 \cdot r_{it} + h(m_t) \cdot P(x_i) \cdot v_i \pmod N \end{aligned}$$

In the above t equations, there are $(t + 1)$ unknowns, i.e., $P(x_i)$ and r_{ij}. Hence, $P(x_i)$ stays hard to detect because Adv can generate infinite number of solutions of the above system of linear equations but cannot figure out which one is correct.

Attack 4 (The residuosity attack)

It is assumed that Adv is able to solve residuosity problem. In this case, he knows the prime factorization, P and Q. Then he tries to solve the equation $\lambda \equiv w^{S^2} \pmod p$. However, he still cannot find S from this equation because he does not know $S^2 \pmod N$ since discrete logarithm problem is not solvable.

Attack 5 (The discrete logarithm attack)

Suppose that discrete logarithm problem is solvable.

(i) From the equation $\lambda \equiv w^{S^2} \pmod p$ Adv can find $\mu \equiv S^2 \pmod N$. However, he still cannot find S due to the difficulty of solving residuosity problem.

(ii) Adv might also try to find all secret keys of the signers from the equation $y_i \equiv g^{P(x_i)} \pmod p$. Since discrete logarithm problem is solvable, then he can find all secret keys $P(x_i)$ and then create all partial signatures of the group. But he cannot compute the group signature S from the equation $S^2 \equiv e^{-2} \sum_{i=1}^{t} s_i \pmod N$ because he does not know the prime factorization of N.

Attack 6 (The impersonate-member attack)

Adv might try to impersonate signer u_i by randomly selects an integer r_i and broadcasting $k_i \equiv g^{r_i} \pmod{p}$. Since the group signature is determined by all t signers, without knowing the individual secret key $P(x_i)$, Adv cannot generate a valid partial signature (k_i, s_i) to satisfy the verification equation.

4. PERFORMANCE ANALYSIS

In previous section, we already show that our scheme is secure against some cryptographic attack. Another evaluation for a signature scheme is efficiency analysis. In this analysis, we investigate the performance of our scheme in terms of number of secret and public keys, computational complexity for both signing and verifying phases, and communication cost. Then, we compare the efficiency of our scheme with the single-problem threshold signature scheme based on discrete logarithm problem proposed by Harn (1994). The reason of choosing scheme by Harn (1994) to be compared is only such scheme has similar properties with our scheme.

The efficiency of our scheme and the comparison are shown in Table 2. We use the following notations to analyze the performance of the scheme:

- SK and PK are the number of secret and public keys respectively.
- T_{exp} is the time complexity for executing the modular exponentiation computation.
- T_{mul} is the time complexity for executing the modular multiplication computation.
- T_{inv} is the time complexity for executing the modular inverse computation.
- T_{sq} is the time complexity for executing the modular square computation.
- T_{sqrt} is the complexity for executing the modular square root computation.
- T_h is the time complexity for performing hash function.
- $|\eta|$ denotes the bit length of η.

5. CONCLUSION

In this paper, we proposed a new threshold signature scheme based on residuosity and discrete logarithm problems. The advantage of our scheme is based on the assumption that it is infeasible to solve two hard number theory problems simultaneously. From the security and performance analysis, it is shown that our scheme is secure against some cryptographic attack and significantly efficient compare with the scheme based on single problem.

TABLE 2: The performance of our scheme and the comparison

		Our scheme	Harn's scheme
No of keys	SK	$t+2$	$t+1$
	PK	$t+2$	$t+1$
Computational complexity	Sign	$(4t)\ T_{exp} +$ $(3t^2+t+1)\ T_{mul} +$ $(t^2-t+1)\ T_{inv} + T_{sq} +$ $T_{sqrt} + T_h$	$(4t)T_{exp}$ $+ (5t^2-2t)T_{mul}$ $+ 2(t^2-t)T_{inv} + T_h$
	Verify	$3\ T_{exp} + T_{mul} + T_{sq}$	$3T_{exp} + T_{mul}$
Size of parameters/ communication cost		$(2t+1)\|N\| + (3t+1)\|p\|$	$(t+1)\|N\|$ $+ (3t+1)\|p\|$

REFERENCES

Diffie, W., and Hellman, M. E. (1976). New direction in cryptography. *IEEE Transaction on Information Theory*. **IT-22**: 644-654.

Rivest, R., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signature and public-key cryptosystem. *Communication of the ACM*. **21**(2): 120-126.

Rabin, M. O. (1979). Digitalized signatures and public key cryptosystems as intractable as factorization. *Technical report MIT/LCS/TR-212*. MIT, Cambridge, MA.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory*. **IT-31**(4): 469-472.

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

Laih, C. S. and Kuo, W. C. (1997). New signature scheme based on factoring and discrete logarithms. *IEICE Transactions on Fundamentals on Cryptography and Information Security*. **E80-A**(1): 46-53.

He, W. H. (2001). Digital signature scheme based on factoring and discrete logarithms. *Electronic Letters*. **37**(4): 220-222.

Wang, C. T., Lin, C. H. and Chang, C. C. (2003). Signature scheme based on two hard problems simultaneously. *Proceedings of the 17th International Conference on Advanced Information Networking and Application*. 557-560.

Ismail, E. S., Tahat, N. M. F. and Ahmad, R. R. (2009). A new signature scheme based on factoring and discrete logarithms. *Journal of Discrete Mathematical Sciences & Cryptography*. **12**(3): 313-318.

Desmedt, Y. (1988). Society and group oriented cryptography: a new concept. *Advances in Cryptology, Proceedings of Crypto '87*. 120-127.

Desmedt, Y. and Frankel, Y. (1989). Threshold cryptosystem. *Advances in Cryptology, Proceedings of Crypto '89*. 307-315.

Desmedt, Y. and Frankel, Y. (1991). Shared generation of authenticators. *Advances in Cryptology, Proceedings of Crypto '91*. 457-469.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*. **22**(11): 612-613.

Harn, L. (1994). Group oriented (*t*,*n*) threshold digital signature scheme and digital multisignature. *IEE Proceedings-Computers and Digital Techniques*. **141**(5): 307-313.

Wang, C. T., Lin, C. H. and Chang, C. C. (1998). Threshold signature schemes with traceable signers in group communications. *Computer Communications*. **21**(8): 771-776.

Lee, W. B. and Chang, C. C. (1999). (*t*,*n*) threshold digital signature with traceability property. *Journal of Information Science and Engineering*. **15**: 669-678.

Harn, L. (1993). Digital signature with (*t*,*n*) shared verification based on discrete logarithms. *Electronic Letters*. **29**(24): 2094-2095.

Horster, P., Michels, M. and Peterson, H. (1995). Comment on "Digital signature with (*t*,*n*) shared verification based on discrete logarithms". *Electronic Letters*. **31**(14): 1137

Wang, C. T., Chang, C. C. and Lin, C. H. (2000). Generalization of threshold signature and authenticated encryption for group communications. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*. **E83-A**(6): 1228-1237.

Hsu, C. L., Wu, T. S. and Wu, T. C. (2002). Improvements of generalization of threshold signature and authenticated encryption for group communications. *Information Processing Letters*. **81**(1): 41-45.