Applied Mathematical Sciences, Vol. 8, 2014, no. 31, 1499 - 1507
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.4142

A Threshold Authenticated Encryption Scheme Using Hybrid Problems

M. S. A. Mohamad

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

E. S. Ismail

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

Abstract

In this paper, we propose a threshold authenticated encryption scheme using both factoring and discrete logarithm problems. We apply the concept of threshold cryptography in the verification and message recovery phase, where *t* out of *n* recipients are required to verify and recover the message. Security analysis shows that our scheme will remain secure even if one of these problems can be solved.

Keywords: Authenticated Encryption, Threshold Cryptography, Factoring, Discrete Logarithm

1 Introduction

An authenticated encryption scheme is a cryptographic scheme that ensures the confidentiality, integrity and authenticity of online documents or messages by allowing the user to sign and encrypt a message at the same time. In such a scheme, the receiver can not only recover the message sent, but also verify the message. By combining the digital signature scheme and the encryption scheme into a single scheme, communication and operation costs can be less than when performing both schemes separately [1].

Diffie and Hellman's [2] introduction of the concept of public-key cryptography has led to the development of a number of digital signature schemes based on various problems in number theory, such as factoring [3], discrete logarithm [4], quadratic residue [5], and elliptic curve [6, 7]. However, if one of the problems can be solved, then the single-problem scheme will not be secure. To overcome this problem, digital signature schemes using two problems have been proposed [8, 9, 10, 11, 12]. Furthermore, two-problem or hybrid-problem schemes are also suitable for applications that need long-term security [13].

The idea of developing an authenticated encryption scheme emerged from the modification of the digital signature. Nyberg and Rueppel [14] proposed a modified version of the Digital Signature Algorithm to facilitate message recovery. However, their scheme allowed only a single signer and a single verifier in the signing and verifying phases. Since then, the development of an authenticated encryption scheme has turned to multiple-participant society-oriented cryptography, also known as threshold cryptography [15, 16]. Hsu and Wu [17], for example, presented an authenticated encryption scheme with (*t*, *n*) shared verification, and Wang et. al. [18], Hsu et. al. [19], and Chen et. al [1] developed schemes with (*t*, *n*) signers and (*k*, *l*) verifiers.

All authenticated encryption schemes reviewed here were developed using a single number theory problem. In this paper, considering the need for long-term security, we develop a threshold authenticated encryption scheme using two number theory problems: factoring and discrete logarithm. The security of our scheme arises from the difficulty of solving both problems simultaneously. We show that our scheme remains secure, even when one of the problems is solved.

2 The Proposed Authenticated Encryption Scheme

In this paper, a hybrid problem-based authenticated encryption scheme is proposed. Like all authenticated encryption schemes, the proposed scheme comprises the following phases:

1. generating parameters and keys;
2. signing and encrypting message; and
3. verifying and decrypting the message.

Phase 1: Generating parameters and keys

In this phase, the system authority generates the keys that will be used throughout the scheme. Before s/he generates the secret and public keys for senders and receivers, s/he will set the following parameters:

i. p - a 1024-bits prime.
ii. $N = ab$ - a factor of $p - 1$, where a and b are two safe primes.
iii. $\overline{N} = \bar{a}\bar{b}$ - a factor of $p - 1$, where $\bar{a}$ and $\bar{b}$ are two safe primes.
iv. $\phi(N)$ - Euler's phi function of N.

v. $\phi(\bar{N})$ - Euler's phi function of $\bar{N}$.
vi. g - a generator of $\mathbb{Z}_p^*$ of order N.

In our scheme, a single sender and many receivers are involved in both signing/encrypting and verifying/decrypting phases. The system authority generates the secret and public keys for both sender and group of receivers, and then sets the threshold polynomial functions to share the secret keys for the receivers. In the key generation procedure, the system authority

1. picks an integer $e \in \mathbb{Z}_N^*$ such that $\gcd\big(e, \phi(N)\big) = 1$ and then calculates d from $ed = 1 \pmod{\phi(N)}$;
2. picks another integer $\alpha \in \mathbb{Z}_{\bar{N}}^*$ such that $\gcd\big(\alpha, \phi(\bar{N})\big) = 1$ and then calculates β from $\alpha\beta = 1 \pmod{\phi(\bar{N})}$;
3. constructs two threshold polynomial functions
$$f_1(x) = d + d_1 x + d_2 x^2 + \cdots + d_{t-1} x^{t-1} \pmod{N}$$
$$f_2(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{N}$$
4. sets $\big(x_i, f_1(x_i), f_2(x_i)\big)$ for each recipient, where x_i is the public identity, while $f_1(x_i)$ and $f_2(x_i)$ are the secret shares for each recipient;
5. sets a secret key for the group of recipients $f_2(x_0) = a_0$, where $a_0 \in \mathbb{Z}_N^*$ and the corresponding public key $y_v = g^{a_0} \pmod{p}$; and
6. sets a secret key for the signer $x_s \in \mathbb{Z}_N^*$ and the corresponding public key $y_s = g^{x_s} \pmod{p}$.

The summary of secret and public keys for sender and receivers is given in Table 1.

Table 1: Secret and public keys for sender and receivers

	Secret keys	**Public keys**
Sender	x_s, β	y_s, α
Receivers	$f_1(x_i), f_2(x_i)$	e, y_v

Phase 2: Signing and encrypting message

To sign and encrypt a message M, the sender

1. chooses a one-time secret integer k such that $0 < k < N$ and $\gcd(k, N) = 1$;
2. calculates $r = Mg^{-k} \pmod{p}$ and $s = k - x_s r \pmod{N}$;
3. generates the signature-ciphertext (c_1, c_2, c_3), where

$$c_1 = (r y_v^{-k})^e \pmod{p},$$
$$c_2 = g^k \pmod{p},$$
$$c_3 = s^\beta \pmod{\bar{N}}; \text{ and}$$

4. sends (c_1, c_2, c_3) to the recipients.

Phase 3: Verifying and decrypting message

Upon receiving (c_1, c_2, c_3) from the sender, t out of n recipients execute the following steps to verify and recover the message:

1. From the individual secret key $f_1(x_i)$ and $f_2(x_i)$, each of them calculates

$$\alpha_i = {c_1}^{f_1(x_i)} {c_2}^{f_2(x_i)} \pmod{p}$$

and then sends α_i along with the public identity x_i to the other participants through a secure channel.

2. After all participants receive α_i and x_i from the other participants, they calculate

$$r = \prod_{i=1}^{t} {\alpha_i}^{L_i} \pmod{p}$$

and

$$s = {c_3}^{\alpha} \pmod{\bar{N}}$$

where

$$L_i = \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{-x_j}{x_i - x_j} \pmod{N}.$$

3. Then, the message M can be recovered by computing

$$M = g^s {y_s}^r r \pmod{p}.$$

The recovered M can be verified by checking the validity of the redundancy within it.

Theorem 1. *If the algorithms in Phases 1 and 2 run smoothly, then the decryption of the encrypted message in Phase 3 is correct.*

***Proof*:**

All equations in Phase 3 are true for all (c_1, c_2, c_3) since:

1. Calculation of r.

$$\prod_{i=1}^{t} {\alpha_i}^{L_i} = \prod_{i=1}^{t} \left({c_1}^{f_1(x_i)} \cdot {c_2}^{f_2(x_i)}\right)^{L_i} = \prod_{i=1}^{t} {c_1}^{f_1(x_i)L_i} \cdot {c_2}^{f_2(x_i)L_i}$$

$$= \prod_{i=1}^{t} {c_1}^{f_1(x_i)L_i} \prod_{i=1}^{t} {c_2}^{f_2(x_i)L_i} = {c_1}^{\sum_{i=1}^{t} f_1(x_i)L_i} \cdot {c_2}^{\sum_{i=1}^{t} f_2(x_i)L_i}$$

$= {c_1}^d \cdot {c_2}^{a_o} = (r{y_v}^{-k})^{ed} \cdot (g^k)^{a_0} = rg^{-a_0 k} \cdot g^{a_0 k} = r \pmod p.$

2. Calculation of s.
   ${c_3}^{\alpha} = \left(s^{\beta}\right)^{\alpha} = s(\mathrm{mod}\ \bar{N}).$

3. Recovering the message.
   $g^s {y_s}^r r \equiv g^{k - x_s r} \cdot g^{x_s r} \cdot r \equiv g^k \cdot g^{-x_s r} \cdot g^{x_s r} \cdot M g^{-k} \equiv M(\mathrm{mod}\ p)$

3 Security Analysis

In this section, we show that our scheme is heuristically secure against some cryptographic attacks. We consider the following attacks:

Attack 1

(i) Suppose that the adversary (Adv) tries to obtain the secret keys for the sender (β, x_s) from the equations $\alpha\beta \equiv 1 \left(\mathrm{mod}\ \phi(\bar{N})\right)$ and $y_s \equiv g^{x_s} \pmod p$. It is clearly infeasible due to the difficulty of solving factoring and discrete logarithm problems.

(ii) Adv also might try to derive the secret keys for the recipients (d, a_0) from the equations $ed \equiv 1 \left(\mathrm{mod}\ \phi(N)\right)$ and $y_v \equiv g^{a_0} \pmod p$. However, without solving factoring and discrete logarithm problems, s/he will never succeed in deriving the secret keys from both equations.

Attack 2

Adv discovers the value of s from the equation $s \equiv {c_3}^{\alpha} \pmod{\bar{N}}$ and then tries to obtain the secret key x_s from the equation $s \equiv k - x_s r \pmod N$. Since k is a one-time secret integer and r can only be discovered if both factoring and discrete logarithm problems are solvable, extracting the secret key x_s from the equation $s \equiv k - x_s r \pmod N$ will always be infeasible.

Attack 3

Assume that the factoring problem is solvable.

(i) Adv could find the secret key for the sender β and try to generate the signature-ciphertext (c_1, c_2, c_3) of a fake message. However, without knowing another secret key x_s, which can only be obtained if the discrete logarithm problem is solvable, Adv cannot calculate s and fails to generate c_3 from the signature-ciphertext.

(ii) Adv also could find the secret key d and try to recover the message from the signature-ciphertext (c_1, c_2, c_3). However, without solving the discrete logarithm problem, s/he cannot find another secret key a_0. Thus, the value of r remains concealed and Adv's attempt to recover the message from the equation $M \equiv g^s {y_s}^r r \pmod p$ fails.

Attack 4
Assume that the discrete logarithm problem is solvable.

(i) Adv knows the secret x_s and tries to generate the signature-ciphertext (c_1, c_2, c_3). Since the factoring problem remains unsolved, Adv does not know the other secret key β and so fails to generate c_3 from the signature-ciphertext.

(ii) With the information about the signature-ciphertext (c_1, c_2, c_3) and the secret key a_0, Adv tries to verify and recover the message. In this case, he tries to calculate the value of r from the equation $r \equiv {c_1}^d {c_2}^{a_o} (\mathrm{mod}\, p)$. However, without solving the factoring problem and finding the value of d, s/he cannot calculate r and so fails to recover the message from the equation $M \equiv g^s {y_s}^r r \ (\mathrm{mod}\, p)$.

4 Performance Evaluation

It has been shown that the proposed authenticated encryption scheme is secure against some attacks. In this section, the efficiency of this scheme is evaluated, in terms of the number of secret and public keys, computational complexity, and communication cost. The following notations are used to analyze the efficiency of this 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.
- $|\mu|$ denotes the bit length of μ.
- t is the number of recipients involved in verifying and decrypting message phase.

The performance of this scheme is shown in Table 2.

In Table 2, we show the performance of our new scheme. In this paper, we do not compare the performance with other schemes because to our knowledge, this is the first threshold authenticated encryption scheme developed using two number theoretical problems. However, compared with a single problem-based scheme, our scheme is less efficient since it needs more computation for two problems. Nevertheless, this is the best hybrid problem-based scheme that we can develop.

TABLE 2. Performance of the proposed authenticated encryption scheme

Criteria		**Evaluation**
No. of keys	SK	$2t + 2$
	PK	4
Computational complexity	Sign/Encrypt	$5\,T_{exp} + 3\,T_{mul} + (t^2 - t)\,T_{inv}$
	Verify/Decrypt	$(3t + 3)\,T_{exp} + (2t^2 - t + 1)\,T_{mul} + (t^2 - t)\,T_{inv}$
Size of parameters / Communication cost		$(t + 1)\|N\| + 2\,\|\bar{N}\| + (t + 5)\|p\|$

5 Conclusion

In this paper, we propose a threshold authenticated encryption scheme using two common number theoretical problems used in cryptography, namely, factoring and discrete logarithm. Security analysis shows that our scheme remains secure even if one of the problems is solved. In performance evaluation, it is shown that this is the best hybrid problem-based scheme that we can develop. Although this scheme appears to perform well, future development will be needed to develop a more efficient threshold authenticated encryption scheme using hybrid problems.

Acknowledgements

The second author acknowledges the financial support received from Universiti Kebangsaan Malaysia under grants FRGS/2/2013/SG04/UKM/02/1. We also thank to Mrs Alena Sanusi for her comments and constructive suggestions on the manuscript.

References

[1] T. S. Chen, K. H. Huang and Y. F. Chung, A practical authenticated encryption scheme based on elliptic curve cryptosystem, Computer Standards & Interfaces, 26 (2004), 461-469.

[2] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, IT-22 (1976), 644-654.

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

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

[5] M. O. Rabin, Digitalized signatures and public key cryptosystems as intractable as factorization, Technical Report MIT/LCS/TR-212, MIT, Cambridge, MA, 1979.

[6] V. S. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology-CRYPTO '85, Proceedings, Lecture Notes in Computer Science, vol. 218, Springer, New York, 1985, 417-426.

[7] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48 (1987), 203-209.

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

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

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

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

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

[13] D. Poulakis, On the cryptographic long term security, Journal of Applied Mathematics & Bioinformatics, 3(1) (2013), 1-15.

[14] K. Nyberg and R. A. Rueppel, A new signature scheme based on the DSA giving message recovery, Proceedings of the First ACM Conference on Computer and Communications Security, ACM Press, 1993, 58-61.

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

[16] Y. Desmedt and Y. Frankel, Shared generation of authenticators, Advances in Cryptology, Proceedings of Crypto '91, 1991, 457-469.

[17] C. L. Hsu and T. C. Wu, Authenticated encryption scheme with (*t*,*n*) shared verification, IEE Proceedings Computers and Digital Techniques, 145(2) (1998), 117-120.

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

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

Received: January 15, 2014