International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 19 (2015) pp 40632-40635

A Novel Authenticated Encryption Technique for Message Passing

[1*]G. Annapooranam, [2]Dr. K. Thangadurai

[1] Department of Computer Science, Manonmaniam Sundaranar University, Tirunelveli.
[2]Research Department of Computer Science, Govt. Arts College Autonomous, Karur.
[1]annapooranam2015@gmail. com, [2]ktramprasad04@yahoo. com

Abstract
Communication through Internet from a source to a destination always needs security measurements. Generally encryption methods with authentication are used for message transmission, which enables secure sending and receiving of message with validity. Traditional methods have limitations such as transmission overheads and less economical when a huge volume of messages has to be communicated. The above said two issues are taken care by the proposed method which overcomes the limitations, notably when compared with existing methods. In addition to that the proposed technique is extended to handle voluminous message passing securely by handling reordering of message blocks, replication and/or dropping of blocks or messages during transmission.

Keywords: Authenticated encryption technique, Security proof, Message recovery, Digital signature

1. Introduction

The exponential growth of Internet usage and communication necessitates secured transmission of information. So the significance of the issue is, how to prove the sender and assure the integrity of the message transmission. To achieve this, confidentiality, non-repudiation and authenticity are necessary which are provided by encryption and digital signature. Encryption and digital signature are the two base mechanisms for public key systems. An authenticated encryption technique follows a logical step to satisfy the basic security properties which are given below.

- Authenticity: Based on computation, it is not possible for an adaptive advisory to retrieve secret content from a ciphertext.
- Confidentiality: Based on computation, it is not possible for an adaptive advisory to act as the sender in communicating messages.
- Security: If the signer's private key is exposed in an instant of time, the constructed signature of the authenticated encryption message key cannot be retrieved before releasing the private key.
- Non-repudiation: it is computationally possible for a third party to resolve an issue between the sender and the receiver in the when the sender rejects the fact that he is the creator of the message.

The encryption of huge message by the existing studies is to split the information into segments and each segment is signed and encrypted separately. But the limitation of this method leads to copy or destroy some signature segments by an intruder in such a way that the receiver does not get the information about the changes. To avoid such situations, a new encryption method is proposed using information link to each segment to follow the flow [1]. But in this method forgery of valid signature and lack of non-repudiation is identified [2]. Then an adaptable encryption method with authentication is proposed [3] and its limitation of security lack is identified which leads to the proposal of two different authenticated methods [5]. In this study, a new secure authentication encryption is proposed and is robustly secure in random oracle model [4, 5, 6]. Random oracle is a black box which reacts to questions (unique) based on random approach. When compared with similar methods, the proposed technique includes many advantages in terms of cost and computational complexity. Also it is extended into authenticated encryption technique based on message connection.

2. The Preamble

This section describes the notations used in security and the attributes of the proposed message connection technique.

Lemma 1: Set (H, Σ, R) as base signature scheme that includes security parameter c. Set M as Probabilistic Polynomial Time machine with only public data input. If M can pick a valid signature (n, h, d, α) by including non-negligible probability, the machine can provide two valid signatures (n, h, d, α) and (n', h', d', α') with similar random tape and different oracle such that $d \neq d'$ in expected time slot.

Description 1: The message connection of authenticated encryption technique can be described using following properties.

Parameter generation: Takes security parameter c as input and provide common parameter CP

Key generation: Gets CP as input and outputs a public key pair (*sky; pky*) for all users

Authenticated encryption code: inputs the keys (*ssky; spky*) of signer, the nth message and public key *rpky* of receiver, outputs an encrypted signature α, which is authenticated.

Verification code and decryption: the nth message is retrieved by the receiver through his/her private key *rsky*. When the receiver inputs (*rpky; rsky*), the public key *spky* from the signer with encrypted sign, outputs a condition for verification as $b \in \{0, 1\}$ and if b=1, signature will be accepted otherwise rejected.

Description 2: An authenticated encryption technique with message connection is assured to be secure by protesting extended forgery for information attack if no polynomial margin opponent M succeeds with potential positives.

a) The competitor *L* executes parameter production code using parameter *c* and sends common parameter CP to opponent M.
b) The allotted receiver R executes key production code to produce key pair (*Rpky; Rsky*) and presents *Rpky*. The opponent M is permitted to get the secret key *Rsky*.
c) The opponent M carry outs a polynomial limited count of inquiries to the competitor *L*.
d) At the end the opponent *M* provide a valid signature α on message *n*. *M* succeeds if *n* is not at all questioned by *M* in step (b).

3. Proposed Encryption Technique

In the proposed technique, the authenticated encrypted signature can be retrieved and checked by the receiver only. The technique includes key generation code, authenticated encryption code and verification code. Based on the robustness of resolving the discrete logarithmic problem the security level of technique can be measured. The technique is more secured in random oracle model.

Key generation pseudo code:

a) Let *p, q* be the largest prime numbers, such that *q|p-1, t*ϵ *F(p)* is a producer of order *q. p, q, t* are the public parameters for system.
b) Set *alpha* and *beta* as signer and receiver, where *alpha* selects random number $u_M \in x_d$ as private key and calculates the public key $d_M = t^{u_M} mod\ p$, at the same time *beta* selects $u_N \in X_q$ as private key and its relevant public key is calculated using,

$$d_{N1} = t^{uN}\ mod\ p\ \&\ d_{N2} = t^{u_N^2} \quad (1)$$

c) Select a secured hash function f(.):$X_p \times X_p \rightarrow X_q$

Encryption pseudo code:

When signer *alpha* needs to generate a secured encryption signature for the message *n* which is to be sent to the receiver *Beta*, *Alpha* has to follow the signing steps as given below:

Step 1: The signer *Alpha* selects $c \in X_q$, a random number and calculates

$$h = t^{-l} d_{N1}^{l} \bmod p \quad (2)$$

$$g = l - f(h, n) u_M \bmod q \quad (3)$$

Step 2: Calculate $r = n.(d_{M1}, d_{M2})^l\ mod\ p$ (4)

Step 3: Now the signer *Alpha* sends *(h, g, r)* to the receiver *Beta*

Signature Verification pseudo code:

While *Beta* receives the signature *(h, g, r)*, message *n* needs to be recovered and verifies the validity of the signature for the message *n*.

Step 1: Calculate the message $n' = r.h^{-uN}\ mod\ p$ (5)

Step 2: Check the equality exists as follows,

$$t^g d_M^{f(h,n')} h\ =?\ (t^g d_M^{f(h,n')})_N^u\ mod\ p \quad (6)$$

or

$$h =?\ (t^g d_M^{f(h,n')})^{p_N - 1}\ mod\ p \quad (7)$$

Beta accepts the signature *(h, g, r)*, If the equation (6) or (7) exists. Since the private key is needed for verification, only *Beta* can verify the process.

4. Analysis of Proposed Technique on Security

The proposed technique is based on discrete logarithmic computation and the details are given below.

Theorem 1. Set *M* as opponent who can generate a forgery for a selected message attack in time instant τ with the success probability $\varepsilon \geq 10(d_g+1)(d_g+d_F)/2^l$. For the execution of queries q_g, q_F, it takes $\tau' < 120686 q_H /$ time. Random oracle model solves the quries on signature oracle and discrete logarithmic computation solves the hash oracle function f(.) in the above said time.

Proof: Based on the theorem 1, let opponent code *A*, is taking at most time *i* and creating at most q_F hash queries and q_g, signing queries can falsify authenticated encryption with ε' probability. Hence *Beta* can use *A* as sub module to generate code *L* to obtain signer's private key. *Alpha* takes this as the code *L* can find the solution for discrete logarithmic computation.

Code *L* selects $d_M \in X_p$, as a random public key for signer, *Alpha* and gives q_M to the opponent *A* along with common parameters. Let *Beta* control the code *L*, and it simulates the oraclof encryption and random for *L* as given below.

Answering F-Oracle queries: At any instant of time, the query from opponent *A* to the random oracle f(.), by *Beta's* simulation along with list of tuples (n_j, h_j, e_j). During the query execution for the input (h_j, n_j), code *L* performs as given below.

- If F-list defines query (h_j, m_j), then *Beta* recover (h_j, m_j) and outputs e_j.
- Otherwise, *Beta* chooses a random number $e_j \epsilon X_q$ and provide e_j by recoding (h_j, n_j, e_j) in the F-list.

Answering authenticated encryption queries. If the opponent *A* queried encryption oracle for the message *n*, then *Beta* should produce a valid signature tuples without the knowledge of private key u_A of *Alpha*.

1. Using two random integer values, calculate

$$h = (t^g d_M^i)^{u_B - 1}\ (mod\ p) \quad (8)$$

2. Calculate $r = n.r^{u_B} \pmod p$ (9)

3. Verify the H-list for hash oracle query and if *(m, h)* got query, then *Beta* gets the hash value *(n, h)* and terminate protocol. Otherwise *Beta* provides encryption text *(g, h, r)* on *n*. Then *Beta* reinitialize all the list and execute the above process for the

second time with different f(.). Based on this Forking lemma [10], *Beta* will get two different signature for same message and data such as *(h, g, r, e)* and *(h, g', r, e')* on the condition to satisfy the following relation.

$$t^g d_M^e h \ =? \ (t^g d_M^e)^{u_N} \ mod \ p = d_N^l \quad (10)$$

and

$$t^{g'} d_M^{e'} h \ =? \ (t^{g'} d_M^{e'})^{u_N} \ mod \ p = d_N^l \quad (11)$$

From equation (10) and (11) the following relationship (12) can be derived.

$$t^g d_M^r h = t^{g'} d_M^{r'} h \ (mod \ p) \quad (12)$$

Based on group knowledge the following relationship can be derived.

$$J + eu_M = J' + e'u_M \ (mod \ q) \quad (13)$$

Here $\gcd(e' - e, q) = 1$ and q is prime, where gcd() represents greatest common devisor. Hence, based on *t*, discrete logarithm u_M of u_M is obtained as follow

$$u_M = \frac{J - J'}{e - e'} \quad (14)$$

Let *Beta* terminate the simulation with the probability ε_{abort}. The simulator shows to the opponent the similar distribution compared to the opponent communication with original signature and random hash except for ε_{abort}. In this process the termination occur at step 3 of this phase. If *beta* chooses *(g, i)* to calculate h, then the event occurs. The probability of termination is at most $q_F/2^l$, since maximum *(g, i)* at H_q. Thus *Beta* terminates at step 3 with the signature query less than $\frac{q_F - q_g}{2^l}$ for any q_g signature. The inference is that *Beta* can resolve the u_M, the discrete algorithm of d_M, the random number based on *t* with probability $-\frac{q_F - q_g}{2^l}$.

Hence, the proposed technique is capable of working against forgery attacks in random oracle model. This provides the inference that the proposed technique is non-repudiation, in such a way that *Beta* cannot repudiate the signature, when *Alpha* provide valid signature. This method also offers forward security such that all messages from *Alpha* to *Beta* will be secret, in case of private key u_M from *M* is stolen or disclosed by accident. Note the format for message encryption is $r = n.(d_{N_1} d_{N_2})^c \ mod \ p$, here $c \in X_q$ – a random number.

Even if the opponent has a chance of getting the private key u_M from *Alpha*, based on the format of *r*, opponent cannot retrieve the message from the sender and receiver.

Notations for evaluation:

τ_e- time of exponentiation calculation
τ_n-time of modular calculation
τ_f- running time of hash function
|*n*|- bit length of *n*

The computational cost from three studies is compared in Table 1. From the comparison it is clear that the proposed technique is more efficient than existing methods.

Table 1

	Existing Method [7]	Existing Method [8]	Existing Method [9]	Proposed Method
SL	2|q|+|p|	2|q|+|p|	2|q|+|p|	2|q|+|p|
CSP	$2\tau_f+4\tau_e+3\tau_n$	$3\tau_f+3\tau_e+3\tau_n$	$3\tau_f+\tau_e+\tau_n$	$\tau_f+2\tau_e+2\tau_n$
MRV	$6\tau_e+2\tau_n$	$3\tau_f+3\tau_e+3\tau_n$	$3\tau_f+\tau_e+\tau_n$	$3\tau_f+2\tau_e+2\tau_n$

SL- Signature Length; CSP- Computation of Signature Production; MRV- Message Recovery & Veirfication

5. Message connection in Authenticated Encryption Technique

In addition to the above efficient technique, handling of big message is also considered in this paper. For this purpose, the signer split the big message *A* into $A_1, A_2, \ldots A_i$ where $A_i \epsilon X_p^*$. The further process sequence is given below.

1. Set random number $c \ \epsilon \ X_q$
2. For k=1, 2,.. i do
3. $h_k = A_i \times f_1(h_{k-1} \oplus A_{i-1} \oplus (d_{N_1} d_{N_2})^c)$ (15)

here, h_1=0 and f_1(.) is hash function.

4. $h' = h_1 || h_2 || \ldots || h_i$, shows message concatenation
5. Signer computation is as follows

$$h = t^{-1} d_{N1}^l \bmod p \quad (16)$$

$$g = l - f(h||h', A) u_M \bmod q \quad (17)$$

$$r = A_1.(d_{N_1} d_{N_2})^c \ mod \ p \quad (18)$$

6. Signer sends *(h, h_1, …h_i, g, r)* to the receiver.

Decryption and Verification:

The recovery of the message A_1 and message segments $A_1, A_2, \ldots A_i$ is required, when receiver receives *(h, h_1, …h_i, g, r)*. The execution of validation for message ($h' = h_1 || h_2 || \ldots || h_i$) verification is given below.

1. Let the message segment is $A_1 = r.h^{-u_N} \ mod \ p$ (19)
2. For k=2, …, i, calculate

$$A_k = h_{i..} \ f_1(h_{k-1} \oplus A_{i-1} \oplus (d_{N_1} d_{N_2})^c)^{-1} \quad (20)$$

3. Message A_k and $A' = A_1 || A_2 || \ldots || A_i$ are to be concatenated
4. Verify the validation of the received message A' using equation

$$t^g d_M^{f(h,A')} h \ =? \ (t^g d_M^{f(h,A')})^{u_N} \quad (21)$$

6. Conclusion

The proposed technique allows the receiver to simultaneously retrieve and verify message. The computational and communication cost are reduced and the proposed method becomes suitable to low storage devices. The proposed authenticated encryption technique is secure in random oracle model. This is proved by comparing the existing methods. Finally it is extended to handle big message by challenging against segment duplication or detection during transmission.

References

1. Tseng, Y, M., Jan, J, K., 2002, "An efficient authenticated encryption scheme with message linkages and low communication costs, " J. Inform. Sci. Eng., 18, pp. 41–56.
2. Eun-Jun Yoon, Kee-Young Yoo, 2005, "Robust authenticated encryption scheme with message linkages, " knowledge-based intelligent information and engineering systems, in: 9th International Conference, KES 2005, Melbourne, Australia, LNAI, vol. 3684, Springer-Verlag, pp. 281–288.
3. Wu, T, S., Hsu, C, L., 2002, "Convertible authenticated encryption scheme, " J. Syst. Softw., 62, pp. 205–209.
4. Bellare, M., Rogaway, P., 1996 "The exact security of digital signatures: how to sign with RSA and Rabin, ", in: Proc. Eurocrypt96, LNCS, vol. 1070, Springer-Verlag, pp. 399–416.
5. Pointcheval, D., Vaudenay. S., 1996 "On Provable Security for Digital Signature Algorithms, " Technical Report LIENS-96-17, LIENS, October 1996.
6. Zhang, J., Mao, J., 2008, "A novel ID-based designated verifier signature scheme, " Inform. Sci., 178 (3), pp. 766–773.
7. Li, Y., Zhang, J., Wang, Y., 2010, "Improvement for forward-secure authenticated encryption scheme, " J. Southeast Univ. (Nat. Sci. Ed.), 37 (Sup(I)), pp. 20–23.
8. Lv, J., Wang, X., "Practical convertible encryption scheme using self-certified public keys, " Appl. Math. Comput, 1699 (2), pp. 1285–1297.
9. Wu. T. S, Lin. H. Y, 2009 "Secure Convertible Authenticated Encryption Scheme Based on RSA, " Informatica, 33, pp. 481-486.