### References

1 GERSHO, A., and GRAY, R.M.: 'Vector quantisation and signal compression' (Kluwer Academic Publisher, 1992)

2 CHOU, P.A., LOOKABAUGH, T., and GRAY, R.M.: 'Optimal pruning with applications to tree-structured source coding and modeling', *IEEE Trans. Inf. Theory*, 1989, **35**, (2), pp. 299–315

3 RISKIN, E.A., and GRAY, R.M.: 'A greedy tree growing algorithm for the design of variable rate vector quantisers', *IEEE Trans. Signal Process.*, 1991, **39**, (11), pp. 2500–2507

4 ANTONINI, M., BARLAUD, M., MATHIEU, R., and DAUBECHIES, I.: 'Image coding using wavelet transform', *IEEE Trans. Image Process.*, 1992, **IP-1**, pp. 205–219


## Cryptosystem of Chua and Ling


M. Joye and J.-J. Quisquater



*Indexing term: Cryptography*

The authors show that the cubic curve cryptosystem proposed by Chua and Ling can easily be reduced to the cryptosystern of Rabin-Williams.


*Introduction:* At Eurocrypt '96, Meyer and Müller [1] presented a new Rabin-type scheme based on elliptic curves. In [2], this system was reduced to the system of Rabin-Williams [3, 4]. Using the same technique, we show that the system of Chua and Ling [5] can also be reduced.

*Chua-Ling's cryptosystem:* This cryptosystem is based on a singular cubic curve of the form

$$C_n(b) : y^2 \equiv x^3 + bx^2 \pmod{n}$$

To set up the system, each user chooses two large primes $p$ and $q$ both congruent to 11 modulo 12. Then, he publishes the value of $n = pq$.

Suppose Alice wants to send a message $m$ to Bob. Then she chooses $\lambda \in \mathbb{Z}/n\mathbb{Z} - \{0, \pm 1\}$ and sets $\mathbf{P} = (m^2, \lambda m^3)$. Next, she computes $c = \lambda^3 \bmod n$ and $b = (\lambda^2 - 1)m^2 \bmod n$, and sends the ciphertext consisting of $c$, $b$, $x_Q = x([2]\mathbf{P})$, $t = (y([2]\mathbf{P})/n)$ and $u = \mathrm{lsb}(y([2]\mathbf{P}))$.

To recover the plaintext $m$, Bob computes the unique $y_Q$ satisfying $y_Q^2 \equiv x_Q^3 + bx_Q^2 \pmod{n}$ with Jacobi symbol $t$ and lsb $n$. He sets $\mathbf{Q} = (x_Q, y_Q)$. Letting $\mathbf{Q}_p = \mathbf{Q} \bmod p$ and $\mathbf{Q}_q = \mathbf{Q} \bmod q$, he computes $\mathbf{P}_{i,p} = (x_{i,p}, y_{i,p})$ $(i = 1, 2)$ such that $[2]\mathbf{P}_{i,p} = \text{on } \mathbf{Q}_p$ on $C_p(b)$ and similarly $\mathbf{P}_{i,q}$. Next, he computes $I_p = \{i : c^2 \equiv y_{i,p}{}^6 x_{i,p}{}^{-9} \pmod{p}\}$. He does the same for the prime $q$. Finally, he computes $m_p = y_{i,p}^3 x_{i,p}^{-4} c^{-1} \bmod p (i \in I_p)$ and $m_q$. So, Bob obtains $m$ using the Chinese remainder theorem such that $m \equiv m_p \pmod{p}$ and $m \equiv m_q \pmod{q}$.

*Reduction to Rabin-Williams:* Since $\mathbf{P} = (m^2, \lambda m^3) \in C_n(b)$, it follows that:

$$x_Q = x([2]\mathbf{P}) \equiv \frac{(3m^2 + 2b)^2}{4\lambda^2 m^2} - 2m^2 - b \pmod{n} \quad (1)$$

and

$$\lambda^2 m^2 \equiv m^2 + b \pmod{n} \quad (2)$$

From eqns. 1 and 2, we construct the polynomials $P_1, P_2 \in (\mathbb{Z}/n\mathbb{Z})[X]$ given by

$$P_1(X) = 4(x_Q + 2X + b)(X + b) - (3X + 2b)^2$$

$$P_2(X) = c^2 X^3 - (X + b)^3$$

Since $m^2$ is a root of $P_1$ and $P_2$, $m^2$ will be a root of $R = \gcd(P_1, P_2)$. The polynomial $R$ has a very high probability of degree 1 [6]. Solving this polynomial in $X$ gives the value of $m^2$.

*Conclusion:* We have shown that we can easily recover the value of $m^2$ from the ciphertext corresponding to a plaintext $m$. Therefore, the Chua-Ling scheme is reduced to the Rabin-Williams cryptosystem.


*Acknowledgments:* We are grateful to S.-K. Chua and S. Ling for sending a preprint of their paper.




*5 September 1997*

*Electronics Letters Online No: 19971239*



M. Joye (*UCL Crypto Group, Department of Mathematics, University of Louvain, Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, Belgium*)

J.-J. Quisquater (*UCL Crypto Group, Microelectronics Laboratories, University of Louvain, Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, Belgium*)

E-mail: jjq@dice.ucl.as.be

Corresponding author: J.-J. Quisquater



### References

1 MEYER, B., and MÜLLER, V., : 'A public key cryptosystem based on elliptic curves over $\mathbf{Z}/n\mathbf{Z}$ equivalent to factoring', *in* MAURER, U. (Ed.): 'Adv. Cryptol. - Eurocrypt '96', (Springer-Verlag, 1996), pp. 49–59 (vol. 1070 of Lecture Notes in Computer Science)

2 JOYE, M., and QUISQUATER, J.-J.: 'Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams', to be published in *Des., Codes and Cryptogr.*

3 RABIN, M.O.: 'Digitalized signatures and public-key functions as intractable as factorization'. Tech. Rep. MIT/LCS/TR-212, MIT, Laboratory for Computer Science, January 1979

4 WILLIAMS, H.C.: 'A modification of the RSA public-key encryption procedure', *IEEE Trans. Inf. Theory*, 1980, **IT-26**, (6) pp. 726–729

5 CHUA, S.K., and LING, S., : 'A Rabin-type scheme on $y^2 \equiv x^3 + bx^2 \bmod n$', *in* JIANG, T., and LEE, D.T. (Eds.): 'Third Annual International Computing and Combinatorics Conf.' (COCOON '97), (Springer-Verlag, 1997), (vol. 1276 of Lecture Notes in Computer Science)

6 COPPERSMITH, D., FRANKLIN, M., PATARIN, J., and REITER, M.,: 'Low exponent RSA with related messages', *in* MAURER, U. (Ed.) 'Adv. Cryptol. - Eurocrypt '96', (Springer-Verlag, 1996), pp. 1–9 (vol. 1070 of Lectures Notes in Computer Science)


## Hash function based on block cipher


Xun Yi and Kwok Yan Lam



*Indexing term: Cryptography*

A new $2m$-bit iterated hash function based on an $m$-bit block cipher with a $2m$-bit key is presented. The results of security analysis show that the hash function can be expected to have ideal computational security against the five attacks when the underlying cipher is assumed to have no weakness.


*Introduction:* In cryptographic applications, hash functions are used within digital signature schemes and within schemes to provide data integrity. Owing to the 'birthday attack', about $2^{32}$ computations of the hash code are needed to find a collision for any hash functions of code length 64 bits. Thus, several efforts [1 – 4] have been made to construct 128 bit hash functions based on a block cipher of block length 64 bits.

In this Letter, we present a new $2m$-bit iterated hash function based on an $m$-bit block cipher with a $2m$-bit key, such as IDEA. The results of security analysis show that the hash function can be expected to have ideal computational security against five attacks when the underlying cipher is assumed to have no weakness.

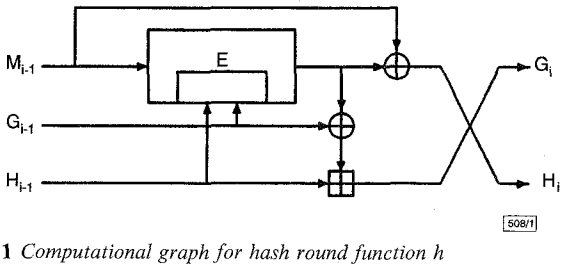


**Fig. 1** *Computational graph for hash round function h*

*Overview of new hash function:* The new hash function is an iterated hash function. The computational graph of its round function $h$ is illustrated in Fig. 1.

The hash round function $h$ can be formulated as follows:

$$(G_i, H_i) = h(G_{i-1}, H_{i-1}, M_{i-1}) \quad (1)$$

where two $m$-bit values $G_i$ and $H_i$ are computed from the two $m$-bit values $G_{i-1}$ and $H_{i-1}$ and from the $m$-bit message block $M_{i-1}$ as follows:

$$G_i = \left(E_{(G_{i-1}\|H_{i-1})}(M_{i-1}) \oplus G_{i-1}\right) \boxplus H_{i-1} \quad (2)$$

$$H_i = E_{(G_{i-1}\|H_{i-1})}(M_{i-1}) \oplus M_{i-1} \quad (3)$$

where $E_K(P)$ describes the ciphertext block responding to plaintext block $P$ enciphered by an $m$-bit block cipher $E$ using $2m$-bit key $K$; $X\|Y$ represents the concatenation of $m$-bit blocks $X$ and $Y$; $X \oplus Y$ indicates the bitwise exclusive-or of $m$-bit blocks $X$ and $Y$; $X \boxplus Y$ denotes the addition modulo $2^m$ of $m$-bit integers $X$ and $Y$.

The 'meta-method' [3] is used to construct the new hash function. The hash function is a function $Hash(\cdot)$ determined by the easily computable round function $h(\cdot)$ from three $m$-bit values to two $m$-bit values in the manner that the message $M = (M_0, M_1, ..., M_{n-1})$, where $M_i$ is $m$-bit value, is hashed to a $2m$-bit hash value $(G, H) = (G_n, H_n)$ by computing eqn. 1 recursively. We write

$$(G, H) = Hash(G_0, H_0, M) \quad (4)$$

to show explicitly the dependence on $(G_0, H_0)$ and $M$, where $(G_0, H_0)$ is a $2m$-bit specified initial value. For message data whose total length in bits is not a multiple of $m$, we can apply deterministic 'padding' [3] to the message to be hashed by eqn. 4 to increase the total length to a multiple of $m$.

The new hash function takes advantage of MD-strengthening [3, 5], i.e. specify that the last block $M_{n-1}$ of the message $(M_0, M_1, ..., M_{n-1})$ to be hashed represents the length of the 'true message' in bits, i.e. the length of unpadded portion of the first $n-1$ blocks. Therefore, the hashed message must contain at least two blocks.

*Attacks on new hash function:* A target attack, free-start target attack, collision attack, semi-free-start collision attack and free-start collision attack [4] can be performed on an iterated hash function. Each attack on the new hash function is treated as follows.

(i) *Target attack*: A target attack on the hash round function $h$ in our proposal reads: given $G_{i-1}$, $H_{i-1}$ and $M_{i-1}$, find $M'_{i-1}$ such that $M'_{i-1} \neq M_{i-1}$ and

$$h(G_{i-1}, H_{i-1}, M'_{i-1}) = h(G_{i-1}, H_{i-1}, M_{i-1}) \quad (5)$$

However, based on eqns. 2 and 3, $M'_{i-1} = M_{i-1}$ can be deduced from eqn. 5. It shows, except from $M_{i-1}$, that no matter what value $M'_{i-1}$ takes, 'target' $h(G_{i-1}, Hi\text{-}1, M_{i-1})$ is never hit. So we can say that the hash round function can completely resist target attack.

In view of the above fact, target attack on the new hash function must attack more than two rounds of it successively. Considering that the dependent relations of hash outputs to hash inputs in more than two rounds are much more complex than those of one round, only a brute-force target attack, in which one randomly chooses a $M'$ until one hits the 'target' $Hash(G_0, H_0, M)$, can be used to attack it. By carrying out brute-force target attack on it, 'hitting a target' requires about $2^{2m}$ computations of hash values.

(ii) *Collision attack and semi-free-start collision attack*: Although slightly different from the target attack, we can still obtain $M'_{i-1} = M_{i-1}$ from eqn. 5 when performing a collision attack and semi-free-start collision attack on the new hash round function. It implies that the hash round function can completely resist a collision attack and a semi-free-start collision attack. At least two rounds of these attacks on the new hash function need to be carried out successively. For more than the two rounds of our proposal, the dependent relations of hash outputs to hash inputs are too complex to provide any help to these attacks on it.

(iii) *Free-start target attack and free-start collision attack*: The hash round function in our proposal consists of two subfunctions, which are illustrated in Fig. 2.

From Fig. 2, we find that the first subfunction is the same as in the DM-scheme. In addition, we can prove that the second subfunction is equivalent (in the sense of security) to that of the DM-scheme. Thus, a free-start-target attack and free-start collision attack on the hash round function implies that we must attack two DM-schemes simultaneously.

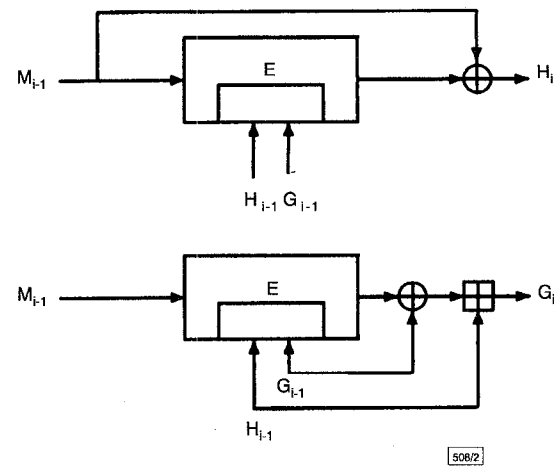


**Fig. 2** *Computational graph for the two subfunctions*

The DM-scheme with MD-strengthening is generally considered to be secure in the sense that, if the block cipher has no known weakness, then no attack better than a bruteforce attack is known. If a free-start target attack and free-start collision attack on one subfunction provides no help in attacking the other subfunction, we can expect that the attacks on the new hash round function will have complexity equal to the product of the complexities of the attacks on the two subfunctions.

On the basis of proposition 2 in [4], the new hash function has roughly the same computational security against free-start target attack and free-start collision attack as its hash round function if the underlying block cipher has no known weakness.

**Table 1**: Computational complexities of five attacks on new hash function

| Type of attacks | Complexities |
|---|---|
| Target attack | $2^{2m}$ |
| Collision attack | $2^m$ |
| Semi-free-start collision attack | $2^m$ |
| Free-start target attack | $2^{2m}$ |
| Free-start collision attack | $2^m$ |

*Conclusion:* A new $2m$-bit iterated hash function, which is based on an $m$-bit block cipher with $2m$-bit key, has been proposed. When the underlying block cipher is assumed to have no weakness, the new hash function can be expected to have ideal computational security against the five attacks (see Table 1 for a summary).


*15 September 1997*
*Electronics Letters Online No: 19971336*

Xun Yi (*National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, People's Republic of China*)

Kwok Yan Lam (*Department of Information System and Computer Science, National University of Singapore, Singapore*)

## References

1 PRENEEL, B., BOSSELAERS, A., and GOVAERTS, R., *et al.*: 'Collision-free hashfunctions based on blockcipher algorithm'. Proc. 1989 Int. Carnahan Conf. on Security Technology, 1989, pp. 203–210

2 QUISQUATER, J., and GIRAULT, M.: '2n-bit hash functions using 11-bit symmetric blcok cipher algorithm'. Proc. Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science no. 434, (Springer-Verlag, 1990), pp. 102–109

3 MERKLE, R.: 'One way hash functions and DES'. Proc. Advances in Cryptology-CRYPTO'89, Lecture Notes in Computer Science no. 435, (Springer-Verlag, 1990), pp. 428–446

4 LAI, X., and MASSEY, J.: 'Hash functions based on block ciphers'. Proc. Advances in Cryptology - EUROCRYPT'92, 1993, Lecture Notes in Computer Science no. 658, (Springer-Verlag, 1993), pp. 55–70
5 DAMGAARD, I.: 'A design principle for hash functions'. Proc. Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science no. 435, (Springer-Verlag, 1990), pp. 416–427

# Improvement of Chang-Wu broadcasting cryptosystem using geometric properties of lines

Tzong-Sun Wu and Tzong-Chen Wu

*Indexing terms: Cryptography, Security of data*

In 1991, Chang and Wu proposed a broadcasting cryptosystem using interpolating polynomials and geometric properties of circles. Nevertheless, the Chang-Wu scheme can be further enforced by using a time-variant parameter and a one-way function to protect legal receivers' secrets from being disclosed. The authors present an improvement of the Chang-Wu scheme using geometric properties of lines. This improvement repairs the security flaws inherent in the original Chang-Wu scheme, while requiring fewer public parameters and less computing time.

*Introduction:* A broadcasting cryptosystem is used to achieve secure communications over an insecure channel so that only the specified subset of users can obtain the message in one single broadcasting transaction. In 1991, Chang and Wu [1] proposed a broadcasting cryptosystem using interpolating polynomials and geometric properties of circles. Recently, Hwang *et al.* [2] and Lin and Chen [3] separately demonstrated a successful attack on the Chang-Wu scheme, and showed that in the Chang-Wu scheme, any malicious user who is a legal receiver of a broadcasting transaction can derive the originator's and all other legal receivers' secrets by plotting another legal broadcasting transaction to these users.

In fact, the original Chang-Wu scheme can be further enforced by using a time-variant parameter and a one-way function to protect legal receivers' secrets from being disclosed. In this Letter, we shall present an improvement of the Chang-Wu scheme using geometric properties of lines. Our improvement repairs the security flaws inherent in the original Chang-Wu scheme, while requiring fewer public parameters and less computing time as compared to the enforced Chang-Wu scheme.

*Brief review of the Chang-Wu scheme:* The following terms are used to facilitate presentation of the Chang-Wu scheme. *CAS*: the central authority server; $U_i$: a user in the system; $S_i$: the secret point for $U_i$; $C_i$: the circle i with respect to $U_i$; $P_i$: the centre of Ci; $w_{ij}$: a point on Ci; $H(x)$: an interpolating polynomial; $O_i$: a point on $H(x)$: *EP*: Euclidean plane; $d(x, y)$: the distance between two points $x$ and $y$ in *EP*.

The Chang-Wu scheme works as follows. Suppose that there are $(n+1)$ users $U_0$, $U_1$, ..., $U_n$ in the system. Initially, *CAS* randomly chooses $(n+1)$ distinct points $S_i$ from *EP*, and distributes $S_i$ to $U_i$ (for $i = 0, 1, ..., n$) via secure channels. Each secure broadcasting transaction consists of two stages: the broadcasting stage (performed by the originator and *CAS*) and the recovery stage (performed by each legal receiver). Details of these two stages are described below.

*Broadcasting stage:* Suppose $U_0$ (the originator) wants to broadcast a secret message $M$ to $U_1$, $U_2$, ..., and $U_m$ ($1 \le m \le n$). Upon receiving $U_0$'s request, CAS performs the following tasks:
(i) Randomly choose $(m+1)$ distinct points $P_i$ (for $i = 0, 1, ..., m$) from *EP*, which are also distinct from $S_0$, $S_1$, ..., $S_m$.
(ii) Construct an $m$-degree interpolating polynomial $H(x)$ passing $P_0$, $P_1$, ..., $P_m$.
(iii) Randomly choose $m$ distinct points $O_i$ (for $i = 1, 2, ..., m$) from $H(x)$, which are also distinct from $P_0$, $P_1$, ..., $P_m$.
(iv) Generate $(m+1)$ circles $C_i$ (for $i = 0, 1, ..., m$), where each $C_i$ has $P_i$ as the centre and $d(P_i, S_i)$ as the radius.
(v) Randomly choose two distinct points $w_{i1}$ and $w_{i2}$ from $C_i$ (for $i = 0, 1, ..., m$), which are also distinct from $S_i$.
(vi) Publish $O_i$, $w_{j1}$ and $w_{j2}$ for $i = 1, 2, ..., m$ and $j = 0, 1, ..., m$.
After that, $U_0$ can initiate a secure broadcasting transaction by performing subsequent tasks:
(vii) Calculate $C_0$ passing $S_0$, $w_{01}$ and $w_{02}$, and obtain its centre $P_0$.
(viii) Reconstruct $H(x)$ with $P_0$, $O_1$, ..., $O_m$.
(ix) Randomly choose an integer $r$ and compute $k = H(r)$.
(x) Broadcast $r$ and the ciphertext of $M$ encrypted by $k$.
The graphical result of the above procedure is shown in Fig. 1.

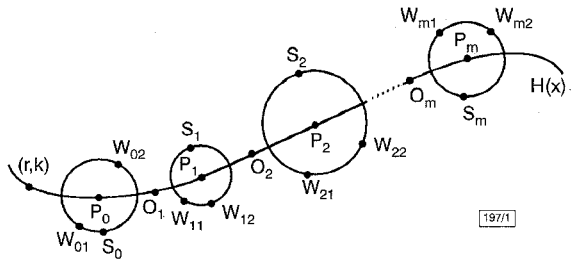


**Fig. 1** *Graphical result of broadcasting stage in Chang-Wu scheme*

*Recovery stage:* On receiving $r$ and the ciphertext of $M$ broadcast by $U_0$, any legal receiver $U_i$ performs the following steps to recover $M$:
(i) Calculate $C_i$ passing $S_i$, $w_{i1}$ and $w_{i2}$, and obtain its centre $P_i$.
(ii) Reconstruct $H(x)$ with $P_i$, $O_1$, ..., $O_m$.
(iii) Compute $k = H(r)$ and use it to decrypt the ciphertext.

*Attacks on Chang-Wu scheme:* The attacks on the Chang-Wu scheme demonstrated in [2, 3] are based on the same idea in essence. From the cryptanalyses discussed in [2, 3], any participant (including the originator and the legal receivers) of a broadcasting transaction can obtain the circles with respect to the others. For instance, $U_0$ first finds a perpendicular line $L_2$ passing the midpoint of $w_{21}$ and $w_{22}$, and then calculates the intersection of $L_2$ and $H(x)$, i.e. $P_2$. With the knowledge of $P_2$ and $w_{21}$ (or $w_{22}$), $U_0$ can easily obtain the circle $C_2$ with respect to $U_2$. Such vulnerability makes the Chang-Wu scheme flawed. In the following, we will demonstrate how can a malicious user find the secret point for any other participant in the system.

Suppose $U_0$ is the malicious user who wants to derive $U_i$'s secret point $S_i$ (for $i = 1, 2, ..., m$). First of all, $U_0$ initiates three different broadcasting transactions to the same values of $U_i$. Let $C_i$, $C_i'$ and $C_i''$ be the circles with respect to $U_i$ for these three transactions, respectively. After that, $U_0$ can easily obtain $S_i$ by finding the intersection of $C_i$, $C_i'$ and $C_i''$, since all these circles pass $S_i$.

*Our improvement:* Intuitively, the security flaws inherent in the Chang-Wu scheme can be repaired by using a time-variant parameter and one-way function to protect legal receivers' secret points from being disclosed. Let $f$ be a one-way function that accepts variable-length input and produces a point with $x$- and $y$-coordinates in *EP*. Such a one-way function $f$ can easily be built from the methods proposed in [4, 5]. Let $T$ be the time-variant parameter. We can replace all secret points $S_i$ by $f(T, S_i)$ in the broadcasting stage of the Chang-Wu scheme. This small modification has sufficient strength to thwart the attacks on the original Chang-Wu scheme. In the following, we describe another improvement of the Chang-Wu scheme using geometric properties of lines.

Initially, *CAS* randomly chooses $(n+1)$ distinct points $S_i$ from *EP*, and distributes $S_i$ to $U_i$ (for $i = 0, 1, ..., n$) via secure channels. Meanwhile, *CAS* publishes a one-way function $f$ defined above.

*Broadcasting stage:* Suppose $U_0$ (the originator) wants to broadcast a secret message $M$ to $U_1$, $U_2$, ..., and $U_m$ ($1 \le m \le n$). Upon receiving $U_0$'s request, *CAS* performs the following tasks:
(i) Randomly choose a line $L(x)$ from *EP*.
(ii) Randomly choose $(m+1)$ distinct points $Q_i$ from $L(x)$, and compute $P_i$ such that $Q_i$ is the midpoint of $P_i$ and $f(T, S_i)$, for $i = 0, 1, ..., m$, where $T$ is a time-variant parameter.
(iii) Randomly choose a point $A$ from $L(x)$, which is distinct from $Q_0$, $Q_1$, ..., $Q_m$.
(iv) Publish $T$, $A$ and $P_i$ for $i = 0, 1, ..., m$.