Ciphertext Policy Attribute Based Encryption for Arithmetic circuits

Mahdi Mahdavi Oliaee and Zahra Ahmadian
mahdavi.mahdi71@gmail.com , z_ahmadian@sbu.ac.ir

***Abstract*—We present the first Ciphertext Policy Attribute Based Encryption (CP-ABE) scheme where access policies are expressed as arithmetic circuits. The idea is first introduced as a basic design based on the multilinear map. Then, two improved versions of that, with or without the property of hidden attributes, are introduced. We also define the concept of Hidden Result Attribute Based Encryption (HR-ABE) which means that the result of the arithmetic function is hidden to the users. We prove that the the proposed schemes have adaptive security, under the assumption of hardness of the $(k-1)$-Distance Decisional Diffie-Hellman problem.**

***Index Terms*—Ciphertext Policy Attribute Based Encryption (CP-ABE), Arithmetic circuit, Multilinear map, Adaptive security, Hidden attributes, Hidden Result.**

I. Introduction

There are many applications in communication systems and cloud based systems, where the sender aims to send a message to a number of users. Based on the traditional public key encryption solutions, the sender must identify all the qualified users and encrypt the message separately for each of which. Attribute Based Encryption (ABE) provides solution for such situation by defining the access structure which is based on a set of user's attributes.

The research on ABE can be applicable in many different aspects of recent technologies, such as Internet of Things (IoT), Personal Healthcare Records (PHRs), vehicular networks, and many other ones. The concept of Attribute Based Encryption (ABE) was invented by Sahai, Waters, et al. [1]. In this scheme, each user has a set of attributes and a set of secret keys related to these attributes. The message is encrypted by the sender based on a number of attributes. If the intersection of the sender and reciever sets are greater than a TTP-selected threshold, the message can be decrypted by the reciever. That is why this scheme is called Fuzzy Identity Based Encryption (Fuzzy IBE). ABE is acctually a generalization of IBE .

Then, Goyal et al [2] defined the concept of Key Policy Attribute Based Encryption (KP-ABE). In this type of ABE scheme, the sender encrypts his message according to a number of attributes. The secret keys of any user were defined with his access structure related to his attributes. If attributes in ciphertext satisfy the receiver's access structure, the user can obtain the plaintext. Contrary to KP-ABE, the concept of Ciphertext Policy Attribute Based Encryption (CP-ABE) was introduced by Bethencourt et al. [3]. The ciphertext is constructed according to access structure and the secret keys of the receiver are constructed according to users' attributes. In these schemes, the attributes of the receiver must be satisfied with the ciphertexts' access structure. Due to the possibility of choosing the access structure by the sender, this scheme is more flexible than KP-ABE. Bethencurt proved the security of his scheme in the generic group. Waters in [4] proposed a CP-ABE scheme and demonstrated the security of his scheme under standard assumptions. All of these schemes supports the monotone circuit access structures. Ostrofsky et al. [5] presented the first schemes for non-monotone circuits. Green et al. [6] prposed the idea of outsourcing the heavy computations to cloud service, to reduce the computational overhead for users.

One of the challenges of this domain is revoking the attributes (keys) and users. Some schemes focuse on resolving this problem [7],[8]. Chase in [9] presented multi authority ABE to answer the key escrow problem. In [10] Attrapondong presents the Dual Policy ABE. In [11] the Hierarchical Attribute Based Encryption (HABE) was presented. In the HABE users with higher level attrebute can decrypt the messages encrypted for lower level one. For example, commanders can decrypt messages that are encrypted for soldiers. Some articles have focused on increasing efficiency, security, and size of the ciphertext and keys [12],[13], and [14].

Two levels of security have been defined for ABE schemes: selective security and adaptive security. In the selective security, the attacker defines the challenge attribute vector (or function) at the beginning of setup phase and send it to the simulator. The simulator constructs public parameters according to the received vector. Then the attacker can request the secret keys, adaptively. These secret keys should not satisfy the challenge vector (or function). On the other hand, in adaptive security, public parameters are defined with a simulator at the beginning and send to the attacker. Then, the attacker defines the challenge attribute vector (or function) and sends it to the simulator. Then the attacker requests secret keys adaptively. These secret keys should not satisfy the challenge vector (or function). Adaptive security is known as complete security. However, there is another security level, called semi-adaptive security [15]. In this level of security, the simulator defines public parameters and sends them to the attacker. Then, the attacker selects the challenge vector (or function) and sends it to the simulator, and requests the secret keys. The simulator constructs secret keys according to request and challenge vector (or function). Then, sends these secret keys to the attacker. These secret keys should not satisfy the challenge vector (or function). Semi-adaptive security is more secure

than selective security but less secure than adaptive security.

Garg et al in [16] presented a backtracking attack for pairing-based ABE with circuits that have a fanout bigger than one. Garg presented KP-ABE for all circuits using multilinear maps. Garg used non-standard assumptions in his security proof. Hard problems related to the multilinear maps are nonstandard cryptographic assumptions. However, his scheme works for any circuits with arbitrary fanout.

The above schemes are designed based on number theory problems and make use of pairing for achieving their goals. Therefore, these schemes are not secure against quantum computers. Agrawal et al. [17] presented Fuzzy ABE based on lattice for the first time. Boyen et al. [18] and Zhang et al. [19] presented the first lattice-based KP-ABE and CP-ABE, respectively. Note that the security of lattice-based ABE schemes are based on the hardness of the Learning With Error (LWE) problem. Gorbunov et al. [20] presented lattice based KP-ABE for circuit with arbitrary fanouts. This scheme is the first ABE scheme that works for any boolean function with standard assumptions. In this scheme, *two to one Recoding* (TOR) technique has been used. Also, this scheme supprots gates that their fan-in is two. The arithmetic circuit has been supported as the access structure in Boneh's scheme for the first time[21], where fully key homomorphic encryption for constructing KP-ABE is proposed. In this scheme, addition and multiplication gates are used instead of the conventional **AND** and **OR** gates. Note that, arithmetic circuits are more general than boolean circuits.

Because of the complexity of LWE, in [22],[23], and [24] Ring-LWE was used for designing ABE schemes. R-LWE reduces computational complexity and memory required. Recently, an adaptively secure scheme based on LWE is proposed [25].

If the attribute vector or policy in the ciphertext is hidden, the ABE is called Predicate Encryption [26]. Predicate Encryption is a special version of Functional Encryption [27], in which the receiver can obtain a function of plaintext. In other words, in this type of Encryption instead of all or nothing in traditional cryptosystems, users can get partial information about data and can not receive any other information. In some schemes, such as [28] and [29], the policy is hidden.

In this paper, we propose the CP-ABE for arithmetic circuits with hidden result by use of the multilinear maps. We proposed three variants of our scheme: A basic one is first introduced, which demonstrates the platform of our idea. Then, improved version I is proposed, which is more general that the basic one and the attribute vector is unknown to the users. Finnally, improved version II is proposed in which the attribute vector of each user is disclosed to himself. The adaptive security of all these schemes is proved based on a new defined hard problem called $k-1$-distance Diffie-Hellman problem. This problem is at least as hard as the k-multilinear Diffie Hellman problem.

II. Preliminaries

In this section, we provide preliminaries that are necessary for the rest of the paper.

A. k-Multilinear map

The multilinear map is defined over k groups of the same order $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_k$. Assume that g_i is the generator of $\mathbf{G}_i$ for $i \in \{1, 2, ..., k\}$. The function $e_{i,j}$ is defined as below:

$$e_{i,j} : \mathbf{G}_i \times \mathbf{G}_j \rightarrow \mathbf{G}_{i+j};\ 1 \leq i, j, i+j \leq k$$
$$e_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab} \tag{1}$$

We can summerize the consecutive computations of several multilinear maps into the following formula.

$$e(g_{i_1}^{x_1}, g_{i_2}^{x_2}, ..., g_{i_m}^{x_m}) = g_n^{\prod_{i=1}^{m} x_i} \tag{2}$$

where $n = \sum_{j=1}^{m} i_j \leq k$. There is a polynomial-time algorithm for computing the above equations. The bilinear map (or pairing) is the special type of this map for $k = 2$.

B. k-Multilinear Diffie-Hellman problem

Given the vector $\left\{\{g_1, g_2, ..., g_k\}, g^s, g^{c_1}, g^{c_2}, ..., g^{c_k}\right\}$, where $g = g_1$, computing the amount of $T = g_k^{s.\prod_{i=1}^{k} c_i}$ is known as the k-Multilinear Diffie-Hellman (k-MDH) problem.

C. k-Multilinear Decisional Diffie-Hellman problem

Assume $g = g_1$, given the vector $\left\{\{g_1, g_2, ..., g_k\}, g^s, g^{c_1}, g^{c_2}, ..., g^{c_k}, g_k^z\right\}$, deciding if $z = \prod_{i=1}^{k} c_i$ or not is known as the k-Multilinear Decisional Diffie-Hellman (k-MDDH) problem.

D. $(k-1)$-Distance Diffie-Hellman problem

Given a k-multilinear map over groups $\mathbf{G}_1, \ldots, \mathbf{G}_k$, and $\left\{g^x, g_k^y\right\}$, we define the problem of computing $T = g_k^{x.y}$ as $(k-1)$-Distance Diffie-Hellman ($(k-1)$-DsDH) problem.

This problem is at least as hard as k-MDH problem, i.e. given access to oracle $\mathcal{O}$ that solves $(k-1)$-DsDH problem, one can solve k-MDH problem. For demonstrating this claim, assume that we are given $\left\{\{g_1, g_2, ..., g_k\}, g^x, g^{c_1}, g^{c_2}, ..., g^{c_k}\right\}$ to compute $g_k^{s.\prod_{i=1}^{k} c_i}$. We first compute $g_k^y = e(g^{c_1}, g^{c_2}, ..., g^{c_k})$, then we query $\mathcal{O}$ by $\left\{g^x, g_k^y\right\}$.

E. $(k-1)$-Distance Decisional Diffie-Hellman problem

Assume that we have a k-Multilinear map over groups $\mathbf{G}_1, \ldots, \mathbf{G}_k$ and are given vector $\left\{g^x, g_k^y, g_k^z\right\}$. We define the problem of deciding if $z = x.y$ or not as $(k-1)$-Distance Decisional Diffie-Hellman ($(k-1)$-DsDDH) problem. This problem is at least as hard as the (k-MDDH) problem. This claim can be proved similar to the hardness proof of $(k-1)$-DsDH.

III. The proposed ABE Scheme, Basic version

CP-ABE schemes for arithmetic circuits aim to realize the access policies consistent with all or a class of arithmetic functions $f(\mathbf{x}) = f(x_1, x_2, ..., x_n)$, $deg(f) \leq k$ where each x_i , $i = 1, 2, ..., n$ corresponds to one attribute and $\mathbf{x} = [x_1, x_2, ..., x_n]$ is the attribute vector. Note that n is the number of attributes and k is called the *depth* of function (circuit). The encryptor of the message can encrypt the ciphertext in a way that only the users whose attribute vectors satisfy $f(\mathbf{x}) = y$ can decrypt the ciphertext, where y is an encryptor-chosen value and is called the *result* and $f(\cdot)$ is chosen by the encryptor, as well, conditioned that it meets the limitations of the functions supported by the design, if any.

A. Limitations and Specifications

In this section, we propose a CP-ABE scheme which can be realized for access structures with arithmetic circuits of the following form.

$$f(\mathbf{x}) = \sum_{j=1}^{|S|} (a_j \prod_{i \in P_j} x_i) \tag{3}$$

where $P_j, j = 1, \ldots, 2^k$ is a subgroup of $\{1, 2, ..., k\}$. S is defined as the set of all P_j that a_j is nonzero. The cardinality of S is denoted by $|S|$.

for the CP-ABE proposed in this section, We are restricted to the functions that $k = n$, $\forall P_i, P_j \in S, i \neq j, P_i \cap P_j = \emptyset$. However, the proposed scheme works for any $y \in Z_q$ which is called the result. Moreover, in this scheme the user does not know the value of his/her own attribute vector as well as the value of result. All of these constraints will be relaxed in the schemes proposed in next sections.

B. Ciphertext Policy Attribute Based Encryption

The proposed CP-ABE scheme is a quadruple $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ of probabilistic polynomial time algorithms, which are described in the following.

$\mathsf{Setup}(\lambda, 1^k)$: This algorithm takes security parameter λ and the number of attributes n as input. Then, it outputs the public parameters (public keys) of the scheme and the master secret key.

The k groups of $\mathbf{G}_1, \mathbf{G}_2, ..., \mathbf{G}_k$ with generators $g_1, g_2, ..., g_k$ respectively, all with the prime order q, are selected as the public parameters of the scheme. A multilinear map $\{e_{i,j}; i, j \in \{1, \ldots, k-1\}\}$ which is defined over these groups is also public. For simplicity g_1 is denoted by g. TTP selects $2k$ random numbers $t_1, t_2, ..., t_k, s_1, s_2, ..., s_k$ from Z_q. Then, the public key PK and the master secret key MSK are generated, as below.

$$PK = \left\{[g^{t_1}, g^{t_2}, ..., g^{t_k}], [g^{\frac{1}{s_1}}, g^{\frac{1}{s_2}}, ..., g^{\frac{1}{s_k}}], [g^{\frac{t_1}{s_1}}, g^{\frac{t_2}{s_2}}, ..., g^{\frac{t_k}{s_k}}]\right\}$$
$$MSK = \{[t_1, t_2, \ldots, t_k], [s_1, s_2, \ldots, s_k]\} \tag{4}$$

$\mathsf{KeyGen}(MSK)$: This algorithm takes the master secret key MSK as input. Then, it outputs the user's secret key SK. For generating the user's secret keys, the values of $x_1, x_2, ..., x_n$ are chosen related to the value of the user's attributes. Then secret keys SK are generated as below.

$$SK = [sk_1, sk_2, ..., sk_k] = [s_1 x_1, s_2 x_2, ..., s_k x_k] \tag{5}$$

Note that the user, who have these secret keys, does not know the value of its own attributes, x_i.

$\mathsf{Enc}(PK, f, y, m)$: This algorithm takes public key PK, arithmetic function f consistent with the specification given in Sec. III-A, result y, and message m as input. It outputs the ciphertext Ctx which can be decrypted only by the users whose attribute vector $\mathbf{x}$ satisfies $f(\mathbf{x}) = y$.

Then, the encryptor chooses random numbers $r_1, r_2, \ldots, r_n$ such that $\forall P_j \in S$, $\prod_{i \in P_j} r_i = R$. Note that since P_js are disjoint, such a set of $r_1, r_2, \ldots, r_n$ always exists. Then, he computes $C_1, C_2, \ldots, C_k$ as follows.

$$C_1 = g^{\frac{r_1 t_1}{s_1}}, C_2 = g^{\frac{r_2 t_2}{s_2}}, \ldots, C_k = g^{\frac{r_k t_k}{s_k}} \tag{6}$$

and C_0 and $Check$ are also computed as

$$\begin{aligned} C_0 &= m.(g_k^{\prod_{v=1}^{k} t_v})^{y.R} \\ Check &= g_k^{y} \end{aligned} \tag{7}$$

Finally, the ciphertext is generated as below:

$$Ctx = [f, C_0, C_1, C_2, ..., C_k, Check] \tag{8}$$

The value of $Check$ is used for checking the result of the function. The value of $g_k^{\prod_{i=1}^{k} t_i}$ can be easily computed by applying a multilinear map as follows.

$$\begin{aligned} e_k(g^{t_1}, g^{t_2}, ..., g^{t_k}) &= e_{k-1,1}(...e_{21}(e_{11}(g^{t_1}, g^{t_2}), g^{t_3})..., g^{t_k}) \\ &= g_k^{\prod_{v=1}^{k} t_v} \end{aligned} \tag{9}$$

The above computation can be done in the KeyGen algorithm by TTP and be defined as a piece of public key.

$\mathsf{Dec}(Ctx, PK, SK)$: This algorithm is a deterministic algorithm that takes ciphertext Ctx, public key PK and the secret key SK as input and outputs message m only if Ctx is an encryption of m under public key PK and $f(\mathbf{x}) = y$.

The decryptor first computes $I_{P_i}, i = 1, \ldots, |S|$ as follows.

$$I_{P_i} = e(C_{p_{i_1}}, C_{p_{i_2}}, ..., C_{p_{i_w}}, g^{t_{j_1}}, g^{t_{j_2}}, ..., g^{t_{j_{(k-w)}}}) \tag{10}$$

where $P_i = \{p_{i_1}, ..., p_{i_w}\}$, $w = |P_i|$ and $\{1, \ldots, k\} \setminus P_i = \{p_{j_1}, ..., p_{j_{(k-w)}}\}$. Then, he computes $Mask$, and decrypts the ciphertext Ctx into message m' as follows.

$$\begin{aligned} Mask &= \prod_{i=1}^{|S|} (I_{P_i})^{a_{P_i} \prod_{j \in P_i} sk_j} \\ m' &= \frac{C_0}{Mask} \end{aligned} \tag{11}$$

The correctness of equation (11) is as follows. We first

simplify (10) acording to the following.

$$\begin{aligned} I_{P_i} &= g_k^{\prod_{j\in P_i}(\frac{r_j \cdot t_j}{s_j})\cdot\prod_{v\notin P_i} t_v} \\ &= g_k^{\frac{\prod_{j\in P_i}(r_j)}{\prod_{j\in P_i}(s_j)}\cdot\prod_{v=1}^{k} t_v} \\ &= g_k^{\frac{R}{\prod_{j\in P_i}(s_j)}\cdot\prod_{v=1}^{k} t_v} \end{aligned} \quad (12)$$

So, the value of $Mask$ is equal to

$$\begin{aligned} Mask &= \prod_{i=1}^{|S|} (I_{P_i})^{a_{P_i}\prod_{j\in P_i} sk_j} \\ &= \prod_{i=1}^{|S|} \left(g_k^{\frac{R}{\prod_{j\in P_i}(s_j)}\prod_{v=1}^{k} t_v}\right)^{a_{P_i}\prod_{j\in P_i} s_j x_j} \\ &= \prod_{i=1}^{|S|} g_k^{R\cdot a_{P_i}(\prod_{j\in P_i}(x_j))\prod_{v=1}^{k} t_v} \\ &= g_k^{\left(\sum_{i=1}^{|S|}\left(a_{P_i}\cdot\prod_{j\in P_i} x_j\right)\right)R.\prod_{v=1}^{k} t_v} \\ &= g_k^{f(\mathbf{x}).R\prod_{v=1}^{k} t_v} \end{aligned} \quad (13)$$

Finally, equations (13) along with (7) yeilds (11).

For example, assume that $S = \{P_1, P_2\}$ where $P_1 = \{1, 3\}$ and $P_2 = \{2\}$. $a_{(P_1)} = a_1, a_{(P_2)} = a_2$ and $f(\mathbf{x}) = a_1x_1x_3 + a_2x_2$. So, the value of $Mask$ is as follows.

$$\begin{aligned} Mask &= \prod_{i=1}^{2} (I_{P_i})^{a_{P_i}\prod_{j\in P_i} sk_j} \\ &= (I_{P_1})^{a_{P_1}\prod_{j\in P_1} sk_j} \cdot (I_{P_2})^{a_{P_2}\prod_{j\in P_2} sk_j} \\ &= (I_{P_1})^{a_1\prod_{j\in\{1,3\}} sk_j} \cdot (I_{P_2})^{a_2\prod_{j\in\{2\}} sk_j} \\ &= (I_{P_1})^{a_1(s_1x_1.s_3x_3)} \cdot (I_{P_2})^{a_2(s_2x_2)} \\ &= g_3^{R\cdot a_1x_1x_3\prod_{v=1}^{3} t_v} \cdot g_3^{R\cdot a_2x_2\prod_{v=1}^{3} t_v} \\ &= g_3^{R(a_1x_1x_3+a_2x_2)\prod_{n=1}^{3} t_n} \\ &= g_k^{f(\mathbf{x}).R\prod_{n=1}^{k} t_n} \end{aligned} \quad (14)$$

Since the attribute vector and the result are hidden for the decryptor, it should check if $Check = g_k^{f(\mathbf{x})}$ to make sure that the decryption is correct and $m' = m$. The decryptor computes $g_k^{f(\mathbf{x})}$ by computing the following.

$$\begin{aligned} Check' &= \prod_{P_i\in S} e\left((g^{\frac{1}{s_{p_1}}})^{sk_{p_1}}, \ldots, (g^{\frac{1}{s_{p_{|P_i|}}}})^{sk_{p_{|P_i|}}}\right)^{a_{P_i}} \\ &= \prod_{P_i\in S} e\left(g^{x_{p_{i_1}}}, \ldots, g^{x_{p_{i_{|P_i|}}}}\right)^{a_{P_i}} \\ &= \prod_{P_i\in S} g_k^{a_{P_i}\prod_{j\in P_i} x_j} \\ &= g_k^{f(\mathbf{x})} \end{aligned} \quad (15)$$

If the result of equation (15) is equal to the received $Check$ value, the receiver will conclude that he is an authorized user to decryption.

C. Security Proof

In this section we prove that the proposed scheme in Sec. III-B acheieves adaptive security.

We show that if there exist a polynomial-time attacker $\mathcal{A}$ for the proposed ABE system for arithmetic circuit with k variables in the adaptive security game, then we can construct a polynomial time algorithm for solving $(k-1)$-DsDDH problem with nonnegligible advantage. The adaptive security game is as below.

We assume that, attacker $\mathcal{A}$ can distinguish between two ciphertexts of messages m_0 and m_1 with a probability of $\frac{1}{2} + \epsilon$, where ϵ is a non-negligible value. We prove that if this attacker exists then there is a polynomial-time challenger Sim that can solve $(k-1)$-DsDDH problem with a probability nonnegligibly greater than $\frac{1}{2}$. In this model, the challenger gets the $(k-1)$-DsDDH parameters then simulate the above scheme parameters to attacker $\mathcal{A}$. The attacker $\mathcal{A}$ adaptively request for secret keys. Then challenger creates secret keys to the attacker. At the next time, the attacker chooses two messages m_0 and m_1 which he sends to the challenger. The challenger randomly chooses one of these messages and simulate Enc algorithm to receive Ctx. Then challenger sends it to $\mathcal{A}$. The attacker $\mathcal{A}$ should decide which message was encrypted and sends the result to the challenger. The challenger can solve to k-MDDH problem according to the received result.

Theorem 1. *Our scheme (section III-B) achieves adaptive security for arithmetic function of the form (19) with k variables under $(k-1)$-DsDDH assumption*

Proof. We follow the adaptive security game and conclude that if there exist the polynomial-time attacker $\mathcal{A}$ that distinguish between two encrypted messages in the proposed scheme, with nonnegligible advantage, then the challenger can construct a polynomial-time algorithm for solving $(k-1)$-DsDDH problem with nonnegligible advantage. The security game for our scheme is as follows.

1) The challenger achieves the $(k-1)$-DsDDH parameters as below.

$$\{\mathbf{G}_1, \mathbf{G}_2, ..., \mathbf{G}_k, g = g_1, g_2, ..., g_k, g^x, g_k^y, g_k^z\}$$

The challenger must distinguish if $z = x \cdot y$ or it is a random value.

2) The challenger randomly chooses $t_1, t_2, ..., t_{k-1} \in Z_q$ and computes $g^{t_i}; 1 \le i \le k-1$. Then, it sets $g^{t_k} = g^{x\cdot\prod_{i=1}^{k-1} r_i^{-1}}$. The challenger also selects random values s_i and computes $g^{\frac{t_i}{s_i}}$ for all $1 \le i \le k$. Then it runs Setup algorithm for simulating public parameters PP and public key PK. Then, challenger sends the public parameters to attacker $\mathcal{A}$ as follows.

PP :

$$\{\mathbf{G}_1, \mathbf{G}_2, ..., \mathbf{G}_k, g = g_1, g_2, ..., g_k\}$$

PK :

$$\begin{bmatrix} g^{t_1} & g^{t_2} & ... & g^{t_k} \\ g^{\frac{t_1}{s_1}} & g^{\frac{t_2}{s_2}} & ... & g^{\frac{t_k}{s_k}} \\ g^{\frac{1}{s_1}} & g^{\frac{1}{s_2}} & ... & g^{\frac{1}{s_k}} \end{bmatrix} \quad (16)$$

3) $\mathcal{A}$ requests the challenger for secret keys SK after receiving public parameters and public keys. The challenger selects a k-tuple random numbers as values of attribute vector then, multiplying by $s_i, 1 \leq i \leq k$, it generates secret keys. Then the challenger sends them to the attacker after any request.
4) $\mathcal{A}$ chooses the challenge function $f(\mathbf{x})$ and two messages m_0 and m_1, as well. Then, it sends $f(\mathbf{x})$, m_0, and m_1 to the challenger.
5) The challenger randomly chooses one of the two messages m_0 and m_1. Then Sim runs algorithm Enc to simulate the ciphertext of m_b that $b \in_r \{0, 1\}$. The ciphertext Ctx is as below.

$$\begin{aligned} Ctx \quad = \quad & [f,\ C_0 = m_b.(g_k^z)^R, \\ & C_1 = g^{\frac{r_1 t_1}{s_1}}, C_2 = g^{\frac{r_2 t_2}{s_2}}, ..., C_k = g^{\frac{r_k t_k}{s_k}}, \\ & Chek = g_k^y] \end{aligned} \quad (17)$$

The challenger sends Ctx to the attacker.
6) The attacker can request secret keys adaptively after receiving Ctx. The challenger solves these requests similar to Step 3.
7) The attacker sends the the guessed value b' to the challenger.

The probability of success of challenger for distinguishing problem $(k-1)-$DsDDH is as follows.

$$\begin{aligned} Pr[\mathsf{Sim}_{(k-1)-\text{DsDDH}} = \text{success}] \quad &= \quad \frac{1}{2} \cdot (\frac{1}{2} + \epsilon) + \frac{1}{2} . \frac{1}{2} \\ &= \quad \frac{1}{2} + \frac{\epsilon}{2} \end{aligned} \quad (18)$$

In the above equation, the probability of resolving $(k-1)-$DsDDH problem is non-negligibly greater than $\frac{1}{2}$. So the attacker $\mathcal{A}$ does not exist because $(k-1)-$DsDDH problem is assumed to be hard. □

IV. The Improved Scheme I, hidden result and attributes

In this section, we propose an improved version of the basic CP-ABE scheme for arithmetic circuits, proposed in Sec. III, which does not have the limitations of the basic scheme. This scheme has the property that the attribute vector and result value are both hidden to the user.

A. Specifications

The arithmetic function that this scheme can realize as access structure is of the following form:

$$f(\mathbf{x}) = \sum_{j=1}^{|S|} \left(a_j \prod_{i \in P_j} x_i^{u_i}\right) \quad (19)$$

where P_j, S and a_j are defined as previous. In this scheme, $n \geq k$ and the constraint of $P_i \cap P_j = \emptyset$ is not required any more. Moreover, the value of attribute vector as well as the result are hidden to the user.

B. Ciphertext Policy Attribute Based Encryption Scheme

This version of proposed CP-ABE scheme, is similar to the basic scheme, introduced in Sec. III-B, with the following modifications in the quadruple $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

$\mathsf{Setup}(\lambda, 1^k)$. The only changes are on the public key and master secret key which are as below.

$$PK = \{[g^{t_1}, g^{t_2}, \cdots, g^{t_k}], [g^{\frac{1}{s_1}}, g^{\frac{1}{s_2}}, \cdots, g^{\frac{1}{s_n}}], \begin{bmatrix} g^{\frac{t_1}{s_1}} & g^{\frac{t_2}{s_1}} & \cdots & g^{\frac{t_k}{s_1}} \\ g^{\frac{t_1}{s_2}} & g^{\frac{t_2}{s_2}} & \cdots & g^{\frac{t_k}{s_2}} \\ \vdots & \vdots & \ddots & \vdots \\ g^{\frac{t_1}{s_n}} & g^{\frac{t_2}{s_n}} & \cdots & g^{\frac{t_k}{s_n}} \end{bmatrix}\}$$

$$MSK = \{[t_1, t_2, ..., t_k], [s_1, s_2, ..., s_n]\} \quad (20)$$

$\mathsf{KeyGen}(MSK)$. The secret keys of users are generated similar to the basic scheme (5).

$\mathsf{Enc}(PK, f, m)$. The ciphertext is computed according to the following equation.

$$\begin{aligned} Ctx \quad = \quad & [f,\ C_0 = m.(g_k^{\prod_{v=1}^{k} t_v})^{y.R}, Check = g_k^y, \\ & \mathbf{C}_1, \mathbf{C}_{P_2}, \cdots, \mathbf{C}_{P_{|S|}}] \end{aligned} \quad (21)$$

where

$$\mathbf{C}_{P_j} = [C_{p_{j_1}}, C_{p_{j_2}}, ..., C_{p_{j_{|P_j|}}}], \forall P_j \in S \quad (22)$$

and $C_{p_{j_i}} = g^{\frac{r_{P_{j_i}} . t_{P_{j_i}}}{s_{P_{j_i}}}}$. Note that $\prod_{i=1}^{|P_j|} r_{p_j}^{u_{p_j}} = R$.

$\mathsf{Dec}(Ctx, PK, SK)$ The decryption algorithm is exactly the same as the basic scheme.

C. Security proof

The security proof of this scheme is completely similar to the security proof of the basic scheme brought in Sec. III-C.

V. The Improved Scheme II, Disclosed attributes, Hidden result

In the two previous schemes the attribute vector is hidden to its owner. Depending on the application, such a property may be desired or not. In this section, we present a variant of the proposed scheme in which the values of the attributes are known by the attribute-owner.

A. limitations and specifications

The function $f(\mathbf{x})$ which can be supported by this scheme as access structure is the same as the improved scheme characterized in Sec. IV-A. The only difference is that, the value of result y is hidden to the user, however the attribute vector is known to its owner.

B. The scheme

In this section we highlight only those part of algorithms (Setup, KeyGen, Enc, Dec) that have changed comparing to the basic scheme in Sec. IV-B.

Setup. The order of all the groups generated in Setup algorithm must be of the form $q = 2N+1$ where $N = q_1 q_2$ is a RSA number. Furthermore, the Discrete Logarithm Problem in any subgroups of these groups of order q_1 and q_2 must be hard. This is to ensure that discrete logarithm problem is unsolvable by Pohling-Hellman algorithm [30]. Having these assumptions, computing the value of $\varphi(\varphi(q)) = \varphi(q-1) = \varphi(2N) = \varphi(N)$ is hard without having the factorization of N, where $\varphi(\cdot)$ is the Euler function. Note that, we have

$$g^{[x^{\varphi(\varphi(q))}]} \bmod q = g^{[x^{\varphi(\varphi(q))} \bmod \varphi(q)]} \bmod q = g^x \qquad (23)$$

The idea of the disclosed attributes is based on equality given in (23). The factorization of N are included in MSK.

KeyGen. In this variant, the secret key, SK, is as below:

$$\begin{aligned} SK &= [sk_1, sk_2, \ldots, sk_n] \\ &= [s_1 x_1^{\varphi(\varphi(p))}, s_2 x_2^{\varphi(\varphi(p))}, \ldots, s_n x_n^{\varphi(\varphi(p))}] \end{aligned} \qquad (24)$$

The Enc and Dec algorithms are the same as IV-B. All the equations **??**, **??** and **??** are valid here due to equation (23).

C. Security Proof

The security proof of this scheme is similar to the security proof of basic scheme brought in III-C, tough with some differences. The adaptive security game for the improved scheme II, is as follows.

1) The challenger receives the $(k-1)$-DsDDH parameters as follows.

   $$\{\mathbf{G}_1, \mathbf{G}_2, ..., \mathbf{G}_k, g_1, g_2, ..., g_k, g^x, g_k^y, g_k^z\}$$

   where $g_1 = g$. The order of all groups is $p = 2N+1$. The challenger also recieves the factorization of N. It must distinguish if of $z = x \cdot y$ or it is a random element of Z_p.
2) The challenger randomely chooses $(k-1)$ values $t_1, t_2, ..., t_{k-1}$ and computes $g^{t_i}, i = 1, \ldots, k-1$. Then, it sets $g^{t_k} = g^x \prod_{i=1}^{k-1} r_i^{-1}$. The challenger also selects random values s_j and computes $g^{\frac{t_i}{s_j}}$, $i = 1, \ldots, k, j = 1, \ldots, n$. Then challenger runs Setup algorithm for simulating the public parameters PP and public keys PK. Then, challenger sends the public parameters to the attacker $\mathcal{A}$ as below.

   $$PP = \{\mathbf{G}_1, \mathbf{G}_2, ..., \mathbf{G}_k, g = g_1, g_2, ..., g_k\}$$

   $$PK = \{[g^{t_1}, g^{t_2}, \cdots, g^{t_k}], [g^{\frac{1}{s_1}}, g^{\frac{1}{s_2}}, \cdots, g^{\frac{1}{s_n}}], \begin{bmatrix} g^{\frac{t_1}{s_1}} & g^{\frac{t_2}{s_1}} & \cdots & g^{\frac{t_k}{s_1}} \\ g^{\frac{t_1}{s_2}} & g^{\frac{t_2}{s_2}} & \cdots & g^{\frac{t_k}{s_2}} \\ \vdots & \vdots & \ddots & \vdots \\ g^{\frac{t_1}{s_n}} & g^{\frac{t_2}{s_n}} & \cdots & g^{\frac{t_k}{s_n}} \end{bmatrix}\}$$

   Note that the challenger keeps the value of q_1 and q_2 secret as a part of the master secret key.
3) The attacker $\mathcal{A}$ requests the secret keys SK corresponding to his selected attribute vector $\mathbf{x} = [x_1, x_2, ..., x_n]$ from the challenger. Having received the public parameters and public keys, the challenger computes $s_i x_i^{\varphi(\varphi(p))}, i = 1, \ldots, n$ and sends them to $\mathcal{A}$ as secret keys.
4) The attacker chooses the challenge function $f(\mathbf{x})$. It also chooses two messages m_0 and m_1. Then, the attacker sends $f(\mathbf{x}), m_0, m_1$ to the challenger.
5) The challenger randomly chooses one of the two messages m_0 and m_1. Then the challenger Sim runs the algorithm Enc to simulate the ciphertext of m_b that $b \in_r \{0, 1\}$. The ciphertext Ctx is simulated as follows and sends it to the attacker.

   $$\begin{aligned} Ctx &= [f,\ C_0 = m.(g_k^z)^R, Check = g_k^y, \\ &\quad \mathbf{C}_1, \mathbf{C}_{P_2}, \cdots, \mathbf{C}_{P_{|S|}}] \end{aligned} \qquad (25)$$

6) The attacker can request secret keys adaptively again after receiving Ctx. The challenger resposes to these requests like step 3.
7) the attacker sends the value of guessed b' to the challenger.

The probability of success of challenger to distinguish problem $(k-1)$-DsDDH is as below:

$$\begin{aligned} Pr[\mathsf{Sim}_{(k-1)-\mathrm{DsDDH}} = \text{success}] &= \frac{1}{2} \cdot (\frac{1}{2} + \epsilon) + \frac{1}{2} \cdot \frac{1}{2} \\ &= \frac{1}{2} + \frac{\epsilon}{2} \end{aligned} \qquad (26)$$

In the above equation, the probability of solving $(k-1)$-DsDDH problem is greater than $\frac{1}{2}$ since $\frac{\epsilon}{2}$ has been considered non-negligible. So, the attacker $\mathcal{A}$ does not exist because the $(k-1)$-DsDDH problem is hard.

VI. Comparison with Boneh's scheme

Comparing to the only ABE scheme for arithmetic functions, proposed by Boneh [21], the proposed schemes in this paper have several advantages, which are listed in the following.

1) The proposed schemes are CP-ABE which is more flexible than KP-ABE.

2) The value of result in our scheme is arbitrary. But, Boneh's scheme just supports $y = 0$, though it can be modified to work for any arbitrary result.
3) The proposed schemes can support both hidden or disclosed attribute values. However, in Boneh's scheme the values of attributes can not be kept hidden, so this scheme can not be used as predicate encryption.
4) In Boneh's scheme, the values of attributes must be in $[-p, p]$, where p is less than the group order q, for **Mult** gates. However, our scheme does not put any constraint on the values of attributes.
5) Despite Boneh's scheme which has selective security, the proposed schemes have adaptive security which is stronger.
6) Despite [21], our scheme can support the exponentiation gate, tough it seems that this feature can be added to Boneh's scheme.
7) since [21] is a lattice-based scheme, the copmutational complexity and key sizes of the keys are larger than our scheme.

However, the disadvantage of our scheme comparing to Boneh's scheme is that our scheme is not post-quantum.

VII. Conclusion

We proposed some CP-ABE schemes for arithmetic circuit access structures. The proposed scheme relies on multilinear maps. We defined the new concept of hidden results ABE which refers to the ABE scheme for arithmetic functions in which the result value for the function is unknown.

In the first proposed scheme, the attribute vector and the result value are hidden to the users. It relies on a k-multilinear map and supports a number of $n = k$ attributes. The improved scheme I works for any number of $n \geq k$ attributes, conditioned that the degree of the function is at most k. In this scheme, the attribute vector and the result value are hidden to the users, too. Finally, we proposed the improved scheme II, where the attribute vector is not hidden to the users and the result value, would become disclosed to users who can decrypt the ciphertext. However, the order of groups must be greater the first two schemes.

We proved that these schemes are adaptively secure under a new defined hardness assumption, called k-Distance Decisional Diffie-Hellman problem, which is at least as hard as the well known k-multilinear decisional Diffie-Hellman problem. Finally, we compared our schemes with Boneh et al.'s scheme and described the advantages of ours.

References

[1] Sahai, A. and Waters, B., 2005, May. Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 457-473). Springer, Berlin, Heidelberg.

[2] Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006, October. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98).

[3] Bethencourt, J., Sahai, A. and Waters, B., 2007, May. Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07) (pp. 321-334). IEEE.

[4] Waters, B., 2011, March. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In International Workshop on Public Key Cryptography (pp. 53-70). Springer, Berlin, Heidelberg.

[5] Ostrovsky, R., Sahai, A. and Waters, B., 2007, October. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 195-203).

[6] Green, M., Hohenberger, S. and Waters, B., 2011, August. Outsourcing the decryption of abe ciphertexts. In USENIX security symposium (Vol. 2011, No. 3).

[7] Lewko, A., Sahai, A. and Waters, B., 2010, May. Revocation systems with very small private keys. In 2010 IEEE Symposium on Security and Privacy (pp. 273-285). IEEE.

[8] Hur, J. and Noh, D.K., 2010. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems, 22(7), pp.1214-1221.

[9] Chase, M., 2007, February. Multi-authority attribute based encryption. In Theory of cryptography conference (pp. 515-534). Springer, Berlin, Heidelberg.

[10] Attrapadung, N. and Imai, H., 2009, June. Dual-policy attribute based encryption. In International Conference on Applied Cryptography and Network Security (pp. 168-185). Springer, Berlin, Heidelberg.

[11] Zou, X., 2013. A hierarchical attribute-based encryption scheme. Wuhan University Journal of Natural Sciences, 18(3), pp.259-264.

[12] Attrapadung, N., Libert, B. and De Panafieu, E., 2011, March. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In International Workshop on Public Key Cryptography (pp. 90-108). Springer, Berlin, Heidelberg.

[13] Li, J., Lin, X., Zhang, Y. and Han, J., 2016. KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Transactions on Services Computing, 10(5), pp.715-725.

[14] Koppula, V. and Waters, B., 2019, August. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. In Annual International Cryptology Conference (pp. 671-700). Springer, Cham.

[15] Brakerski, Z. and Vaikuntanathan, V., 2016, August. Circuit-ABE from LWE: unbounded attributes and semi-adaptive security. In Annual International Cryptology Conference (pp. 363-384). Springer, Berlin, Heidelberg.

[16] Garg, S., Gentry, C., Halevi, S., Sahai, A. and Waters, B., 2013, August. Attribute-based encryption for circuits from multilinear maps. In Annual Cryptology Conference (pp. 479-499). Springer, Berlin, Heidelberg.

[17] Agrawal, S., Boyen, X., Vaikuntanathan, V., Voulgaris, P. and Wee, H., 2011. Fuzzy Identity Based Encryption from Lattices. IACR Cryptol. ePrint Arch., 2011, p.414.

[18] Boyen, X., 2013, March. Attribute-based functional encryption on lattices. In Theory of Cryptography Conference (pp. 122-142). Springer, Berlin, Heidelberg.

[19] Zhang, J. and Zhang, Z., 2011, November. A ciphertext policy attribute-based encryption scheme without pairings. In International Conference on Information Security and Cryptology (pp. 324-340). Springer, Berlin, Heidelberg.

[20] Gorbunov, S., Vaikuntanathan, V. and Wee, H., 2015. Attribute-based encryption for circuits. Journal of the ACM (JACM), 62(6), pp.1-33.

[21] Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V. and Vinayagamurthy, D., 2014, May. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 533-556). Springer, Berlin, Heidelberg.

[22] Zhu, W., Yu, J., Wang, T., Zhang, P. and Xie, W., 2014. Efficient attribute-based encryption from R-LWE. Chin. J. Electron, 23(4), pp.778-782.

[23] Fun, T.S. and Samsudin, A., 2015, August. Lattice ciphertext-policy attribute-based encryption from ring-LWE. In 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET) (pp. 258-262). IEEE.

[24] Chen, Z., Zhang, P., Zhang, F. and Huang, J., 2017. Ciphertext policy attribute-based encryption supporting unbounded attribute space from R-LWE. TIIS, 11(4), pp.2292-2309.

[25] Tsabary, R., 2019, August. Fully secure attribute-based encryption for t-CNF from LWE. In Annual International Cryptology Conference (pp. 62-85). Springer, Cham.

[26] Katz, J., Sahai, A. and Waters, B., 2008, April. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In annual international conference on the theory and applications of cryptographic techniques (pp. 146-162). Springer, Berlin, Heidelberg.

[27] Boneh, D., Sahai, A. and Waters, B., 2011, March. Functional encryption: Definitions and challenges. In Theory of Cryptography Conference (pp. 253-273). Springer, Berlin, Heidelberg.

[28] Belguith, S., Kaaniche, N., Laurent, M., Jemai, A. and Attia, R., 2018. Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. Computer Networks, 133, pp.141-156.

[29] Xiong, H., Zhao, Y., Peng, L., Zhang, H. and Yeh, K.H., 2019. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing. Future Generation Computer Systems, 97, pp.453-461.

[30] Pohlig, S. and Hellman, M., 1978. An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (Corresp.). IEEE Transactions on information Theory, 24(1), pp.106-110.