Leakage-resilient Attribute-based Encryption with CCA2 Security

Leyou Zhang and Yujie Shang
(Corresponding author: Yujie Shang)

School of Mathematics and Statistics, Xidian University
Xi'an, Shaanxi 710071, China
(Email: yjshang123@163.com)

(Received Jan. 22, 2018; Revised and Accepted July 13, 2018; First Online June 5, 2019)

Abstract

Leakage-resilient Attribute-Based Encryption (ABE) is one of efficient methods to solve the side-channel attacks. However, most of existing works only achieved a weak security-CPA security and were not practical. Few works are focused on strong security-CCA security which is left as an open problem. In this paper, we solve this problem and construct directly a CCA secure ABE. For the sake of realizing this target, a CPA secure scheme is introduced at first. Based on this basic scheme, a λ-leakage resilient CCA2 secure ABE is proposed in the standard model. It tolerates up to $(\log p - \omega(\log \kappa))$-bit leakage of the private key and its leakage parameter is independent of the message length, where κ is the security parameter and p is the prime order of the underlying group. Additionally, the proposed scheme is efficient and practical over the available, where the private keys are constant and independent of depth of attributes of the users. It also achieves anonymity and full security.

Keywords: Attribute-Based Encryption; Bounded Memory Leakage; Chosen Ciphertext Security; Leakage-Resilient

1 Introduction

1.1 Background

Leakage-resilient cryptography: In traditional cryptography, security guarantees are proven under the assumption that the secret key must be kept safely and other internal state is not leaked to the adversary. Even if a single bit of these secrets is leaked, the protection guaranteed by the proof is lost. However, the study of side-channel attack [14] and cold-boot attack [12] shows that this idealized assumption does not hold in real life. Through the side-channel attack, malicious users that exploit the physical nature of cryptographic operations (such as timing, power, radiation, *etc.*) or the reuse of the secret key or the randomness in a number of applications can get some information of secret key. Cold-boot attack that exploits physical property of DRAM chip also brings great threats to computer systems. Traditional cryptography is not hard enough to resist these attacks, so leakage-resilient cryptography emerges as the times require. Recently many leakage-resilient models are proposed. Each model has its own strengths and weakness, which is appropriate for specific attacking scenarios and inadequate for others. These models are summarized as follows.

Only computation leaks information: This model was considered by Micali *et al.* [18] to deal with physical observation via side channel attacks. In this model, one assumes that leakage occurs every time the device performs a computation, but that any parts of the memory not involved in the computation cannot be leaked. However, this model fails to capture a wide range of devastating attacking scenarios. In these attacks information about the entire secret state can leak even if no computation takes place. This motivates consideration of more general models.

Relative leakage model (memory-attacks model): Alwen *et al.* [2] introduced the relative leakage model in which the adversary can learn arbitrary information about secret keys, with the only restriction that the number of leaked bits is bounded by some parameter λ.

Bounded retrieval model: This model is strictly stronger than the relative leakage model. In this model, the leakage parameter λ is an arbitrary and independent parameter of the system. The size of secret keys can be increased to allow λ bits of leakage, without affecting the public key size, communication and computation efficiency. It has been employed in many constructions of cryptographic primitives.

Continual leakage model: The above line of research bounds the leakage throughout the entire lifetime of the secret keys. Another paradigm considered continual leakage model in which the leakage from the secret memory is bounded per time period, but unbounded overall. Constructions of cryptographic primitives secure in this model include identity-based encryption (IBE) [15] and attribute-based encryption (ABE) [29] schemes.

Auxiliary input model: To further relax the restriction, Dodis *et al.* [8] studied auxiliary inputs, which allow any f that no polynomial time adversary can invert with non-negligible probability. Yuen *et al.* [27] proposed the first IBE scheme that is proved secure even when the adversary is equipped with auxiliary inputs. In [27], they also proposed the model of continual auxiliary leakage (CAL) that combines the concepts of auxiliary inputs with continual memory leakage. This model allows continual leakage and the leakage between updates has minimal restriction. More precisely, no polynomial time algorithm can use the leaked information to output valid secret keys.

Akavia *et al.* [1] first introduced the concept of key leakage. To generalize the leakage, it is assumed that there is a leakage oracle and the adversary can make query to the leakage oracle adaptively. However, in order to avoid obtaining the full content of the secret information for adversary, the system must be designed to consider the amount of leakage that the system can tolerate, for which the number of leakage information obtained by the adversary need to be limited. In this paper, we focus on bounded memory-leakage model(or relative leakage model) [1], where the adversary is allowed to learn arbitrary information about the secret key, with the only restriction that the number of leakage bits is bounded by some parameter λ. Recently, the bounded memory-leakage model has received considerable attentions.

1.2 Attribute-Based Encryption

Attribute-based encryption: Sahai and Waters [21] presented the concept of Attribute-Based Encryption (ABE). The earliest ABE scheme can only support threshold access control. Later, in order to achieve more flexible access control, Goyal *et al.* [11] further constructed Key-Policy ABE (KP-ABE), where attributes are used to annotate the ciphertexts and formulas over these attributes are ascribed to users' secret keys. In particular, they proposed complementary form of KP-ABE, *i.e.* Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In this paper, our concern is CP-ABE. CP-ABE is complementary in that attributes are associated with the user's credentials and the formulas over these credentials are attached to the ciphertext by the encrypting party. Subsequently, Bethencourt *et al.* [4] constructed the first CP-ABE scheme where access structures are described by a monotonic "access tree". However, this scheme proved its security under the generic bilinear group model. Then Waters [26] presented more efficient and expressive CP-ABE. Moreover, they presented a new methodology for realizing CP-ABE system from a general set of access structures in the standard model under concrete and non-interactive assumptions. However, ciphertext size scales linearly with the complexity of the access formula in [26]. In subsequent work, Hohenberger *et al.* [13] presented online/offline ABE to address the problem that encryption and key generation computational coats scale with the complexity of the access policy or number of attributes. Chung *et al.* [6] surveyed various access policy attribute- based proxy re-encryption schemes and analyzed these schemes. In addition, they listed the comparisons of them by some criteria. Liu *et al.* [16] also surveyed related studies of ABE in cloud data storage with revocation and defined their requires. Rouselakis *et al.* [20] proposed an efficient large-universe multi-authority CP-ABE system in 2015. Their construction achieves maximum versatility by allowing multiple authorities to control the key distribution for an exponential number of attributes. Recently, Takashima [23] proposed new proof techniques for DLIN-based adaptively secure ABE, which allow attribute reuse in an available formula without the previously employed redundant multiply encoding technique.

1.3 Related Work

Leakage-resilient attribute-based encryption: Attribute-based encryption (ABE) has been a hot area at present since it can support fine-grained access control for encrypted data in cloud. It is a great challenge to design leakage-resilient attribute-based encryption scheme in the context of leakage resilience.

Akavia *et al.* [1] defined a new attack called "memory attack"(including adaptive memory attacks and non-adaptive memory attacks), which was inspired by "cold-boot attack" introduced by Halderman *et al.* [12]. Moreover, it showed that public-key encryption scheme proposed by Oded [19], and the IBE scheme proposed by Gentry, Peikert and Vaikuntanathan [10] can withstand memory attacks. Subsequently, Alwen *et al.* [2] constructed the first leakage-resilient public-key encryption scheme in the Bounded-Retrieval Model (BRM), provided security against various forms of adversarial "key leakage" attacks. Furthermore, it presented the concept of "Identity-Based Hash Proof System" (IB-HPS) and constructed three schemes based on IB-HPS. The first scheme is secure in the standard model, while the latter two rely on the Random Oracle Model. In the same year, Alwen *et al.* [3] constructed an efficient three-round leakage-resilient authenticated key agreement protocols (AKA), but in the Random-Oracle Model. In 2010, Chow *et al.* [5] designed the first Leakage-Resilient Identity-Based Encryption (LR-IBE) systems from static assumptions by using hash proof technique in the standard model. They constructed three schemes based on BRM. The first one based on Boneh-Boyen IBE is only selectively secure under the simple Decisional Bilinear Diffie-Hellman assumption (DBDH). Although the second one based on Waters IBE achieves full security, it has longer parameter size. The third system is based on Lewko-Waters IBE, and achieves full security with shorter public parameters, but is based on three static assumptions related to composite order bilinear groups. In 2013, Zhang *et al.* [29] presented two leakage-resilient attribute-based encryption schemes, LR-CP-ABE and LR-KP-ABE. The schemes have higher decryption efficiency, however, they are proven to be adaptively secure in composite order bilinear groups. In 2015, Bayat *et al.* [17] proposed a secure attribute key agreement protocol resilient to KCI attack in the random oracle model. In 2016, Zhang *et al.* [28] presented efficient leakage-resilient ABE schemes that achieve shorter secret key size. Moreover, they are proved adaptively secure in the standard model. However, none of the above schemes can achieve CCA secure, so it is significant to construct a CP-ABE scheme that achieves CCA security in the context of leakage resilience.

Our contributions: We aim at CCA secure CP-ABE construction in this paper. And two CP-ABE schemes are proposed based on q-ABDHE assumption. The first one is CPA secure and the other one is CCA2 secure in the standard model. Our schemes are simple and practical. Inspired by the above challenge, we prove its security by using the practical Cramer-Shoup cryptosystem [7]. The proposed scheme supports express access control by a AND gate [9] and achieves anonymity in the standard model. The leakage bound of the main scheme is $(\log p - \omega(\log \kappa))$, where κ is the security parameter and p is the prime order of the underlying group. The ciphertext size of the scheme is $5 \log p$ and encryption needs $3n + 1$ exponential operations which has lower computation complexity than the available. As we have seen, this is the first practical leakage-resilient fully CCA2 secure ABE scheme in the standard model and the leakage parameter of which is independent of the message length. However, the leakage ratio here is still approximately equal to 1/6. Increasing the leakage ratio will be the direction of our efforts in the future.

1.4 Organization

The rest paper is organized as follows. Section 2 describes some preliminaries which includes some basic notations, definitions and security model. The basic construction and security analysis will be presented in Section 3. The main construction will be presented in Section 4 and followed with security analysis in Section 5. Section 6 gives a detailed performance analysis. At last, we end this work with a brief conclusion.

2 Preliminaries

2.1 Notations

Let κ denote the security parameter. For a randomized algorithm $A(\cdot), a \leftarrow A(\cdot)$ denotes running the algorithm and obtaining a as an output, which is distributed over the internal random coins of A. PPT and $nelg(\kappa)$ denote probabilistic polynomial time and a negligible function of κ, respectively.

2.2 Bilinear Maps and Complexity Assumption

Definition 1. *Bilinear maps: Let G and G_T be two multiplicative cyclic groups of prime order p. We assume that the discrete logarithm problems in both G and G_T are intractable [24]. Let $e : G \times G \rightarrow G_T$ be a bilinear map with the following properties:*

1) *Bilinear: $e(P^a, Q^b) = e(P, Q)^{ab}$, for all $P, Q \in G$, and $a, b \in Z_p^*$.*

2) *Non-degenerate: There exists $P \in G$ such that $e(P, P) \neq 1$.*

3) *Computable: There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G$.*

Definition 2. *Complexity assumption: Let G and G_T be two multiplicative cyclic groups of order p, which are determined by some security parameter κ. The complexity assumption used in our scheme is a truncated version of the decisional q-augmented bilinear Diffie-Hellman exponent assumption (q-ABDHE). That is, an algorithm $\mathcal{B}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving truncated decision q-ABDHE if $|Pr[\mathcal{B}(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, e(g, g')^{\alpha^{q+1}}) = 0] - Pr[\mathcal{B}(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, Z) = 0]| \geq \epsilon$, where the probability is over the random choice of generators g, g' in G, the random choice of α in Z_p, the random choice of $Z \in G_T$,and the random bits consumed by $\mathcal{B}$. We refer to the distribution on the left as P_{ABDHE} and the distribution on the right as R_{ABDHE}.*

We say that the truncated q-ABDHE assumption holds in G if no polynomial time algorithm has advantage at least ϵ in solving the truncated q-ABDHE problem in G.

2.3 Access Structure

Definition 3. *Let $S = \{attr1, attr2, ..., attrn\}$ be a set of attributes. For $attri \in S(i = 1, 2, ..., n), a_i \in Z_p$ is a set of possible values. Let $l = (l_1, l_2, .., l_n), l_i \in a_i$ be an attribute list for a user, and $W = (P_1, P_2, ..., P_n)$ be* *an access structure. The notation $l \models W$ expresses that an attribute list l satisfies an access structure W, namely, $l_i = W_i (i = 1, 2, ..., n)$. The notation $l \nvDash W$ expresses that an attribute list l not satisfies an access structure W.*

2.4 CCA2 Security of Leakage Resilient ABE

Similar to previous works, an ABE system consists of four algorithms: *Setup, KeyGen, Encrypt,* and *Decrypt. Setup* algorithm takes as input a security parameter κ, and outputs PKG's public parameters*params* and the master secret key *msk*. *KeyGen* algorithm takes the master secret key *msk* and attributes S as input, and generates the private key for it. On input a message m, *params* and access policy W, *Encrypt* algorithm outputs a ciphertext C for attributes. Receiving a ciphertext, the recipient with attributes S decrypts the ciphertext C using algorithm *Decrypt*, with the ciphertext C and his private key sk_i as input.

A CP-ABE for a general access structure W over the monotone attribute universe space is composed of four PPT algorithms:

Setup(1^κ): The setup algorithm takes as input a security parameter κ and outputs system public parameters*params* and the master secret key *msk*.

KeyGen(msk, S): This algorithm takes as input an attribute set S, and the master secret key *msk*, and outputs a private key sk_i.

Encrypt($params, m, W$): The encryption algorithm takes as input a monotone access structure W and a message m, and outputs a ciphertext C.

Decrypt(sk_i, C): This algorithm takes as input a ciphertext CT for an access structure W and a private key sk_i for a set S, and outputs m if and only if the attribute set S satisfies the monotone access structure W.

The anonymous CCA2 security of leakage resilient ABE is defined via the following game, which is refined from the definition in [14]. Consistent with the work of [14], our security definition also only allows leakage attacks against the private keys of the various attributes, but not the master secret key. Additionally, we also only allow the adversary to make leakage queries before seeing the challenge ciphertext.

Setup: The challenger generates (*params,msk*) $\leftarrow$ *Setup*(1^κ), and sends *params* to the adversary $\mathcal{A}$.

Phase 1: In this phase, the adversary $\mathcal{A}$ can make the following three kinds of queries adaptively.

Key generation queries: On input attribute set S, the challenger runs *KeyGen* and replies with the resulting private key sk_i.

Leakage queries: On input a PPT leakage function $f_i : \{0,1\}^* \rightarrow \{0,1\}^{\lambda_i}$, the challenger replies with $f_i(sk_i)$, if $\sum_{k=1}^{i} \lambda_k \leq \lambda$; Otherwise, outputs $\perp$.

Decryption queries: On input the ciphertext *(params,m, W)*, the challenger first runs *KeyGen* algorithm, and then decrypts C using the resulting private key.

Challenge: The adversary $\mathcal{A}$ submits two pairs of equal length messages and access structures $(m_0, W_0), (m_1, W_1)$ to the challenger where every attribute sets S does not satisfy W_0 and W_1. The challenger $\mathcal{B}$ selects a bit $b \in \{0,1\}$ randomly and encrypts m_b with W_b, and sends $C^* \leftarrow Encrypt(params, W_b, m_b)$ to the adversary $\mathcal{A}$ as the challenge ciphertext.

Phase 2: This Phase is almost the same as Phase 1 except the attribute sets which satisfy the challenge access structure can be queried.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$.

The adversary wins the game if $b' = b$.

We call an adversary $\mathcal{A}$ in the above game a ANON-IND-λ-LR-ID-CCA2 adversary. The advantage of adversary $\mathcal{A}$ is defined by

$$Adv_{\mathcal{A}}(\kappa, \lambda) = |Pr[b = b'] - \frac{1}{2}|.$$

Definition 4. *ANON-λ-LR-CCA2-ABE: An ABE scheme $\mathcal{E}$ = $(Setup, KeyGen, Encrypt, Decrypt)$ is anonymous λ-leakage resilient CCA2 secure if for any probabilistic polynomial time ANON-IND-λ-LR-ID-CCA2 adversary $\mathcal{A}$, it holds that*

$$Adv_{\mathcal{A}}(\kappa, \lambda) \leq negl(\kappa).$$

If the adversary is not allowed to make decryption queries, he or she is called a ANON-IND-λ-LR-ID-CPA adversary.

3 Basic Construction: Chosen-Plaintext Security

3.1 Construction

Let G and G_T be groups of order p, and let $e : G \times G \rightarrow G_T$ be the bilinear map. The ABE system works as follows.

Setup(1^κ): On input the security parameter κ, PKG picks random generators $g, h \in G$ and a random $\alpha \in Z_p$. It sets $g_1 = g^\alpha \in G$. Then the public parameters *params* and the master secret key *msk* are set to be:

$$params = \{G, g, g_1, h\}, msk = \alpha.$$

KeyGen(msk, S): To generate a private key for given attributes $S = (a_1, a_2, ..., a_n)$, where $a_i \in Z_p$ and $i \in \{1, 2, ..., n\}$, PKG randomly chooses $r_i \in Z_p$ and outputs the corresponding private key sk_i for a_i:

$$sk_i = \{r_i, D_i\}, D_i = (hg^{-r_i})^{1/(\alpha - a_i)}.$$

If $\alpha = a_i$, PKG aborts. We require that PKG always uses the same values $r_i \in Z_p$ for the same a_i.

Encrypt$(params, m, W)$: Given the attributes $S = (a_1, a_2, ..., a_n)$ as well as the access policy $W = (P_1, P_2, .., P_n)$, the encrypted message $m \in G_T$, the sender picks $r, s \in Z_p$ at random and takes s_i such that $\sum_{i=1}^{n} s_i = s$. Then the sender outputs the ciphertext

$$C = (u_i, v_i, r, w), i \in \{1, 2, ..., n\},$$

where

$$u_i = \begin{cases} g_1^{s_i} g^{-s_i a_i}, & if\ a_i \in P_i \\ \tau, & else. \end{cases}$$

$v_i = e(g, g)^{s_i}, w = m \cdot e(g, h^r)^{-s}$. τ is an arbitray element in G.

Decrypt(sk_i, C): To decrypt a ciphertext $C = (u_i, v_i, r, w), i \in \{1, 2, ..., n\}$, the recipient outputs

$$m = w \cdot (\prod_{i=1}^{n} e(u_i, D_i) v_i^{r_i})^r.$$

Correctness analysis: Assuming the ciphertext $C = (u_i, v_i, w)$ received by the recipient with attribute S is valid, then

$$\begin{aligned} &(\prod_{i=1}^{n} e(u_i, D_i) v_i^{r_i})^r \\ =&(\prod_{i=1}^{n} e(g^{s_i(\alpha - a_i)}, (hg^{-r_i})^{1/(\alpha - a_i)}) \cdot e(g, g)^{s_i r_i})^r \\ =&(\prod_{i=1}^{n} e(g^{s_i}, hg^{-r_i}) \cdot e(g, g)^{s_i r_i})^r \\ =&\prod_{i=1}^{n} e(g, h^{s_i})^r \\ =&e(g, h)^{sr}. \end{aligned}$$

The decryption algorithm can then divide out this value from w and obtain the message m.

3.2 Security

We now prove that the above ABE system is ANON-IND-LR-ID-CPA secure under the truncated decision q-ABDHE assumption. Note that a CPA security is defined similarly as CCA2 game in Section 2, but with the restriction that the adversary cannot make decryption queries.

Theorem 1. *Assume the truncated decision q-ABDHE assumption holds for (G, G_T, e), then the above ABE scheme is ANON-IND-LR-ID-CPA secure, where $q = q_t + 2$ and q_t is the maximum number of key generation queries made by adversary. In addition, p is the prime order of the underlying group and κ denotes the security parameter.*

Proof. Let $\mathcal{A}$ be an adversary that breaks the ABE scheme above with an advantage ϵ. Then we can construct an algorithm $\mathcal{B}$, which can solve the truncated decision q-ABDHE assumption with the same advantage ϵ as follows.

On input a random truncated decision q-ABDHE tuple $(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, Z)$, where the elements $g, g' \in G$, $Z \in G_T$ and $\alpha \in Z_p$ are chosen independently and uniformly at random. By doing the following game with $\mathcal{A}$, $\mathcal{B}$ decides Z is either $e(g, g')^{\alpha^{q+1}}$ or a random element of G_T.

Setup: $\mathcal{B}$ generates a random polynomial $f(x) \in Z_p[x]$ of degree q. It sets $h = g^{f(\alpha)}$, computing h from $(g, g^{\alpha}, ..., g^{\alpha^q})$. It sends the public key (G, g, g_1, h) to $\mathcal{A}$. Since g, α, and $f(x)$ are chosen uniformly at random, h is uniformly random and this public key has a distribution identical to that in the actual construction.

Phase 1: In this phase, the adversary $\mathcal{A}$ can make the following queries adaptively.

Key generation queries: On input the attribute $a_i \in Z_p$, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, let $F_i(x) = (f(x) - f(a_i))/(x - a_i)$ and sets $sk_i = \{r_i, D_i\} = (f(a_i), g^{F_i(\alpha)})$.

Leakage queries: On input a leakage function $L_i : \{0, 1\}^* \to \{0, 1\}^{\lambda_i}$ for a_i, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, $\mathcal{B}$ replies with $L_i(sk_i)$ if $\sum_{k=1}^{i} \lambda_k \leq \lambda$; otherwise, $\mathcal{B}$ output $\perp$.

Challenge: The adversary $\mathcal{A}$ submits two pairs of equal length messages and access structures $(m_0, W_0), (m_1, W_1)$ to the challenger, which never appeared in a key generation query and appeared in leakage queries with at most λ bits leakage. Challenger $\mathcal{B}$ chooses $b \in \{0, 1\}$ randomly and encrypts m_b with W_b. Let $f_2(x) = x^{q+2}$ and $F_{2,i^*}(x) = (f_2(x) - f_2(a_i^*))/(x - a_i^*)$, which is a polynomial of degree $q + 1$. Challenger $\mathcal{B}$ sets $u_i^* = (g')^{\frac{f_2(\alpha) - f_2(a_i^*)}{n}}$, $v_i^* = (Z \cdot e(g', \prod_{i=0}^{q} g^{F_{2,i^*,i} \cdot \alpha^i}))^{\frac{1}{n}}$, $w^* = m_b/(e(u_i^*, D_i^*) \cdot v_i^{*r_i^*})^{r^* \cdot n}$, where $F_{2,i^*,i}$ is the coefficient of x^i in $F_{2,i^*}(x)$, and r^* is chosen randomly from Z_p. Challenger $\mathcal{B}$ sends $C^* = (u_i^*, v_i^*, r^*, w^*)$ as challenge ciphertext to the adversary. Indeed, in this case $s_i^* = \frac{\log_g g' \cdot F_{2,i^*}(\alpha)}{n}$.

Phase 2: This phase is almost the same as **Phase 1**, with the restriction that no leakage queries, and neither key generation queries on W^*.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b = b'$, $\mathcal{B}$ outputs 0(indicating that $Z = e(g,g')^{\alpha^{q+1}}$); otherwise, it outputs 1.

When the input tuple is sampled from $\mathcal{P}_{ABDHE} = \{T, e(g,g')^{\alpha^{q+1}}\}$ (where $T = (g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q})$, then $A's$ view is identical to its view in a real attack game and therefore $\mathcal{A}$ satisfies $|Pr[b = b'] - 1/2| \geq \epsilon$. When the input tuple is not sampled from $\mathcal{P}_{ABDHE}$ tuple (T, Z) (where Z is uniform in G_T) then $Pr[b = b'] = 1/2$. Therefore, we have that

$$Adv_{\mathcal{B}}^{ABDHE} = |Pr[\mathcal{B}(T, e(g,g')^{\alpha^{q+1}}) = 1] - Pr[\mathcal{B}(T,Z) = 1]|$$

$$\geq |(\frac{1}{2} \pm \epsilon) - \frac{1}{2}| = \epsilon.$$

□

4 Main Construction: Chosen-Ciphertext Security

We now present an efficient CP-ABE system that is ANON-IND-ID-CCA2 secure under the truncated decision q-ABDHE assumption. The proposed leakage-resilient attribute-based encryption scheme consists of four algorithms, each of which is described as follows:

Setup(1^{κ}): On input the security parameter κ, PKG picks random generators $g, h_1, h_2, h_3 \in G$ and a random $\alpha \in Z_p$. It sets $g_1 = g^{\alpha} \in G$ and chooses a hash function H from a universal one-way hash function family $\mathscr{H}$. Then the public parameters $params$ and the master secret key msk are set to be:

$$params = \{G, g, g_1, h_1, h_2, h_3, H\}, msk = \alpha.$$

KeyGen(msk, S): To generate a private key for given attributes $S = (a_1, a_2, ..., a_n)$, where $a_i \in Z_p$ and $i \in \{1, 2, ..., n\}$, PKG randomly chooses $r_{i,j} \in Z_p$ for $j \in \{1, 2, 3\}$ and outputs the corresponding private key sk_i for a_i:

$$sk_i = \{r_{i,j}, D_{i,j}\}, D_{i,j} = (h_j g^{-r_{i,j}})^{1/(\alpha - a_i)}.$$

Encrypt($params, m, W$): Given the attributes $S = (a_1, a_2, ..., a_n)$ as well as the access policy $W = (P_1, P_2, .., P_n)$, the encrypted message $m \in G_T$, the sender picks $r, s \in Z_p$ at random and takes s_i such that $\sum_{i=1}^{n} s_i = s$. Then the sender outputs the ciphertext

$$C = (u_i, v_i, w, r, y_i), \ i \in \{1, 2, .., n\}.$$

where

$$u_i = \begin{cases} g_1^{s_i} g^{-s_i a_i}, & if \ a_i \in P_i \\ \tau, & else. \end{cases}$$

$v_i = e(g,g)^{s_i}, w = m \cdot e(g, h_3 h_1^r)^{-s}, y_i = e(g, h_2 h_3^{\beta_i})^{s_i}$, $\beta_i = H(u_i, v_i, w, r)$. τ is an arbitray element in G.

Decrypt(sk_i, C): To decrypt a ciphertext $C = (u_i, v_i, w, r, y_i)$, the recipient computes $\beta_i = H(u_i, v_i, w, r)$ and check weather

$$y_i = e(u_i, D_{i,2} D_{i,3}^{\beta_i}) v_i^{(r_{i,2} + r_{i,3} \cdot \beta_i)}.$$

If the check fails, outputs $\perp$. Otherwise, outputs

$$m = w \cdot \prod_{i=1}^{n} e(u_i, D_{i,3} D_{i,1}^{r}) v_i^{(r_{i,3} + r_{i,1} \cdot r)}.$$

Correctness analysis: Assuming the ciphertext $C = (u_i, v_i, w, r, y_i)$ received by the recipient with attribute S is valid, then

$$\begin{aligned} & e(u_i, D_{i,2} D_{i,3}^{\beta_i}) v_i^{(r_{i,2} + r_{i,3} \cdot \beta_i)} \\ =& e(g^{s_i(\alpha - a_i)}, (h_2 h_3^{\beta_i})^{1/(\alpha - a_i)} g^{-(r_{i,2} + r_{i,3} \cdot \beta_i)/(\alpha - a_i)}) \\ & \cdot e(g,g)^{s_i(r_{i,2} + r_{i,3} \cdot \beta_i)} \\ =& e(g^{s_i}, h_2 h_3^{\beta_i} \cdot g^{-(r_{i,2} + r_{i,3} \cdot \beta_i)}) \cdot e(g,g)^{s_i(r_{i,2} + r_{i,3} \cdot \beta_i)} \\ =& e(g, h_2 h_3^{\beta_i})^{s_i} \\ =& y_i. \end{aligned}$$

where $\beta_i = H(u_i, v_i, w, r)$, and

$$\begin{aligned} & \prod_{i=1}^{n} e(u_i, D_{i,3} D_{i,1}^{r}) v_i^{(r_{i,3} + r_{i,1} \cdot r)} \\ =& \prod_{i=1}^{n} e(g^{s_i(\alpha - a_i)}, (h_3 h_1^r)^{1/(\alpha - a_i)} g^{-(r_{i,3} + r_{i,1} \cdot r)/(\alpha - a_i)}) \\ & \cdot e(g,g)^{s_i(r_{i,3} + r_{i,1} \cdot r)} \\ =& \prod_{i=1}^{n} e(g^{s_i}, h_3 h_1^r \cdot g^{-(r_{i,3} + r_{i,1} \cdot r)}) e(g,g)^{s_i(r_{i,3} + r_{i,1} \cdot r)} \\ =& \prod_{i=1}^{n} e(g, h_3 h_1^r)^{s_i} \\ =& e(g, h_3 h_1^r)^{s}. \end{aligned}$$

The decryption algorithm can then divide out this value from w and obtain the message m.

5 Security Analysis

We now prove that the proposed ABE system is ANON-λ-LR-ID-CCA2 secure under the truncated decision q-ABDHE assumption.

Theorem 2. *Assume the truncated decision q-ABDHE assumption holds for* (G, G_T, e)*,then the above ABE scheme is anonymous* $(\log p - w(\log \kappa))$*-leakage resilient CCA2 secure, where* $q = q_i + 2$ *and* q_i *is the maximum number of key generation queries made by adversary. In addition, p is the prime order of the underlying group and* κ *denotes the security parameter.*

Proof. Let $\mathcal{A}$ be an adversary that breaks the ANON-IND-ID-CCA2 security of the ABE scheme above with an advantage ϵ. Then we can construct an algorithm $\mathcal{B}$, which can solve the truncated decision q-ABDHE assumption with the same advantage ϵ as follows.

On input a random truncated decision q-ABDHE tuple $(G, g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q}, Z)$, where the elements $g, g' \in G$, $Z \in G_T$ and $\alpha \in Z_p$ are chosen independently and uniformly at random. By doing the following game with $\mathcal{A}$, $\mathcal{B}$ decides Z is either $e(g, g')^{\alpha^{q+1}}$ or a random element of G_T.

Setup: $\mathcal{B}$ generates random polynomials $f_j(x) \in Z_p[x]$ of degree q for $j \in \{1, 2, 3\}$ and sets $h_j = g^{f_j(\alpha)}$. The public parameters are published as *params* $= \{G, g, g_1, h_1, h_2, h_3, H\}$, where H is chosen at random from one universal one-way hash function family $\mathscr{H}$ and g_1 set to be g^{α}.

Phase 1: In this phase, the adversary $\mathcal{A}$ can make the following queries adaptively.

Key generation queries: On input $a_i \in Z_p$, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, let $F_{i,j}(x) = (f_j(x) - f_j(a_i))/(x - a_i)$ and sets $sk_i = (r_{i,j}, h_{i,j}) = (f_j(a_i), g^{F_{i,j}(\alpha)})$.

Leakage queries: On input a leakage function $L_i : \{0,1\}^* \rightarrow \{0,1\}^{\lambda_i}$ for a_i, if $a_i = \alpha$ then $\mathcal{B}$ can use α to solve the truncated decision q-ABDHE. Else, $\mathcal{B}$ replies with $L_i(sk_i)$ if $\sum_{k=1}^{i} \lambda_k \leq \lambda$; otherwise, output $\perp$.

Decryption queries: On input the ciphertext C for a_i, $\mathcal{B}$ first generates a private key for a_i as above. Then $\mathcal{B}$ decrypts C by performing the *Decrypt* algorithm with this private key and sends the result to the adversary eventually.

Challenge: The adversary $\mathcal{A}$ submits two pairs of equal length messages and access structures $(m_0, W_0), (m_1, W_1)$ to the challenger. For each attribute set S, it neither satisfies W_0 nor does it satisfy W_1. Challenger $\mathcal{B}$ chooses $b \in \{0, 1\}$ randomly and encrypts M_b with W_b. Let $f_4(x) = x^{q+2}$ and $F_{4,i^*}(x) = (f_4(x) - f_4(a_i^*))/(x - a_i^*)$, which is a polynomial of degree $q + 1$. Challenger $\mathcal{B}$ sets $u_i^* = (g')^{\frac{f_4(\alpha) - f_4(a_i^*)}{n}}$, $v_i^* = (Z \cdot e(g', \prod_{i=0}^{q} g^{F_{4,i^*,i} \cdot \alpha^i}))^{\frac{1}{n}}$, $w^* = m_b/(e(u_i^*, h_{i^*,3} h_{i^*,1}^{r^*}) \cdot v_i^{*(r_{i^*,3} + r_{i^*,1} \cdot r^*)})^n$, where $F_{4,i^*,i}$ is the coefficient of x^i in $F_{4,i^*}(x)$, and r^* is chosen randomly from Z_p. After setting $\beta_i^* = H(u_i^*, v_i^*, w^*, r^*)$, challenger $\mathcal{B}$ sets $y_i^* = e(u_i^*, h_{i^*,2} h_{i^*,3}^{\beta_i^*}) \cdot v_i^{*(r_{i^*,2} + r_{i^*,3} \cdot \beta_i^*)}$, and sends $C^* = (u_i^*, v_i^*, w^*, r^*, y_i^*)$ as challenge ciphertext to the adversary.

Phase 2: This phase is almost the same as **Phase 1**, with the restriction that no leakage queries, and neither key generation queries on v_i^* nor decryption queries on (a_i^*, C^*) are allowed to make.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$. If $b = b'$, $\mathcal{B}$ outputs 0(indicating that $Z = e(g, g')^{\alpha^{q+1}}$); otherwise, it outputs 1.

When the input tuple is sampled from $\mathcal{P}_{ABDHE} = \{T, e(g, g')^{\alpha^{q+1}}\}$ (where $T = (g', (g')^{\alpha^{q+2}}, g, g^{\alpha}, ..., g^{\alpha^q})$, then A's view is identical to its view in a real attack game and therefore $\mathcal{A}$ satisfies $|Pr[b = b'] - 1/2| \geq \epsilon$. When the input tuple is not sampled from $\mathcal{P}_{ABDHE}$ tuple (T, Z) (where Z is uniform in G_T) then $Pr[b = b'] = 1/2$. Therefore, we have that

$$Adv_{\mathcal{B}}^{ABDHE} = |Pr[\mathcal{B}(T, e(g, g')^{\alpha^{q+1}}) = 1] - Pr[\mathcal{B}(T, Z) = 1]|$$

$$\geq |(\frac{1}{2} \pm \epsilon) - \frac{1}{2}| = \epsilon.$$

□

Lemma 1. *If* $\mathcal{B}$*'s input is sampled according to* P_{ABDHE}*,* $\mathcal{A}$*'s view is identical to the actual attack.*

Proof. It is clear that the public parameters in the simulation have an identical distribution to the actual construction from the $\mathcal{A}$'s view of point. This is because g, α and $f_j(x)$ for $j \in \{1, 2, 3\}$ are all chosen uniformly at random, so h_1, h_2 and h_3 are uniformly random.

For the challenge ciphertext, it also has the correct distribution in the case of $\mathcal{B}$'s input sampled according to P_{ABDHE}, *i.e.*, $Z = e(g, g')^{\alpha^{q+1}}$. Indeed, in this case $s_i^* = \frac{\log_g g' \cdot F_{4,i^*}(\alpha)}{n}$. □

Lemma 2. *If* $\mathcal{B}$*'s input is sampled according to* R_{ABDHE}*,* $\mathcal{A}$ *has only a negligible advantage in outputting the correct bits b and c.*

Proof. Please refer to **Lemma 4** of [22], because the proof of **Lemma 2** is similar to it. Here we will not go into details of them. □

6 Performance Analysis

In this Section, we will give a comparison of our work with the schemes proposed by work [29] and [28], in terms of leakage bound ,security, underlying group, ciphertext size and anonymity. The results are shown in this paper. From Table 1, it is easy to see that our scheme can tolerate up to $(\log p - \omega(\log \kappa))$-bit leakage of the private key and its leakage parameter is independent of the message length. Obviously, it tolerates a larger amount of leakage

Table 1: Performance analysis

Scheme	Leakage bound λ	Security	Underlying group	Anonymity
[28]	-	CPA secure	Composite order	No
[29]	$2+(\omega-1-2\tau)(\log p_2)$	CPA secure	Composite order	No
Section 4	$\log p-\omega(\log\kappa)$	CCA secure	Prime order	Yes

Table 2: Performance analysis

Scheme	Public key size	Ciphertext size	Enc. time
[28]	$3\log p_1+2\log N$	$3\log p_1+2\log N$	$(3m+3)$E
[29]	$4\log p_1+\log p_3+\log N$	$4\log p_1+\log N$	$(3m+4)$E
Section 4	$5\log p$	$5\log p$	$(3n+1)$E

than work [29]. In particular, our scheme is the only one that based on prime order group and achieves CCA2 security. In addition, it also achieves anonymity. Moreover, from Table 2 we can see that our ciphertext size, public key size and encryption time is shorter than [29] and [28]. Thus, our scheme is more practical and efficient.

In Tables 1 and 2, κ is the security parameter of the scheme and p is the prime order of the underlying group in this paper. G and G_T denote two multiplicative cyclic groups. In [29] and [28], $N=p_1p_2p_3$ is the order of composite group. Additionally, m is the row of $LSSS$ matrix of [29] and [28]. Obviously, N is greater than p due to $N=p_1p_2p_3$. It is clear that m is greater than n because each row of $LSSS$ matrix is mapped to attribute.

We now argue that [28] and [29] are not hidden policy. Reference [25], we take [28] as an example. Some components C_1, C_{2x}, C_{3x} in ciphertext expose some information of access policy. Precisely, given an access policy (A,ρ), the adversary chooses $I'\subset\{1,...,m\}$ and $\{w_x\in Z_N\}_{x\in I'}$. Then, the adversary can run a test

$$\prod_{x\in I'}(e(C_{2x},g)e(C_{3x},T_{\rho(x)}))^{w_x}\overset{?}{=}e(C_1,g^a).$$

The adversary can use the above equation to determine whether CT is encrypted by the access policy (A,ρ). Thus, the CP-ABE scheme of is said to provide no hidden policy. However, our schemes can achieve policy hidden.

7 Conclusion

As an important primitive, ABE has attracted much attention in the context of leakage resilience in recent years. However, almost all of the existing leakage-resilient ABE schemes only achieve CPA security in this new setting. We construct a new ABE scheme, which is proved CCA2 secure under the truncated decision q-ABDHE assumption. Compared with the previous leakage-resilient ABE schemes, we show that our scheme is more practical and more efficient. In addition, we also show the anonymity of the scheme. However, the leakage ratio here is still approximately equal to 1/6. In the future work, we will try to give some new scheme with higher ratio.

Acknowledgments

This work was supported in part by the National Nature Science Foundation of China under Grant (61472307, 61402112, 61100165, 61100231), Natural Science Basic Research Plan in Shaanxi Province of China(Program NO. 2016JM6004), the National Key Research and Development Program of China under Grants No. 2017YFB0802002.

References

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, “Simultaneous hardcore bits and cryptography against memory attacks,” in *Theory of Cryptography Conference*, pp. 474–495, 2009.

[2] J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Walfish, and D. Wichs, “Public-key encryption in the bounded-retrieval model,” *Lecture Notes in Computer Science*, vol. 2009, no. 5, pp. 113–134, 2010.

[3] J. Alwen, Y. Dodis, and D. Wichs, “Leakage-resilient public-key cryptography in the bounded-retrieval model,” in *Annual International Cryptology Conference*, pp. 36–54, 2009.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[5] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, “Practical leakage-resilient identity-based encryption from simple assumptions,” in *ACM Conference on Computer and Communications Security*, pp. 152–161, 2010.

[6] P. S. Chung, C. W. Liu, and M. S. Hwang, “A study of attribute-based proxy re-encryption scheme in cloud environments,” *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[7] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in *International Cryptology Conference*, pp. 13–25, 1998.

[8] Y. Dodis, Y. T. Kalai, and S. Lovett, "On cryptography with auxiliary input," *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* pp. 621–630, 2009. ISBN: 978-1-60558-506-2

[9] K. Emura, A. Miyaji, K. Omote, A. Nomura, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *International Conference on Information Security Practice and Experience*, pp. 13–23, 2009.

[10] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*pp. 197–206, 2008. ISBN: 978-1-60558-047-0

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[12] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felte, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the Acm*, vol. 52, no. 5, pp. 91–98, 2008.

[13] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *International Workshop on Public Key Cryptography*, pp. 293–310, 2014.

[14] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: Leaking secrets," in *International Crytology Conference*, 1999. (https://www.paulkocher.com/doc/DifferentialPowerAnalysis.pdf)

[15] A. Lewko, Y. Rouselakis, and B. Waters, "Achieving leakage resilience through dual system encryption," in *Conference on Theory of Cryptography*, pp. 70–88, 2011.

[16] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[17] B. Majid and M. R. Aref, "An attribute based key agreement protocol resilient to kci attack," *International Journal of Electronics & Information Engineering*, vol. 2, 2015.

[18] S. Micali and L. Reyzin, "Physically observable cryptography," in *Conference on Theory of Cryptography*, pp. 278–296, 2004.

[19] R. Oded, "On lattices, learning with errors, random linear codes and cryptography," *Journal of the Acm*, vol. 56, no. 6, pp. 1–40, 2009.

[20] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *International Conference on Financial Cryptography and Data Security*, pp. 315–332, 2015.

[21] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[22] S. F. Sun, D. Gu, and S. Liu, "Efficient leakage-resilient identity-based encryption with cca security," *Springer International Publishing*, pp. 149–167, 2013.

[23] K. Takashima, "New proof techniques for dlin-based adaptively secure attribute-based encryption," in *Australasian Conference on Information Security and Privacy*, pp. 85–105, 2017.

[24] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[25] Z. Wang and M. He, "Cp-abe with hidden policy from waters efficient construction," *International Journal of Distributed Sensor Networks*, vol. 12, no. 5, 2016.

[26] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Lecture Notes in Computer Science*, vol. 2008, pp. 321–334, 2011.

[27] T. H. Yuen, S. M. Sherman, Y. Zhang, and S. M. Yiu, "Identity-based encryption resilient to continual auxiliary leakage," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 117–134, 2012.

[28] L. Zhang, J. Zhang, and Y. Mu, "Novel leakage-resilient attribute-based encryption from hash proof system," *Computer Journal*, vol. 60, no. 2, p. 4, 2016.

[29] M. Zhang, W. Shi, C. Wang, Z. Chen, and Y. Mu, "Leakage-resilient attribute-based encryption with fast decryption: Models, analysis and constructions," in *International Conference on Information Security Practice and Experience*, pp. 75–90, 2013.

Biography

Leyou Zhang is a professor in the school of mathematics and statistics at Xidian University, Xi'an China. He received his PhD from Xidian University in 2009. From Dec. 2013 to Dec. 2014, he is a research fellow in the school of computer science and software engineering at the University of Wollongong. His current research interests include network security, computer security, and cryptography.

Yujie Shang is a master degree student in the school of mathematics and statistics, Xidian University. Her research interests focus on computer and network security.