Journal of Computer and System Sciences 89 (2017) 41–50

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

ABE with improved auxiliary input for big data security

Zhiwei Wang[a,c,d,*], Cheng Cao[a], Nianhua Yang[b], Victor Chang[e]

[a] School of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China
[b] Shanghai University of International Business and Economics, Shanghai 201620, China
[c] Key Laboratory of Information Security, School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China
[d] Shanghai Key Laboratory of Information Security Integrated Management Technology, Shanghai 200240, China
[e] IBSS, Xi'an Jiaotong Liverpool University, Suzhou 215123, China

ARTICLE INFO

Article history:
Received 1 March 2016
Received in revised form 7 December 2016
Accepted 16 December 2016
Available online 27 December 2016

Keywords:
ABE
Improved auxiliary input
Encryption randomness
Big data application

ABSTRACT

Attribute-based encryption (ABE) is recommended by the Cloud Security Alliance (CSA) as one of the possible cryptographic tools for access control in big data applications. In ABE, the shared file can be encrypted with the specific policy only once, and it can be decrypted by any receiver whose attributes are satisfied. When ABE is deployed in some open network scenarios, it is inevitably attacked by side channel attacks, because the big data are coming from diverse end-points. In this paper, we propose leakage resilient CP-ABE and KP-ABE schemes in the improved auxiliary input model, which allows the attacker query more leakage information regarding the encryption randomness after seeing the challenge ciphertext. Moreover, we construct an improved strong extractor from the modified Goldreich–Levin theorem for the security proof and prove that our scheme security relies on the Wang et al. construction.

1. Introduction

Confidentiality, integrity, and access control are the most important issues for the security and privacy of open networks, such as wireless sensor networks, cloud computing, and fog/edge computing [1–6]. For access control, there are two fundamentally different approaches for controlling data visibility to different entities. The first one is controlling data visibility by limiting access to the underlying operating systems, while the second one is encrypting the data using cryptography. Compared with the first approach, the second exposes a smaller, more well-defined attack surface. In order to access the sensitive information securely, many end users in big data applications utilize X.509 certificates for identification and cryptographic session establishment. However, it requires too much time and processing to periodically update cryptographic keys. Thus, the Cloud Security Alliance (CSA) recommended identity-based encryption (IBE) or attribute-based encryption (ABE) [8–10] for access control in big data security [7]. Compared with IBE, ABE may be a better choice for access control, because it does not need prior knowledge of the number of recipients, their identities, or certificates. It allows the data owner to define their own access policy on the data, such that only authorized receivers, whose attributes satisfy the policy, can decrypt the ciphertexts. Sahai et al. [22] proposed the concept of attribute-based encryption (ABE) in 2005. There are two kinds of ABE systems: The first is ciphertext-policy ABE (CP-ABE), where ciphertexts are encrypted with access policies, and keys are extracted from attributes; second is key-policy ABE (KP-ABE), where keys and ciphertexts are just the reverse.

[*] Corresponding author.
E-mail address: zhwwang@njupt.edu.cn (Z. Wang).

http://dx.doi.org/10.1016/j.jcss.2016.12.006

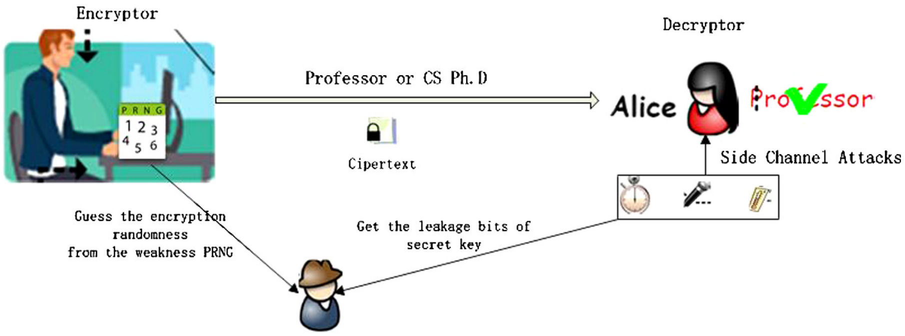

Fig. 1. Secret key and encryption randomness leakage.

Big data are obtained from diverse terminators and contain more personal sensitive data, such as geographical information [11], forensic data [12], and healthcare data [13]. Thus, it is becoming increasingly important to tether the data at the source. Much legislation, like the Personal Information Protection Act (China) and Data Protection Act (UK) can only provide help after the sensitive data is compromised. However, at this point, the damage has been done. If X.509-based encryption or IBE are deployed in big data applications, then they require that each file should be encrypted by a receiver public key or ID. If the file will be sent to several receivers, then it should be encrypted several times. However, CP-ABE only requires the shared file to be encrypted with the specific policy once, and can be decrypted by every receiver whose attributes are satisfied. Thus, CP-ABE saves significant encryption computational cost, and can deal with a large amount and quantity of data. If the ABE scheme is deployed in these big data applications, such as cloud storage forensics [14,17–21], it can perfectly protect the personal data. For example, in data exfiltration from the Internet of things (IoT) devices [15,16], the IoT device is labeled by *(Serial number, MAC address, IP address)*, while each person in this system is labeled by *(Name, Sex, Identity number, IP address)*. We can set a policy using ABE that only the person whose name is “Mike” or the device whose serial number is “123-45678” can gain access to the data. Chang et al. [38] proposed a multilayered approach for the security of cloud computing adoption framework (CCAF), which consisted of three items. ABE may be very suitable for CCAF due to its access control property.

One of the important issues in ABE is achieving a more expressive access policy. The Sahai [22] scheme specified the policy as threshold access policies with one threshold gate. Since that time, Lewko et al. [24] used monotone span programs (MSPs) as access policy, which proven secure in a standard model. However, the Lewko et al. schemes were very inefficient, because the length of ciphertexts and keys, and number of pairings in decryption are all polynomial in the size of MSPs. Some ABE systems later made use of a linear secret sharing scheme (LSSS), or used Boolean formulas as access policy. Waters [31] employed an LSSS scheme as the access policy to realize CP-ABE under noninteractive cryptographic assumptions. In [30], Goyal et al. proposed a mapping from a universal access tree to formulas, by which a bounded CP-ABE scheme was constructed. Recently, Zhang et al. [23] proposed a CP-ABE and KP-ABE, resilient to continual leakage by minimal sets.

Another important issue of ABE is avoiding the side-channel attacks, which allow attackers to learn partial information about the secret key by observing physical properties of a cryptographic execution, such as timing, power assumption, temperature, and radiation [25–29]. The concept of leakage resilient cryptography has been proposed, which has led to construction of many cryptographic primitives. Leakage resilience has been analyzed in many previous studies under a variety of leakage models. There are primarily three leakage models: 1) The bounded retrieval model [33–35], where the total number of bits leaked over the system lifetime is significantly less than the bit-length of the key. Here, it is hoped that the attack is detected and stopped before the whole secret is leaked; 2) The continual leakage model [36,37,23]. It is assumed that the leakage between consecutive updates is bounded in terms of a fraction of the secret key size, and the secret key should be continually refreshed. There is no leakage during the update process; 3) The auxiliary input model [39,40,42,43], developed from the *relative leakage* model [25], which allows any non-invertible function f, that no probabilistic polynomial-time (PPT) attacker can compute the actual pre-image with a non-negligible probability. That is to say, although such a function theoretically reveals the entire secret key SK, it is still computationally infeasible to recover SK from $f(SK)$.

Obviously, the auxiliary input model is the strongest among these three models [40]. However, there is still a shortcoming in this model that only allows the leakage of a secret key and does not allow the attacker to query leakage information about the encryption randomness after seeing the challenge ciphertext. In practice, that is not true, and the encryption randomness r can also be leaked by poor implementation of a pseudorandom number generator (PRNG) as in Fig. 1. Michaelis et al. found that there exists significant weakness of PRNG in some Java runtime libraries [41]. In big data applications, data are usually encrypted by the devices with constrained resources. Thus, the data encryption may use these weak pseudorandom numbers from Java runtime libraries as randomness. Some terminal devices are exposed in the open air, such as wireless sensors. The attacker can easily guess the randomness used in the encryption. If the attacker can obtain the entire randomness r, it can encrypt the two challenge messages M_0 and M_1, and compare them to the challenge ciphertext, thus, winning the security game. Although CSA suggested ABE as a possible cryptographic tool to enforce access control in big data applications, we should avoid the scenario that the attacker can identify the corresponding plaintext data by looking at the ciphertext. Thus, we should not only protect the decryption secret key but also protect the encryption randomness in the auxiliary model. Yuen et al. [42] proposed a post-challenge auxiliary input model, which not only allows the attacker to make secret key leakage queries before seeing the challenge ciphertext, but also allows the attacker to make randomness leakage queries after seeing the challenge ciphertext. We call it the improved auxiliary input model.

The contributions of this paper are threefold. First, we propose the first CP-ABE and KP-ABE schemes in the improved auxiliary input model. Compared with the auxiliary input model, the improved model considers not only the decryptor leakage (leakage of secret key), but also encryptor leakage (leakage of randomness). All the former leakage resilient ABE schemes [23,43] are only resilient to the decryptor leakage, and our construction is the first one that considers the leakage from two sides: encryptor and decryptor, which is much more suitable for big data applications, such that many terminal devices are resource constrained. Second, for the special structure of the secret key in the CP-ABE scheme with auxiliary input, we construct an improved strong extractor from the modified Goldreich–Levin theorem. Third, we compare the performance of our scheme with the other three leakage resilient CP-ABE schemes.

Organization. In Section 2, we introduce a strong extractor from the modified Goldreich–Levin theorem and access structure. In Section 3, we provide the definition and security model of ABE with improved auxiliary input. In Section 4, we devise a CP-ABE scheme with improved auxiliary input, and prove its security. In Section 5, we construct a KP-ABE scheme with improved auxiliary input, and provide the security proof. In Section 6, we conclude our paper.

2. Background

In this section, we first introduce the strong extractor from the modified Goldreich–Levin theorem. Second, we provide the definitions for the access structure and LSSS.

2.1. Strong extractor from modified Goldreich–Levin theorem

In [42], Yuen et al. proposed the definition of a strong extractor with auxiliary input as follows:

Definition 1 *((ϵ, μ)-strong extractor).* Denote Ex as $Ex : \{0,1\}^{l_1} \times \{0,1\}^{l_2} \to \{0,1\}^{l_3}$. If for every PPT attacker $\mathfrak{A}$, and $\forall(x, f)$, such that $x \in \{0,1\}^{l_2}$ and f is a PPT computable function $f : \{0,1\}^{|r'|} \to \{0,1\}^*$, such that, given $f(r')$, no PPT algorithm can recover r' greater than ϵ, we have:

$$|Pr[\mathfrak{A}(r, f(x), Ex(r,x)) = 1] - Pr[\mathfrak{A}(r, f(x), u) = 1]| \le \mu.$$

(r and u are randomly chosen from $\{0,1\}^{l_1}$ and $\{0,1\}^{l_2}$ respectively.) Then, we say that Ex is a (ϵ, μ)-strong extractor with auxiliary input.

Moreover, in [42], Yuen et al. found that the modified Goldreich–Levin theorem can be used to construct the strong extractor. We review the theorem as follows:

Theorem 1 *(Modified Goldreich–Levin theorem). Let q be a big prime, and let H be any subset of $GF(q)$. Let f map from $H^{\bar{m}}$ to $\{0,1\}^*$ be any PPT computable function. Then, a vector s is uniformly randomly chosen from $H^{\bar{m}}$, and we have $y = f(s)$. Then, randomly selected vector r is from $GF(q)^{\bar{m}}$, and u is randomly chosen from $GF(q)$. If a PPT distinguisher $\mathfrak{A}$ runs in time t, and there exists a probability ϵ, such that*

$$|Pr[\mathfrak{A}(y, r, <r, s>) = 1] - Pr[\mathfrak{A}(y, r, u) = 1]| = \epsilon,$$

then, there exists an inverter $\mathfrak{B}$ that can compute s from y in time $t' = t \cdot poly(\bar{m}, |H|, 1/\epsilon)$ with the probability

$$Pr[s \leftarrow H^{\bar{m}}, y \leftarrow f(s) : \mathfrak{B}(y) = s] \ge \frac{\epsilon^3}{512 \cdot m \cdot q^2}.$$

Yuen et al. showed that a strong extractor with auxiliary input can be constructed by using an inner product in the modified Goldreich–Levin theorem.

Theorem 2. *Let x be randomly chosen from $\{0,1\}^l$, and r be randomly chosen from $GF(q)^l$, where $l = poly(\lambda)$ and λ is a security parameter. Then, randomly choose u from $GF(q)$. Let f be a PPT computable function $f : \{0,1\}^{|r'|} \to \{0,1\}^*$, such that, given $f(r')$, no PPT algorithm can recover r' greater than ϵ. Then, given f, no PPT distinguisher $\mathfrak{A}'$ can distinguish $(r, f(x), <r, x>)$ from $(r, f(x), u)$ with the probability $\iota \ge (512lq^2\epsilon)^{1/3}$.*

An improved strong extractor is used in our construction, which is combined by m strong extractor from the modified Goldreich–Levin theorem. Lemma 1, regarding the improved strong extractor can be proven as follows:

Lemma 1. *Let λ be security parameter, and m be $m = poly(\lambda)$, l be $l = poly(\lambda)$. Let $x_1, \cdots, x_m$ be randomly chosen from $\{0,1\}^l$, and $r_1, \cdots, r_m$ be randomly chosen from $GF(q)^l$. Then, randomly choose $u_1, \cdots, u_m$ from $GF(q)$. Let f be a PPT computable function $f : \{0,1\}^{|r'|} \to \{0,1\}^*$, such that, given $f(r')$, no PPT algorithm can recover r' greater than ϵ. Then, given f, no PPT distinguisher $\mathfrak{A}'$ can distinguish $(r_1, \cdots, r_m, f(x_1), \cdots, f(x_m), <r_1, x_1>, \cdots, <r_m, r_m>)$ from $(r_1, \cdots, r_m, f(x_1), \cdots, f(x_m), u_1, \cdots, u_m)$ with the probability $\iota \geq [(1-(1-\epsilon)^{1/m})512lq^2]^{1/3}$.*

Proof. In order to use the modified Goldreich–Levin theorem, we let $H = \{0,1\} \subset GF(q)$ and $\bar{m} = l$. Assuming that there exists an algorithm that can distinguish $(r_1, \cdots, r_m, f(x_1), \cdots, f(x_m), <r_1, x_1>, \cdots, <r_m, x_m>)$ from $(r_1, \cdots, r_m, f(x_1), \cdots, f(x_m), u_1, \cdots, u_m)$ in time $t = poly(\lambda)$ with probability ι, then, there exists an inverter $\mathfrak{A}$, such that:

$$Pr[\mathfrak{A}(f(x_1)) = x_1 \vee \cdots \vee \mathfrak{A}(f(x_m)) = x_m] \geq 1 - (1 - \frac{\iota^3}{512lq^2})^m,$$

if $\iota \geq [(1-(1-\epsilon)^{1/m})512lq^2]^{1/3}$. It contradicts the non-invertible property of f. □

2.2. Access structure

The following definition is given by [32].

Definition 2 *(Access structure).* Let $\{S_1, \cdots, S_n\}$ be a set of attributes. We call an authorized collection $\mathbb{A} \subset 2^{\{S_1,\cdots,S_n\}}$ monotone on the condition that $\forall B, C$, $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. A monotone collection $\mathbb{A}$ is a monotone access structure, which is a non-empty set of subsets of $\{S_1, \cdots, S_n\}$. If the sets are not in $\mathbb{A}$, then they are unauthorized sets.

The definition of LSSS can be seen in [32]. From the discussion in [32], each LSSS scheme Π for the access structure $\mathbb{A}$ can be used to *linear reconstruction*. Let $\mathcal{C} \in \mathbb{A}$ be any authorized set, and let $I \subset \{1, \cdots, l\}$ be defined as $I = \{i : \rho(i) \in \mathcal{C}\}$. Then, there exist constants $\{\omega_i \in \mathbb{Z}_N\}_{i \in I}$, such that, $\sum_{i \in I} \omega_i \lambda_i = \mu$, if $\{\lambda_i\}$ are valid shares of any μ in Π. These $\{\omega_i\}$ can be found in polynomial time.

3. ABE with improved auxiliary input

3.1. Definition

A CP-ABE scheme for a general monotone access structure $\mathbb{A}$ is composed of four PPT algorithms as follows:

1. **Setup(1^λ)**: The setup algorithm takes a security parameter λ as input, and outputs the master public/secret key pair (MPK, MSK).
2. **KeyGen($MSK, \mathbb{S}$)**: This algorithm takes an attribute set $\mathbb{S}$ and master secret key MSK as input, and outputs a secret key $SK_{\mathbb{S}}$.
3. **Encrypt($M, \mathbb{A}$)**: The Encrypt algorithm takes a monotone access structure $\mathbb{A}$ and message M as input, and outputs a ciphertext CT.
4. **Decrypt(CT, SK)**: This algorithm takes a ciphertext CT for an access policy $\mathbb{A}$ and secret key SK for a set $\mathbb{S}$ as input, and outputs M if, and only if, the attribute set $\mathbb{S}$ satisfies $\mathbb{A}$.

Let Π and $\mathcal{M}$ be the monotone attribute space and message space, respectively. $\forall M \in \mathcal{M}$, $\forall \mathbb{A} \in 2^{\Pi}$ and $\forall \mathbb{S} \in \mathbb{A}$, $M \leftarrow$ Decrypt(SK, Encrypt($MPK, M, \mathbb{A}$)), where $(MPK, MSK) \leftarrow$ Setup(1^λ), $SK \leftarrow KeyGen(MSK, \mathbb{S})$.

3.2. Security model

Given an attack model, a candidate cryptographic scheme is usually proven secure by a security game. It proves that if an attacker can compute certain scheme properties, then it can break a number of theoretical problems widely assumed to be hard. Alternatively, it can break the security of simple cryptographic primitives that are used as building blocks of the scheme. In this section, we provide the security model of CP-ABE for semantic security with improved auxiliary input (IAI-CP-ABE), which is similar to the classic CPA model and auxiliary input model, except that the attacker $\mathfrak{A}$ can submit several randomness leakage queries later in the security game. Let $\mathcal{F}_s$ and $\mathcal{F}_0$ denote two PPT computable function families, where the set of functions asked in secret key leakage oracle is $\mathcal{F}_s$, while the set of functions asked in randomness leakage oracle is $\mathcal{F}_0$. We define the security model by an indistinguishable game between a challenger, $\mathfrak{C}$, and an attacker, $\mathfrak{A}$. In order to record the queried and leaked keys, we set an empty list: $\mathfrak{R} = \langle \bar{j}, \mathbb{S}, SK_{\mathbb{S}} \rangle$, where $\bar{j}$ is a index handle.[1]

[1] $\bar{j}$ is used to index the attributes set and the secret key.

Setup. The challenger, $\mathfrak{C}$, runs the Setup algorithm to generate MPK and MSK, and sends MPK to $\mathfrak{A}$.

Query 1. The attacker, $\mathfrak{A}$, can perform the following queries:

- **Key extraction query($\mathcal{Q}_E$):** When $\mathfrak{A}$ makes a key extraction query on an attribute set $\mathbb{S}$, $\mathfrak{C}$ first checks the list, $\mathfrak{R}$, for the tuple with the form $\langle \bar{j}, \mathbb{S}, SK_{\mathbb{S}} \rangle$. If such tuple is not found, then $\bar{j}$ is set to 1, and $\mathfrak{C}$ answers $SK_{\mathbb{S}} \leftarrow KeyGen(MSK, \mathbb{S})$. Then, $\mathfrak{C}$ puts $\langle \bar{j}, \mathbb{S}, SK_{\mathbb{S}} \rangle$ into the list $\mathfrak{Q}$. Otherwise, $\mathfrak{C}$ returns $SK_{\mathbb{S}}$ from the tuple $\langle \bar{j}, \mathbb{S}, SK_{\mathbb{S}} \rangle$, and sets $\bar{j} = \bar{j} + 1$.
- **Key leakage query($\mathcal{Q}_L$):** When $\mathfrak{A}$ makes a key leakage query on an attribute set, $\mathbb{S}$, with a function $f \in \mathcal{F}_s$, $\mathfrak{C}$ returns $f(MSK, \mathfrak{Q}, MPK, \mathbb{S})$.

Challenge. $\mathfrak{A}$ outputs two messages $M_0, M_1 \in \mathcal{M}$ and a monotone access structure $\mathbb{A}^*$, such that, $\forall \mathbb{S}$ does not satisfy $\mathbb{A}^*$. $\mathfrak{C}$ randomly chooses a bit $b \in \{0, 1\}$, and returns the cipher-text $CT^* \leftarrow Encrypt(MPK, M_b, \mathbb{A}^*)$, where the randomness used in encryption is r'.

Query 2.
- **Key extraction query($\mathcal{Q}_E$):** $\mathfrak{A}$ can make the key extraction queries like Query 1 except the queries on the attribute sets which satisfy $\mathbb{A}^*$.
- **Randomness query($\mathcal{Q}_R$):** When $\mathfrak{A}$ makes a randomness leakage query on r' with a function $f' \in \mathcal{F}_0$, $\mathfrak{C}$ returns $f'(r')$.

Response. Finally, $\mathfrak{A}$ outputs a guess b' of b. $\mathfrak{A}$'s advantage in this game can be defined as $ADV_{\mathfrak{A}}(1^\lambda) = |2Pr[b = b'] - 1|$.

We say that a CP-ABE scheme is IAI-CPA secure w.r.t. auxiliary inputs from $\mathcal{F}_s$ and $\mathcal{F}_0$ on the condition that $ADV_{\mathfrak{A}}$ is negligible for any PPT attacker $\mathfrak{A}$ in the above game. We have the following definition:

Definition 3 *(IAI-CPA-CP-ABE).* If a CP-ABE is CPA secure w.r.t. auxiliary input families $\mathcal{F}_s$ and $\mathcal{F}_0$, then it is said to be improved auxiliary input CPA secure (IAI-CPA).

4. Construction of CP-ABE with improved auxiliary input

4.1. Our construction

The key point for the construction in both the auxiliary input model and improved auxiliary input model is how to split the secret key and randomness into m pieces, which is the "hardcore" of the modified Goldreich–Levin theorem. The modified Goldreich–Levin theorem states that if the secret key pieces and randomness belong to field $GF(q)$ (q is a λ-bit prime), then, the inverter running time is closed to $poly(2^\lambda)$, which cannot be borne by the inverter. Wang et al. [43] found that the secret key of Waters' CP-ABE scheme [31] can be easily split into m pieces, which is also the most efficient construction of CP-ABE. Thus, they chose it to construct the CP-ABE scheme in the auxiliary model. The Wang et al. scheme keeps the nice features of the Waters scheme, such as the security in the standard model, and static hardness assumption basis. Thus, in this work, we design a CP-ABE scheme with an improved auxiliary input based on the Wang et al. construction [43]. We let $\Lambda' = (Setup', KeyGen', Encrypt', Decrypt')$ be the Wang et al. scheme, where the encryption randomness is in $\mathbb{Z}_N^m$, and inner product $< \tau_i, s_i >$ for $i = 1, \cdots, m$ is $(\epsilon_r, negl(\lambda))$-strong extractors in auxiliary input model, where vectors $\tau_i \in \{0, 1\}^l$ and $s_i \in \mathbb{Z}_N^l$. We can construct a CP-ABE scheme Λ with improved auxiliary input as follows:

Setup(1^λ): The Setup algorithm runs $(MPK', MSK') \leftarrow Setup'(1^\lambda)$, and randomly chooses vectors $\tau_1, \cdots, \tau_m$ from $\{0, 1\}^l$. Then, the master public key is $MPK = (MPK', \tau_1, \cdots, \tau_m)$, and master secret key is $MSK = MSK'$.

KeyGen($MSK, MPK, \mathbb{S}$): The KeyGen algorithm takes an attribute set $\mathbb{S}$, and master public/secret key pair (MPK, MSK) as input. It runs

$$SK_{\mathbb{S}} \leftarrow KeyGen'(MSK, MPK, \mathbb{S}).$$

Encrypt(MPK, M, Λ): The Encrypt algorithm takes an LSSS scheme $\Gamma = (\mathcal{A}, \rho)$ for a monotone access policy $\mathbb{A}$[2] as input. It randomly selects vectors $s_1, \cdots, s_m \in \mathbb{Z}_N^l$, and then computes $s'_1 = < \tau_1, s_1 >, \cdots, s'_m = < \tau_m, s_m >$. The generated ciphertext is

$$CT = Encrypt'(MPK, M, \Gamma; s'_1, \cdots, s'_m).$$

Decrypt(CT, SK, MPK): It recovers $M \leftarrow Decrypt'(CT, SK, MPK)$.

Theorem 3. *If Λ' is a CPA secure CP-ABE scheme leakage resilient to auxiliary input with respect to the secret key SK, and inner product, $< \tau_i, s_i >$ for $i = 1, \cdots, m$ is $(\epsilon_r, negl(\lambda))$-strong extractors in the auxiliary input model, then Λ is a CPA secure CP-ABE scheme with improved auxiliary input.*

[2] $\mathcal{A}$ is a $l \times n$ matrix, and function ρ maps the rows of $\mathcal{A}$ to the attributes.

Table 1
Performance comparison of CP-ABE schemes.

Schemes	[37]	[23]	[43]	Our scheme
Encrypt	$2(\xi+2l)Mu$	$(\xi+2\kappa)Mu$	$(2l+m+1)E$	$(2l+m+1)E+m\cdot Ip$
Decrypt	$(\xi+2l+1)Pr$	$(\xi+3)Pr$	$(m+2\|I\|)Pr$	$(m+2\|I\|)Pr$
Leakage bound	$\eta=2+(\xi-1-2\varpi)\log p_2$	$\eta=2+(\xi-1-2\varpi)\log p_2$	no	no
Leakage model	bounded leakage	continuous leakage	auxiliary input	improved auxiliary input

Proof. We denote the randomness used in the challenge ciphertext as $s_1^*,\cdots,s_m^*$. Assuming that $Game_0$ is the CPA security game of $\varLambda$ scheme with the auxiliary input, $Game_1$ is the same as $Game_0$, except that $s_1'=<\tau_1,s_1^*>,\cdots,s_m'=<\tau_m,s_m^*>$ are replaced by the random values $s_1'',\cdots,s_m''$ from $\mathbb{Z}_N$, when encrypting the challenge ciphertext $CT=Encrypt'(MPK,M,\varGamma;s_1'',\cdots,s_m'')$. The attacker, $\mathfrak{A}$, creates leakage queries $f_i(s_1^*),\cdots,f_i(s_m^*)$ for both games.

Let $ADV_{\mathfrak{A}}^{Game_i}(\varLambda)$ denote the advantage that the attacker, $\mathfrak{A}$, wins in $Game_i$. Then, we give a proof by contradiction that $|ADV_{\mathfrak{A}}^{Game_0}(\varLambda)-ADV_{\mathfrak{A}}^{Game_1}(\varLambda)|$ is negligible for any PPT attacker, $\mathfrak{A}$. We assume that there exists an attacker, $\mathfrak{A}$, that can make $|ADV_{\mathfrak{A}}^{Game_0}(\varLambda)-ADV_{\mathfrak{A}}^{Game_1}(\varLambda)|\ge\epsilon_{\mathfrak{A}}$ be a non-negligible probability.

The challenger, $\mathfrak{C}$, is given

$$(\{\tau_1,\cdots,\tau_m\},\{\{f_1(s_1^*),\cdots,f_1(s_m^*)\},\cdots,\{f_q(s_1^*),\cdots,f_q(s_m^*)\}\},\{T_1,\cdots,T_m\}),$$

where $T_{0i}=<\tau_i,s_i^*>$ or $T_{1i}=u$, which is randomly selected from $\mathbb{Z}_N$, for $i=1,\cdots,m$. Given $\{\{f_1(s_1^*),\cdots,f_1(s_m^*)\},\cdots,\{f_q(s_1^*),\cdots,f_q(s_m^*)\}\}$, no PPT attacker can recover at least one of $s_1^*,\cdots,s_m^*$ greater than $1-(1-\epsilon_r)^m$. Then, $\mathfrak{C}$ runs $(MPK,MSK)\leftarrow Setup(1^\lambda)$ and $SK\leftarrow KeyGen(MSK,MPK,\mathbb{S})$. $\mathfrak{C}$ gives $(MPK,\tau_1,\cdots,\tau_m)$ to the attacker, $\mathfrak{A}$, and $\mathfrak{C}$ can answer secret key leakage queries because it has SK. Then, $\mathfrak{A}$ submits two messages M_0 and M_1 with the same length to $\mathfrak{C}$. $\mathfrak{C}$ randomly chooses a bit b, and returns the challenge ciphertext

$$CT^*=Encrypt(MPK,M_b,\varGamma;T_1,\cdots,T_m)$$

to $\mathfrak{A}$. Finally, $\mathfrak{A}$ outputs its guess bit b', and if $b=b'$, then $\mathfrak{C}$ outputs 1; otherwise, it outputs 0.

Because $|ADV_{\mathfrak{A}}^{Game_0}(\varLambda)-ADV_{\mathfrak{A}}^{Game_1}(\varLambda)|\ge\epsilon_{\mathfrak{A}}$, then

$$\begin{aligned}ADV_{\mathfrak{C}}&=1/2|Pr[b=b'|T_{11},\cdots,T_{1m}]+Pr[b\ne b'|T_{01},\cdots,T_{0m}]-1|\\&=1/2|Pr[b=b'|T_{11},\cdots,T_{1m}]+(1-Pr[b=b'|T_{01},\cdots,T_{0m}])-1|\\&=1/2|Pr[b=b'|T_{11},\cdots,T_{1m}]-Pr[b=b'|T_{01},\cdots,T_{0m}]|\ge\epsilon_{\mathfrak{A}}/2.\end{aligned}$$

Thus, if $\epsilon_{\mathfrak{A}}$ is non-negligible, then $ADV_{\mathfrak{C}}$ is also non-negligible, which denotes that $\mathfrak{C}$ breaks the improved strong extractors of the modified Goldreich–Levin theorem (Lemma 1). Therefore, $Game_0$ and $Game_1$ cannot be distinguished with non-negligible probability.

In $Game_1$, we find that the challenge ciphertext

$$CT^*=Encrypt(MPK,M_b,\varGamma;T_1,\cdots,T_m),$$

where $T_1,\cdots,T_m$ are randomly chosen from $\mathbb{Z}_N$. Thus, the answers

$$\{\{f_1(s_1^*),\cdots,f_1(s_m^*)\},\cdots,\{f_q(s_1^*),\cdots,f_q(s_m^*)\}\}$$

to the randomness leakage queries will not provide any information of CT^*. Then, $Game_1$ is the same CPA secure game of the $\varLambda'$ scheme. As $\varLambda'$ is CPA secure with auxiliary input, we have that $ADV_{\mathfrak{A}}^{Game_1}$ is negligible. So, the $\varLambda$ scheme is CPA secure with improved auxiliary input. □

4.2. Performance comparison

In this section, we choose three schemes, e.g., the Lewko et al. scheme [37], Zhang et al. scheme [23], and Wang et al. scheme [43], to compare with our scheme in performance. These four schemes are all CP-ABE schemes with leakage resiliency. However, the representations of access policy in these schemes are different.

Let P denote the pairing computation cost, E denote the exponent cost, Mu denote the point multiplication, and Ip denote the inner product. For [37,43], and our scheme, we assume that the LSSS matrix is $l\times n$. For [37] and [23], we denote the leakage parameter as ξ, the allowable leakage probability as ϖ, and the leakage bound (secret key) as η. For [23], let κ denote the number of minimal sets. In decryption, we only evaluate the computational costs of pairing, because the cost of the pairing operation is significantly heavier than other operations.

From Table 1, we can conclude that the computational cost of the two schemes in the bound leakage and continuous leakage models are primarily dependent on the leakage parameter ξ, while the computational cost of the Wang et al. scheme

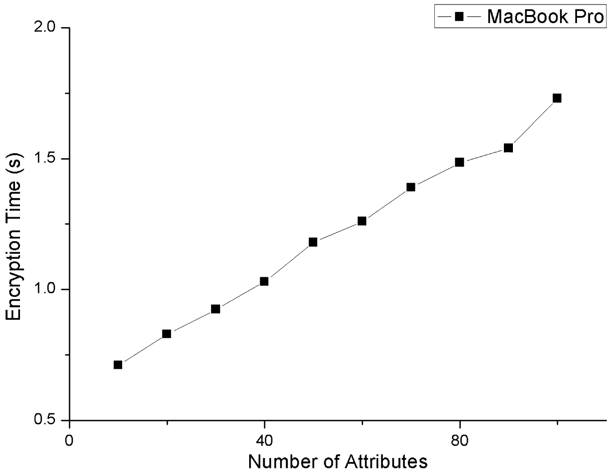

Fig. 2. Performance of encryption on MacBook.

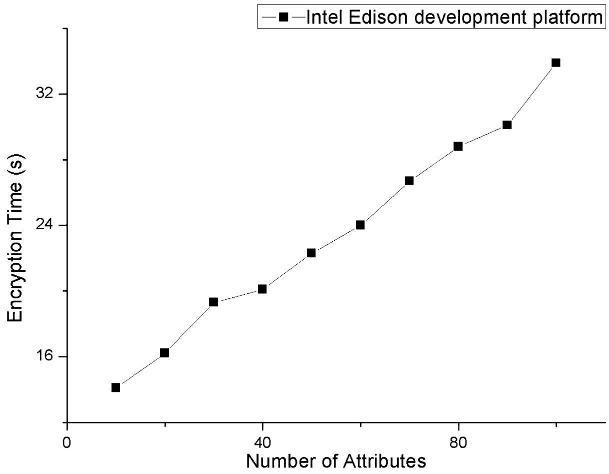

Fig. 3. Performance of encryption on Edison.

and our scheme are primarily dependent on m, which is the number of pieces, and these two schemes with auxiliary input have no leakage bound. Compared with the Wang et al. scheme [43], although there are added m inner products in the encryption of our scheme, our scheme can capture leakage, both from the secret key and randomness (improved auxiliary input model).

To test the performance of our CP-ABE scheme, we implemented our scheme on two platforms as shown in Figs. 2–4. The first platform is a MacBook Pro with Intel core i5 CPU (2.5 GHz). The second is an Edison platform with a dual-core, dual-threaded Intel Atom CPU at 500 MHz. The Edison platform is designed to rapidly prototype IoT products. In big data applications, data are usually generated and encrypted by constrained resource devices like IoT devices. Thus, we test the encryption time of our scheme on the Intel Edison development platform as shown in Fig. 3. We implemented our CP-ABE scheme in C by using the pairing based cryptography (PBC) library [44], and the Type-A curves that offer the highest efficiency among all types of curves. We let $m = 80$, then, the probability of hard to invert is about 2^{80}.

In big data applications, the decryption algorithm is usually executed by powerful devices, such as cloud servers. Thus, we only tested it on the MacBook Pro as shown in Fig. 4.

5. Construction of KP-ABE with improved auxiliary input

In [43], Wang et al. also proposed a KP-ABE scheme with auxiliary input, let $\Xi' = (Setup', KeyGen', Encrypt', Decrypt')$ denote the Wang et al. KP-ABE scheme, where the encryption randomness is in $\mathbb{Z}_N^m$. Let $\mathbb{D} = \{\mathbb{C}_1, \cdots, \mathbb{C}_n\}$ be a monotone access structure, and all $\mathbb{C}_i$s are authorized attribute sets. We can construct a KP-ABE scheme Ξ with improved auxiliary input as follows:

Setup(1^λ): The Setup algorithm runs $(MPK', MSK') \leftarrow Setup'(1^\lambda)$, and randomly chooses vectors $r_1, \cdots, r_m$ from $\{0,1\}^l$. Then, the master public key is $MPK = (MPK', r_1, \cdots, r_m)$, and master secret key is $MSK = MSK'$.

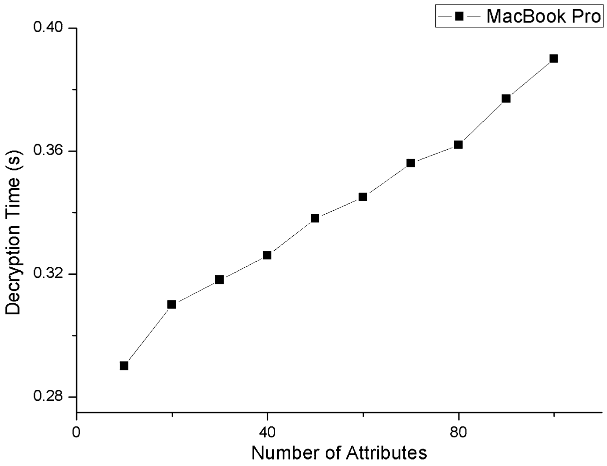

Fig. 4. Performance of decryption on MacBook.

KeyGen($MSK, MPK, \mathbb{D}$**)**: The KeyGen algorithm takes a monotone access structure $\mathbb{D}$, and master public/secret key pair (MPK, MSK) as input. It runs

$$SK_{\mathbb{S}} \leftarrow KeyGen'(MSK, MPK, \mathbb{D}).$$

Encrypt($MPK, M, \mathbb{C}$**)**: The Encrypt algorithm takes an attribute set $\mathbb{C}$, a message M and master public key MPK as input. It randomly selects vectors $s_1, \cdots, s_m \in \mathbb{Z}_N^l$, and then computes $s'_1 = <r_1, s_1>, \cdots, s'_m = <r_m, s_m>$. The generated ciphertext is

$$CT = Encrypt'(MPK, M, \mathbb{C}; s'_1, \cdots, s'_m).$$

Decrypt(CT, SK, MPK**)**: It recovers $M \leftarrow Decrypt'(CT, SK, MPK)$.

Theorem 4. *If Ξ' is a CPA secure KP-ABE scheme leakage resilient to auxiliary input with respect to secret key SK, and inner product $<r_i, s_i>$ for $i = 1, \cdots, m$ is $(\epsilon_r, negl(\lambda))$-strong extractors in the auxiliary input model, then Ξ is a CPA secure CP-ABE scheme with improved auxiliary input.*

Proof. Similar to the proof of Theorem 1, we also denote the randomness used in the challenge ciphertext as $s_1^*, \cdots, s_m^*$. Assuming that $Game_0$ is the CPA security game of Λ scheme with auxiliary input, $Game_1$ is the same as $Game_0$ except that $s'_1, \cdots, s'_m$ are replaced by the random values $s''_1, \cdots, s''_m$ from $\mathbb{Z}_N$, when encrypting the challenge ciphertext. The attacker, $\mathfrak{A}$, creates leakage queries $f_i(s_1^*), \cdots, f_i(s_m^*)$ for both games.

Let $ADV_{\mathfrak{A}}^{Game_i}(\Lambda)$ denote the advantage that the attacker, $\mathfrak{A}$, wins in $Game_i$. Because an improved strong extractor has been used in our construction, we can prove that $|ADV_{\mathfrak{A}}^{Game_0}(\Lambda) - ADV_{\mathfrak{A}}^{Game_1}(\Lambda)|$ is negligible for any PPT attacker $\mathfrak{A}$. First, we assume that there exists an attacker, $\mathfrak{A}$, that can make $|ADV_{\mathfrak{A}}^{Game_0}(\Lambda) - ADV_{\mathfrak{A}}^{Game_1}(\Lambda)| \geq \epsilon_{\mathfrak{A}}$ be a non-negligible probability.

Similar to the proof of Theorem 1, the challenger, $\mathfrak{C}$, is also given

$$(\{\tau_1, \cdots, \tau_m\}, \{\{f_1(s_1^*), \cdots, f_1(s_m^*)\}, \cdots, \{f_q(s_1^*), \cdots, f_q(s_m^*)\}\}, \{T_1, \cdots, T_m\}),$$

where $T_{0i} = <\tau_i, s_i^*>$ or $T_{1i} = u$, which is a random value from $\mathbb{Z}_N$, for $i = 1, \cdots, m$. No PPT attacker can recover at least one of $s_1^*, \cdots, s_m^*$ greater than $1 - (1 - \epsilon_r)^m$ owing to the improved strong extractor property. Then, $\mathfrak{C}$ runs $(MPK, MSK) \leftarrow Setup(1^\lambda)$ and $SK \leftarrow KeyGen(MSK, MPK, \mathbb{S})$. $\mathfrak{C}$ can answer the secret key leakage queries because it has SK. Finally, $\mathfrak{A}$ submits two messages M_0 and M_1 with the same length to $\mathfrak{C}$, and $\mathfrak{C}$ returns the challenge ciphertext

$$CT^* = Encrypt(MPK, M_b, \mathbb{C}; T_1, \cdots, T_m)$$

to $\mathfrak{A}$, where b is a random bit. Finally, $\mathfrak{A}$ outputs its guess bit b', and if $b = b'$, then $\mathfrak{C}$ outputs 1; otherwise, it outputs 0. Because $|ADV_{\mathfrak{A}}^{Game_0}(\Lambda) - ADV_{\mathfrak{A}}^{Game_1}(\Lambda)| \geq \epsilon_{\mathfrak{A}}$, we easily have that $ADV_{\mathfrak{C}} \geq \epsilon_{\mathfrak{A}}/2$. Thus, if $\epsilon_{\mathfrak{A}}$ is non-negligible, then $ADV_{\mathfrak{C}}$ is also non-negligible, which denotes that $\mathfrak{C}$ breaks the property of improved strong extractors. Therefore, $Game_0$ and $Game_1$ cannot be distinguished with non-negligible probability.

In $Game_1$, all the elements in the challenge ciphertext CT^* are randomly chosen from $\mathbb{Z}_N$. Thus, the answers to the leakage queries will not provide any information of CT^*. Then, $Game_1$ is the same CPA secure game of the Ξ' scheme. Thus, the Ξ scheme is also CPA secure with improved auxiliary input. □

Moreover, we tested the encryption time of our KP-ABE scheme on MacBook Pro and Edison platform, and the result is similar to the CP-ABE scheme.

6. Conclusion

Access control is a significant security and privacy challenge in big data security, and ABE is a good cryptographic tool for access control in many scenarios of open networks, such as cloud incident handling, wireless sensor networks, etc. However, when ABE is deployed in big data applications, there are practical threats for both data owner and user. For example, the data user's (decryptor) secret key may be leaked by the side channel attacks, while the randomness used by the data owner (encryptor) can also be leaked owing to a PRNG weakness. However, existing leakage resilient ABE schemes only capture the leakage from the decryptor, and thus, designing a leakage resilient ABE scheme to capture the leakage from both sides remains an open problem. In this paper, we tackle this problem by proposing a security model of leakage resilient ABE with improved auxiliary input, which allows the attacker to make more leakage queries after seeing the challenge ciphertext. Then, we propose a concrete CP-ABE scheme and KP-ABE scheme with improved auxiliary input based on the Wang et al. construction. From the theoretical analysis and experimental result, our schemes are good secure solutions for the volume and velocity of big data. Furthermore, we propose an improved strong extractor from the modified Goldreich–Levin theorem for the security proof, and we prove that our schemes are CPA secure under the security of the Wang et al. construction. Because the encryption is usually executed by devices with constrained resources in big data applications, improving the efficiency of the encryption algorithm in our schemes is an interesting research direction in the future.

Acknowledgments

This research is partially supported by the National Natural Science Foundation of China under Grant Nos. 61373006, 61672016, the Qing Lan Project, the Open Project Program under Grant Nos. GDXXAQ2016-06, AGK201603 and the Humanities and Social Science Research Planning Fund of the Education Ministry of China under grant No. 15YJCZH201.

References

[1] Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, Fengxiao Huang, Enabling personalized search over encrypted outsourced data with efficiency improvement, IEEE Trans. Parallel Distrib. Syst. 27 (9) (2016) 2546–2559, http://dx.doi.org/10.1109/TPDS.2015.2506573.

[2] Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 27 (2) (2015) 340–352.

[3] Jian Shen, Haowen Tan, Jin Wang, Jinwei Wang, Sungyoung Lee, A novel routing protocol providing good transmission reliability in underwater sensor networks, J. Internet Technol. 16 (1) (2015) 171–178.

[4] Yongjun Ren, Jian Shen, Jin Wang, Jin Han, Sungyoung Lee, Mutual verifiable provable data auditing in public cloud storage, J. Internet Technol. 16 (2) (2015) 317–323.

[5] Yanjiang Yang, Haiyan Zhu, Haibing Lu, Jian Weng, Youcheng Zhang, Kim-Kwang Raymond Choo, Cloud based data sharing with fine-grained proxy re-encryption, Pervasive Mob. Comput. 28 (June 2016) 122–134.

[6] Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, Jianying Zhou, Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data, in: ESORICS 2015, in: Lect. Notes Comput. Sci., vol. 9327, 2015, pp. 146–166.

[7] Cloud Security Alliance, Expand top ten big data security and privacy challenges, 2015.

[8] Rong Jiang, Rongxing Lu, Kim-Kwang Raymond Choo, Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data, Future Gener. Comput. Syst. (2016), http://dx.doi.org/10.1016/j.future.2016.05.005 (in press), available online 12 May 2016.

[9] Christian Esposito, Aniello Castiglione, Kim-Kwang Raymond Choo, Encryption-based solution for data sovereignty in federated clouds, IEEE Cloud Comput. 3 (1) (2016) 12–17.

[10] Hongbing Wang, Peng Zeng, Kim-Kwang Raymond Choo, MDMR-IBE: efficient multiple domain multi-receiver identity-based encryption, Secur. Commun. Netw. 7 (11) (2014) 1641–1651.

[11] Lingjun Zhao, Lajiao Chen, Rajiv Ranjan, Kim-Kwang Raymond Choo, Jijun He, Geographical information system parallelization for spatial big data processing: a review, Clust. Comput. 19 (1) (2016) 139–152.

[12] Darren Quick, Kim-Kwang Raymond Choo, Big forensic data reduction: digital forensic images and electronic evidence, Clust. Comput. 19 (2) (2016) 723–740.

[13] Surya Nepal, Rajiv Ranjan, Kim-Kwang Raymond Choo, Trustworthy processing of healthcare big data in hybrid clouds, IEEE Cloud Comput. 2 (2) (2015) 78–84.

[14] Nurul Hidayah Ab Rahman, Niken Dwi Wahyu Cahyani, Kim-Kwang Raymond Choo, Cloud incident handling and forensic-by-design: cloud storage as a case study, Concurr. Comput. (2016), http://dx.doi.org/10.1002/cpe.3868 (in press), available online.

[15] Christian J. D'Orazio, Kim-Kwang Raymond Choo, Laurence T. Yang, Data exfiltration from internet of things devices: iOS devices as case studies, IEEE Int. Things J. PP (99) (2016) 1–6.

[16] Niken Dwi Wahyu Cahyani, Ben Martini, Kim-Kwang Raymond Choo, AKBP Muhammad Nuh Al-Azhar, Forensic data acquisition from cloud-of-things devices: windows smartphones as a case study, Concurr. Comput. (2016), http://dx.doi.org/10.1002/cpe.3855 (in press), available online.

[17] Ben Martini, Kim-Kwang Raymond Choo, Distributed filesystem forensics: XtreemFS as a case study, Digit. Investig. 11 (4) (2014) 287–299.

[18] Ben Martini, Kim-Kwang Raymond Choo, Cloud storage forensics: ownCloud as a case study, Digit. Investig. 10 (4) (2013) 295–313.

[19] Ben Martini, Kim-Kwang Raymond Choo, Cloud forensic technical challenges and solutions: a snapshot, IEEE Cloud Comput. 1 (4) (2014) 20–25.

[20] Darren Quick, Kim-Kwang Raymond Choo, Google drive: forensic analysis of data remnants, J. Netw. Comput. Appl. 40 (2014) 179–193.

[21] Darren Quick, Kim-Kwang Raymond Choo, Digital droplets: microsoft SkyDrive forensic data remnants, Future Gener. Comput. Syst. 29 (6) (2013) 1378–1394.

[22] A. Sahai, B. Waters, Fuzzy identity based encryption, in: EUROCRYPT'05, in: Lect. Notes Comput. Sci., vol. 3494, Springer-Verlag, Berlin, 2005, pp. 457–473.

[23] Mingwu Zhang, Wei Shi, Chunzhi Wang, Zhenhua Chen, Yi Mu, Leakage-resilient attribute-based encryption with fast decryption: models, analysis and constructions, in: ISPEC 2013, in: Lect. Notes Comput. Sci., vol. 7863, 2013, pp. 75–90.

[24] A. Lewko, T. Okamoto, A. Sahai, T. Takashima, B. Waters, Fully securefunctional encryption: attribute-based encryption and (hierarchical) inner product encryption, in: EUROCRYPT'10, in: Lect. Notes Comput. Sci., vol. 6110, Springer-Verlag, Berlin, 2010, pp. 62–91.

[25] A. Akavia, S. Goldwasser, V. Vaikuntanathan, Simultaneous hardcore bits and cryptography against memory attacks, in: TCC'09, in: Lect. Notes Comput. Sci., vol. 5444, Springer-Verlag, Berlin, 2009, pp. 474–495.

[26] J. Alwen, Y. Dodis, M. Naor, Public-key encryption in the bounded-retrieval model, in: EUROCRYPT'10, in: Lect. Notes Comput. Sci., vol. 6110, Springer-Verlag, Berlin, 2010, pp. 113–134.

[27] Y. Dodis, A. Lewko, B. Waters, D. Wichs, Storing secrets on continually leaky devices, in: FOCS'11, 2011, pp. 688–697.

[28] B. Yang, M. Zhang, LR-UESDE: a continual-leakage resilient encryption with unbounded extensible set delegation, in: ProvSec'12, in: Lect. Notes Comput. Sci., vol. 7496, Springer-Verlag, Berlin, 2012, pp. 125–142.

[29] M. Zhang, B. Yang, T. Takagi, Bounded leakage-resilient functional encryption with hidden vector predicate, Comput. J. 56 (4) (2013) 464–477.

[30] V. Goyal, A. Jain, O. Pandey, A. Sahai, Bounded ciphertext policy attribute-based encryption, in: Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'08, Springer-Verlag, Berlin, 2008, pp. 579–591.

[31] Brent Waters, Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, in: Public Key Cryptography, 2011, pp. 53–70.

[32] Amos Beimel, Secure Schemes for Secret Sharing and Key Distribution, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[33] J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Wallsh, D. Wichs, Public-key encryption in the bounded-retrieval model, in: EUROCRYPT, 2010, pp. 113–134.

[34] J. Alwen, Y. Dodis, D. Wichs, Leakage-resilient public-key cryptography in the bounded-retrieval model, in: CRYPTO, 2009, pp. 36–54.

[35] D. Di Crescenzo, R.J. Lipton, S. Wallsh, Perfectly secure password protocols in the bounded retrieval model, in: TCC, 2006, pp. 225–244.

[36] Y. Dodis, K. Haralambiev, A. Lopez-Alt, D. Wichs, Cryptography against continuous memory attacks, in: FOCS, 2010, pp. 511–520.

[37] A. Lewko, Y. Rouselakis, B. Waters, Achieving leakage resilience through dual system encryption, in: TCC 2011, in: Lect. Notes Comput. Sci., vol. 6597, 2011, pp. 70–88.

[38] Victor Changa, Yen-Hung Kuob, Muthu Ramachandrana, Cloud computing adoption framework: a security framework for business clouds, Future Gener. Comput. Syst. 57 (April 2016) 24–41.

[39] Y. Dodis, S. Goldwasser, Y.T. Kalai, C. Peikert, V. Vaikuntanathan, Public key encryption schemes with auxiliary inputs, in: D. Micciancio (Ed.), TCC 2010, in: Lect. Notes Comput. Sci., vol. 5978, Springer, Heidelberg, 2010, pp. 361–381.

[40] Tsz Hon Yuen, Sherman S.M. Chow, Ye Zhang, Siu-Ming Yiu, Identity-based encryption resilient to continual auxiliary leakage, in: EUROCRYPT 2012, 2012, pp. 117–134.

[41] K. Michaelis, C. Meyer, J. Schwenk, Randomly failed! The state of randomness in current java implementations, in: E. Dawson (Ed.), CT-RSA 2013, in: Lect. Notes Comput. Sci., vol. 7779, Springer, Heidelberg, 2013, pp. 129–144.

[42] Tsz Hon Yuen, Ye Zhang, Siuming Yiu, Joseph K. Liu, Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks, in: ESORICS 2014, Part I, in: Lect. Notes Comput. Sci., vol. 8712, 2014, pp. 130–147.

[43] Zhiwei Wang, Siu Ming Yiu, Attribute-based encryption resilient to auxiliary input, in: ProvSec 2015, in: Lect. Notes Comput. Sci., vol. 9451, 2015, pp. 371–390.

[44] B. Lynn, The pairing-based cryptography (pbc) library, http://crypto.stanford.edu/pbc.