Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 749568, 5 pages
http://dx.doi.org/10.1155/2014/749568

Research Article

A Function Private Attribute-Based Encryption

Fei Han and Jing Qin

School of Mathematics, Shandong University, Jinan 250000, China

Correspondence should be addressed to Jing Qin; qinjing@sdu.edu.cn

Received 5 December 2013; Accepted 23 December 2013; Published 23 January 2014

Academic Editor: Jin Li

The function privacy notion was proposed by Boneh, Raghunathan, and Segev in August 2013. It guarantees that the secret key reveals nothing to malicious adversary, beyond the unavoidable minimal information such as the length of ciphertext. They constructed a function private identity-based encryption that contains equality functionality. In this work we construct a new function private attribute-based encryption which supports more complex functionality. And we transform it to a searchable encryption. In searchable encryption, the trapdoor of searching keywords can be seen as the secret key. Hence, using this system can efficiently resist keyword guessing attack.

1. Introduction

Functional encryption [1, 2] is now being seen as a powerful tool especially on the application of cloud security, such as searchable encryption, secure auditing, and secure data sharing. It is a new paradigm for public key encryption. In this system, the decryption ability of a receiver is determined by whether the secret key and the ciphertext can be computed by the function. Identity-based encryption (IBE) [3, 4] can be seen as a functional encryption that supports a equality functionality. Fuzzy identity-based encryption [5] is the first functional encryption that supports nontrivial functionality, whose functionality is a k out of n threshold function. Then it is extended to attribute-based encryption (ABE) [6] classified as key-policy ABE(KP-ABE) and ciphertext-policy ABE(CP-ABE). Subsequently, many other functional encryption schemes are constructed to support certain specific functionality such as predicate encryption [7] and inner product encryption [8]. Security is also concerned about by scholars, from a selective-set security model [5–7] to a fully security model [8]. Meanwhile, other public key cryptographic primitives are also developed [9, 10]. Gorbunov et al. [11] extended the access control policy to polynomial size circuit based on LWE assumption. They used a novel technique named as "Two-to-One Recoding" (TOR) to achieve this goal and also built a scheme based on bilinear maps using a weak TOR scheme. Then, Boneh et al. [12] built an attribute-based encryption for arithmetic circuits with much shorter secret keys. And their scheme is more suitable to the access policies that can be naturally represented as arithmetic circuits.

Recently, Boneh et al. [13, 14] put forth a novel security notion, function private, to protect the privacy of secret key in identity-based encryption. If a scheme is function private, the secret key of the scheme is indistinguishable with a random element chosen from the secret key space. They introduced an approach called "Extract-Augment-Combine" to achieve the function privacy. However, in their schemes, only the function privacy of IBE is realized, and how to construct a function private functional encryption is left as an open problem. We partly solved it in this work by proposing a function privacy KP-ABE scheme using a similar technique introduced in [13].

Searchable encryption is also a special class of function encryption, which is motivated by the demand for applying securely search on remote encrypted data. It is firstly introduced by Song et al. [15]. It is built on private key, so it is used to be called searchable symmetric encryption. However, it was not fully secure and only supported the two-party model. Then, many secure searchable encryptions based on symmetric encryption are proposed [16, 17]. But these schemes were still unsuitable to the third-party situation. Boneh et al. proposed the first searchable public key encryption, public key encryption with keyword search (PEKS) [18].

It is the first searchable public key encryption that enables a third party to implement a keyword search. Abdalla et al. [19] proposed a transformation from anonymous IBE to PEKS and fulfilled the security definition. All of the above schemes only support single designated receiver. Han et al. [20] constructed a scheme that supports nondesignated receivers using KP-ABE. The scheme is secure and satisfies a weak anonymity called attribute private. They also proposed a general transformation from KP-ABE to ABEKS (attribute-based encryption with keyword search) and constructed a secure searchable attribute-based encryption.

Recently, Byun et al. [21] raised an attack called off-line keyword guessing attack (KGA) on searchable encryption, due to the relatively small keywords set (such as a frequently using keyword "urgent"). So an attacker can use the brute-force technique to searching by all keywords to find a collision of the keyword. Jeong et al. [22] asserted that the consistency of searchable public key encryption contradicts keyword guessing attack. Subsequently, scholars studied this attack and proposed some schemes which can resist keyword guessing attack [23–25]. In this paper, we proved that function privacy of function encryption can be transformed to the KGA security of searchable encryption.

Our Contributions. Inspired by the work of Boneh et al. [13], we construct a function private attribute-based encryption based on the scheme of [20]. Moreover, our scheme achieves data security, attribute privacy, and function privacy. Then, we construct a searchable attribute-based encryption against keyword guessing attack using the transformation introduced in [20]; our construction is more natural compared with previous constructions [23–25].

2. Preliminaries

Notations. For an integer $n \in \mathbb{N}$, we denote by $[n]$ the set $\{1, 2, \ldots, n\}$ and by $\mathbb{U}_n$ the uniform distribution over the set $\{0,1\}^n$. For a random variable X, we denote by $x \leftarrow X$ the process of sampling a value x according to the distribution of X. Similarly, for a finite set S, we denote by $s \leftarrow S$ the process of sampling a value s, according to the uniform distribution over S. We denote by $X = (X_1, \ldots, X_T)$ a joint distribution of T random variables.

The *min-entropy* of a random variable X is $H_\infty(X) = -\log(\max_x \Pr[X = x])$. A *k-source* is a random variable X with $H_\infty(X) \geq k$. A T, *k-block source* is a random variable $X = (X_1, \ldots, X_T)$, where, for every $i \in [T]$ and $x_1, \ldots x_{i-1}$, it holds that $H_\infty(X_i \mid X_1 = x_1, \ldots, X_{i-1} = x_{i-1}) \geq k$. The *statistical distance* between two random variables X and Y over a finite domain Ω is $\mathrm{SD}(X, Y) = \sum_{w \in \Omega} |\Pr[X = w] - \Pr[Y = w]|/2$. Two random variables X and Y are δ-*close*, if $\mathrm{SD}(X, Y) \leq \delta$.

Definition 1 (access structure, see [26]). Let $\{P_1, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, \ldots, P_n\}}$ is monotone if, for all ,C: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (resp., monotone access structure) is a collection (resp., monotone collection) $\mathbb{A}$ of nonempty subsets of $\{P_1, \ldots, P_n\}$; that is, $\mathbb{A} \subseteq 2^{\{P_1, \ldots, P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

In our settings, attributes will play the role of parties. We will only deal with the monotone access structures.

We now introduce the LSSS definition adapted from [26].

Definition 2 (linear secret sharing scheme (LSSS)). A secret sharing scheme Π over a set of parties $\mathcal{P}$ is called linear (over $\mathbb{Z}_p$), if

(i) the shares for each party form a vector over $\mathbb{Z}_p$,

(ii) there exists a matrix A called the share-generating matrix for Π. The matrix A has l rows and n columns. For all $i = \{1, \ldots l\}$, the ith row of A is labeled by a party $\rho(i)$ (ρ is a function from $\{1, \ldots l\}$ to $\mathcal{P}$). When we consider the column vector $v = (s, r_2, \ldots r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared and $r_2, \ldots r_n \in \mathbb{Z}_p$ are randomly chosen, then Av is the vector of l shares of the secret s according to Π. The share $(Av)_i$ belongs to a party $\rho(i)$.

The linear reconstruction property is described as follows. Assume that Π is an LSSS for access structure A. Let S be an authorized set, and define $I \subseteq \{1, \ldots l\}$ as $I = \{i \mid \rho(i) \in S\}$. Then there exist constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$, such that, for any valid shares $\{\lambda_i\}$ of a secret s according to Π, we will have $\sum_{i \in I} \omega_i \lambda_i = s$. These constants $\{\omega_i\}$ can be found in polynomial time of the size of share-generating matrix A [26]. And, for unauthorized sets, no such constants $\{\omega_i\}$ exist.

Definition 3 (see [13]). A collection $\mathcal{H}$ of functions $H : U \to V$ is universal if, for any $x_1, x_2 \in U$, such that $x_1 \neq x_2$, it holds that $\Pr_{H \leftarrow \mathcal{H}}[H(x_1) \neq H(x_2)] = 1/|V|$.

Lemma 4 (see [13], leftover hash lemma for block sources). *Let $\mathcal{H}$ be a universal collection of function $H : U \to V$, and let $X = (X_1, \ldots, X_l)$ be an (l, k)-block-source where $k \geq \log|V| + 2\log(1/\varepsilon) + \Theta(1)$. Then, the distribution $(H, H(X_1), \ldots H(X_l))$, where $H \leftarrow \mathcal{H}$, is εl-close to the uniform distribution over $\mathcal{H} \times V^l$.*

The proof is omitted here; we refer the readers to [13] for more detail.

The security model for function private attribute-based encryption is described as follows. This model is derived from [13]. The original model in [13] is for identity-based encryption; our security model is for attribute-based encryption.

Definition 5 (real-or-random function-privacy oracle for ABE). The real-or-random function-privacy oracle $\mathrm{RoR}^{\mathrm{FP}}$ takes input triples of the form (mode, msk, V), where mode $\in$ {Real, Rand}, msk is a master secret key, and $\mathbb{A} = (A_1, \ldots, A_l) \in S^{m \cdot l}$ is representing a joint distribution over $S^{m \cdot l}$ (i.e., each A_i is a distribution over S^m). If mode = Real then the oracle samples A is chosen from $\mathbb{A}$ and if mode = rand then the oracle samples $A \leftarrow S^{m \cdot l}$ uniformly. It then invokes the algorithm KeyGen (msk,·) on A for outputting a secret key sk_A.

Definition 6 (function-privacy adversary, see [13]). An (l, k)-block-source function private adversary $\mathscr{A}$ is an algorithm that is given as input a pair $(1^\lambda, \text{pp})$ and oracle access to RoR^{FP} (mode, msk,·) for some mode $\in$ {Real, Rand} and to KeyGen(msk,·). It is required that each of $\mathscr{A}$'s queries to RoR^{FP} be an (l, k)-block-source.

Definition 7 (function privacy of ABE). An attribute-based encryption scheme ABE = (Setup, KeyGen, Enc, Dec) is (l, k)-*block-source function private* if, for any probabilistic polynomial-time (l, k)-block-source function private adversary $\mathscr{A}$, there exists a negligible function $g(\lambda)$ such that

$$\begin{aligned}\text{Adv}^{\text{FP}}_{\mathscr{ABE},\mathscr{A}}(\lambda) = \Big|&\Pr\left[\text{Exp}^{\text{real}}_{\text{FP},\mathscr{ABE},\mathscr{A}}(\lambda) = 1\right] \\ &- \Pr\left[\text{Exp}^{\text{rand}}_{\text{FP},\mathscr{ABE},\mathscr{A}}(\lambda) = 1\right]\Big| \le g(\lambda),\end{aligned} \tag{1}$$

where, for each mode $\in$ {Real, Rand} and $\lambda \in \mathbb{N}$, the experiment $\text{Exp}^{\text{mode}}_{\text{FP},\mathscr{ABE},\mathscr{A}}(\lambda)$ is defined as follows:

(1) $(\text{pp}, \text{msk}) \leftarrow \text{Setup}(1^\lambda)$;

(2) $b \leftarrow \mathscr{A}^{\text{RoR}^{\text{FP}}(\text{mod } e, \text{msk},\cdot),\ \text{KeyGen}(\text{msk},\cdot)}(1^\lambda, \text{pp})$;

(3) Output b.

3. The Concrete Scheme

3.1. The Original Scheme. The construction of attribute-based encryption in [20] is described as follows;

$$\text{Setup}(\lambda, U) \longrightarrow (\text{PK}, \text{MSK}). \tag{2}$$

First, the algorithm chooses a bilinear group G of order $p_1\, p_2\, p_3\, p_4$, and then picks up random numbers $\alpha \in \mathbb{Z}_N$, g, $X_1 \in G_{p_1}$, where G_{p_1} is the subgroup of order p_1 in G. For any attribute i in global universe attribute set U, the algorithm picks up a hash function H, computes $H(i)$, and then chooses a random number $s_{H(i)} \in \mathbb{Z}_N$, X_3, g_4 as the generators of G_{p_3}, G_{p_4}, $X_4 \in G_{p_4}$, $t = X_1X_4$. We define

$$\begin{aligned}\text{PK} &= \left\{N, g, g_4, e(g,g)^\alpha, H, t, T_{H(i)} = g^{s_{H(i)}}, \forall i\right\}, \\ \text{MSK} &= \left\{X_1, X_3, \alpha\right\},\end{aligned} \tag{3}$$

$$\text{Enc}\ (M, \text{PK}, H, S) \longrightarrow \text{CT}. \tag{4}$$

This algorithm picks up a random $s \in \mathbb{Z}_N$, $R, R' \in G_{p_4}$, and computes $H(S) = \{H(i) \mid i \in S\}$ for any attribute $i \in S$. The ciphertext is given as

$$\begin{aligned}\text{CT} = \Big\{&C = Me(g,g)^{\alpha s}, C_0 = g^s R, C_{H(i)} = \left(tT_{H(i)}\right)^s R', \\ &\forall i \in S\Big\},\end{aligned} \tag{5}$$

which also includes the hashed attributed set $H(S)$.

$$\text{KeyGen}\left((\mathbb{A}, \rho), \text{MSK}, \text{PK}, H\right) \longrightarrow \text{SK}, \tag{6}$$

where $\mathbb{A}$ is a matrix, A_x is the xth row of $\mathbb{A}$, ρ is a map, and $\rho : A_x \to \rho(x) \in H(S)$. This algorithm picks up a random vector u such that the first term of u is α and the other terms are random numbers. For each A_x, it chooses random numbers $r_x \in \mathbb{Z}_N$, W_x, $V_x \in G_{p_3}$, and the secret key SK is given as

$$K^1_x = g^{A_x u}\left(X_1 T_{\rho(x)}\right)^{r_x} W_x, \qquad K^2_x = g^{r_x} V_x, \tag{7}$$

$$\text{Dec}\,(\text{CT}, \text{PK}, \text{SK}) \longrightarrow M. \tag{8}$$

Let $H(S)$ denotes the hashed attribute set of CT, and $(\mathbb{A}, \rho)$ denote the matrix and row mapping associated with SK. If $H(S)$ satisfies $\mathbb{A}$; then the algorithm finds a constants ω_x, such that $\sum_{\rho(x)\in H(S)} \omega_x A_x = 1$ (1 represents the vector of the first term is 1, and others are 0). Compute

$$\begin{aligned}&\prod_{\rho(x)\in H(S)} \frac{e\left(C_0, K^1_x\right)^{\omega_x}}{e\left(C_{\rho(x)}, K^2_x\right)^{\omega_x}} \\ &\quad= \prod_{\rho(x)\in H(S)} \frac{e(g,g)^{s\omega_x A_x u} e\left(g, X_1 T_{\rho(x)}\right)^{s\omega_x r_x}}{e\left(g, X_1 T_{\rho(x)}\right)^{s\omega_x r_x}} \\ &\quad= e(g,g)^{s\sum_{\rho(x)\in H(S)} \omega_x A_x u} = e(g,g)^{\alpha s}.\end{aligned} \tag{9}$$

The message can be recovered by $C/e(g,g)^{\alpha s}$.

3.2. The Modification. Above, the original scheme is proved to be data secure and attribute private in [20]. To make our scheme function private, we need to modify the KeyGen algorithm and Dec algorithm.

(1) In KeyGen algorithm, we let the matrix $\mathbb{A}$ be $m * l$; for every attribute i, we denote u_i as $(s_{i,1}\alpha, s_{i,2}, \ldots, s_{i,m})$. The other parameters remain the same. Then, SK is as follows:

$$\left\{K^1_i = g^{A_i u_i}\left(X_1 T_{\rho(i)}\right)^{r_i} W_i, K^2_i = g^{r_i} V_i, s_{i,1}\right\}, \quad i \in [l]. \tag{10}$$

(2) In Dec algorithm, the decrypter finds constants w_i, such that $\sum_{\rho(i)\in H(S)} \omega_i s_{i,1} A_x = 1$; then we can process our Dec algorithm:

$$\begin{aligned}&\prod_{\rho(i)\in H(S)} \frac{e\left(C_0, K^1_i\right)^{\omega_i}}{e\left(C_{\rho(i)}, K^2_i\right)^{\omega_i}} \\ &\quad= \prod_{\rho(i)\in H(S)} \frac{e(g,g)^{s\omega_i A_i u_i} e\left(g, X_1 T_{\rho(i)}\right)^{s\omega_i r_i}}{e\left(g, X_1 T_{\rho(i)}\right)^{s\omega_i r_i}} \\ &\quad= e(g,g)^{s\sum_{\rho(i)\in H(S)} \omega_i A_i u_i} = e(g,g)^{\alpha s}.\end{aligned} \tag{11}$$

In the Dec computation, we let $u_i = s_{i,1} u'_i$ (where the first term of u is α and the other terms are random numbers). Then u'_i can be seen as a vector where the first term is α and the others

are random numbers. u_i' can be seen as u of original scheme. And

$$\sum_{\rho(i)\in H(S)} \omega_i A_i u_i = \sum_{\rho(i)\in H(S)} \omega_i A_i s_i u = u \cdot (1, 0, \ldots, 0) = \alpha. \tag{12}$$

So we can enable our modified scheme to act like the original scheme.

4. Security Analysis

Our modification does not violate the original scheme's security. Since the data security and attribute privacy is proved in [20]; we will prove the function privacy of the modified scheme only.

Function Privacy. Let $\mathcal{A}$ be a computational bounded adversary that makes a polynomial number of queries to the $\mathrm{RoR}^{\mathrm{FP}}$ oracle. We prove that the distribution of $\mathcal{A}$'s view in the experiment $\mathrm{Exp}^{\mathrm{real}}_{\mathrm{FP},\mathcal{ABE},\mathcal{A}}$ is computationally close to the view in the $\mathrm{Exp}^{\mathrm{rand}}_{\mathrm{FP},\mathcal{ABE},\mathcal{A}}$. We denote these two distributions by $\mathrm{View}_{\mathrm{Real}}$ and $\mathrm{View}_{\mathrm{Rand}}$.

By simulating, the adversary queries KeyGen and $\mathrm{RoR}^{\mathrm{FP}}$ oracle and then gets the random variable $A = (A_1, \ldots, A_l)$ corresponding to the (l, k)-source. For each $i \in [l]$, let $(a_{i,1}, \ldots, a_{i,m})$ denote the sample from A_i. Also let $u_i = (s_{i,1}, \ldots s_{i,m}) \in S^m$. Then we can assume that

$$\mathrm{View}_{\mathrm{mode}} = \left(\left(\sum_{j=1}^{m} s_{1,j} a_{1,j} \right), \ldots \left(\sum_{j=1}^{m} s_{l,j} a_{l,j} \right) \right). \tag{13}$$

for mode = {Real, Rand}. For mode = Real, $A = (A_1, \ldots, A_l)$ is drawn from $\mathbb{A}$; for mode = Rand, A is uniformly chosen from $S^{m \cdot l}$. And $u_i \in S^m$ for $i \in [l]$.

Note that the collection of functions $\{g_{s_1,s_2,\ldots,s_m} : S^m \to S\}_{s_1,\ldots,s_m \in S}$ defined as $g_{s_1,s_2,\ldots,s_m}(a_1, \ldots, a_m) = \sum_{i=1}^{m} s_i a_i$ is universal. After applying Lemma 4, we can easily imply that the statistical distance between $\mathrm{View}_{\mathrm{Real}}$ and uniform distribution is negligible. The same clearly holds for $\mathrm{View}_{\mathrm{Rand}}$. This completes the proof of function privacy.

5. Extension to Searchable Encryption

We have constructed a function private attribute-based encryption. In the above scheme, the entropy of secret key is large enough. By the transformation described in [20], we can easily get a searchable attribute-based encryption (ABEKS). Consider

$$\begin{aligned}
&\mathrm{Setup}_{\mathcal{ABEKS}}(\lambda, U) = \mathrm{Setup}_{\mathcal{ABE}}(\lambda, U),\\
&\mathrm{Enc}_{\mathcal{ABEKS}}(M, \mathrm{PK}, H(S)) = \mathrm{Enc}_{\mathcal{ABE}}(M, \mathrm{PK}, H(S)),\\
&\mathrm{KeyGen}_{\mathcal{ABEKS}}((\mathbb{A}, \rho), \mathrm{MSK}, \mathrm{PK}) =\\
&\mathrm{KeyGen}_{\mathcal{ABE}}((\mathbb{A}, \rho), \mathrm{MSK}, \mathrm{PK}),\\
&\mathrm{TrapDoor}_{\mathcal{ABEKS}}(\mathbb{A}, \rho) =\\
&\mathrm{KeyGen}_{\mathcal{ABE}}((\mathbb{A}, \rho), \mathrm{MSK}, \mathrm{PK}),\\
&\mathrm{Test}_{\mathcal{ABEKS}}(\mathrm{CT}, \mathrm{PK}, \mathrm{SK}) = \mathrm{Dec}_{\mathcal{ABE}}(\mathrm{CT}, \mathrm{PK}, \mathrm{SK}).
\end{aligned}$$

Since an adversary cannot efficiently guess a concrete trapdoor built on some access structure owing to the privacy of secret key of ABE scheme, our scheme can resist keyword guessing attack. In fact, when an adversary $\mathcal{A}$ implements a keyword guessing attack, he will randomly pick a valid access control policy associated with a keywords set and run a test to determine whether this keyword set is used to generate a trapdoor.

The security experiment is described as follows:

$$\begin{aligned}
&\mathrm{Exp}^{\mathrm{KGA}}_{\mathcal{ABEKS},\mathcal{A}}(\lambda):\\
&(\mathrm{PK}, \mathrm{MSK}) \longleftarrow \mathrm{Setup}_{\mathcal{ABEKS}}(\lambda, U),\\
&T_{\mathbb{A}} \longleftarrow \mathrm{TrapDoor}_{\mathcal{ABEKS}}(\mathbb{A}, \rho),\\
&\mathbb{A}' \longleftarrow \mathcal{A}(pk, T_{\mathbb{A}}), C_{\mathbb{A}'} \longleftarrow \mathrm{Enc}_{\mathcal{ABEKS}}(\mathbb{A}', pk, H(S)).\\
&\text{If } \mathrm{Test}(C_{\mathbb{A}'}, \mathrm{PK}, T_{\mathbb{A}}), \text{ then return 1, else return 0.}
\end{aligned}$$

We define the advantage of $\mathcal{A}$ in the above experiment as

$$\mathrm{Adv}^{\mathrm{KGA}}_{\mathcal{ABEKS},\mathcal{A}}(\lambda) = \Pr\left[\mathrm{Exp}^{\mathrm{KGA}}_{\mathcal{ABEKS},\mathcal{A}}(\lambda) = 1\right]. \tag{14}$$

Theorem 8. *ABEKS scheme can resist keyword guessing attack, if the original ABE scheme is function private.*

Proof. Let $\mathcal{A}$ be a polynomial time algorithm that implements a keyword guessing attack on ABEKS and let $\mathcal{B}$ be an adversary that breaks the function privacy of ABE. If $\mathcal{A}$ can efficiently obtain a valid keywords set corresponding with some trapdoor, then $\mathcal{B}$ can distinguish the secret key with some random element sampled from secret key space using this trapdoor (i.e., secret key in ABE); that is,

$$\mathrm{Adv}^{\mathrm{KGA}}_{\mathcal{ABEKS},\mathcal{A}}(\lambda) < \mathrm{Adv}^{\mathrm{FP}}_{\mathcal{ABE},\mathcal{B}}(\lambda) \le g(\lambda), \quad g(\lambda) \text{ is a negligible function.} \tag{15}$$

Hence, the proof is completed. □

6. Conclusion

In this paper, we present a function private attribute-based encryption, which at the heart of our construction is a method of randomizing the secret key, so we have achieved that the secret key in our scheme is indistinguishable with the random element sampled from the secret key space. And then we extend it to a searchable attribute-based encryption which resists keyword guessing attack.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors want to express their sincere thanks to the anonymous referees for their valuable comments and suggestions. This work is supported by the National Nature Science Foundation of China under Grant no. 61272091 and the National Nature Science Foundation of Shandong Province under Grant no. ZR2012FM005.

References

[1] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: definitions and challenges," in *Theory of Cryptography*, pp. 253–273, Springer, Berlin, Germany, 2011.

[2] B. Waters, "Functional encryption: origins and recent developments," in *Public-Key Cryptography—PKC 2013*, pp. 51–54, Springer, Berlin, Germany, 2013.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology-CRYPTO 2001*, pp. 213–229, Springer, Berlin, Germany, 2001.

[4] J. Li, F. Zhang, and Y. Wang, "A new hierarchical ID-based cryptosystem and CCA-secure PKE," in *Embedded and Ubiquitous Computing, International Conference (EUC)*, Lecture Notes in Computer Science, pp. 362–371, Springer, 2006.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2005*, pp. 457–473, Springer, Berlin, Germany, 2005.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, November 2006.

[7] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology—EUROCRYPT 2008*, pp. 146–162, Springer, Berlin, Germany, 2008.

[8] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology—EUROCRYPT 2010*, pp. 62–91, Springer, Berlin, Germany, 2010.

[9] J. Li and Y. Wang, "Universal Designated Verifier Ring Signature (Proof) without random oracles," in *Embedded and Ubiquitous Computing, International Conference (EUC)*, Lecture Notes in Computer Science, pp. 332–341, Springer, 2006.

[10] J. Li, K. Kim, F. Zhang, and X. Chen, "Aggregate proxy signature and verifiably encrypted proxy signature," in *Proceedings of the International Conference on Provable Security (ProvSec '07)*, Lecture Notes in Computer Science, pp. 208–217, Wollongong, Australia, 2007.

[11] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pp. 545–554, ACM, 2013.

[12] D. Boneh, V. Nikolaenko, and G. Segev, "Attribute-Based Encryption for Arithmetic Circuits," Cryptology ePrint Archive, Report 2013/669, 2013, http://eprint.iacr.org/2013/669/.

[13] D. Boneh, A. Raghunathan, and G. Segev, "Function-private identity-based encryption: hiding the function in functional encryption," in *Advances in Cryptology—CRYPTO 2013*, 2013.

[14] D. Boneh, A. Raghunathan, and G. Segev, "Function-Private Subspace-Membership Encryption and Its Applications, Cryptology ePrint Archive," Report 2013/403, 2013, http://eprint.iacr.org/2013/403.

[15] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 44–55, May 2000.

[16] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proceedings of the 3rd International Conference on Applied Cryptography and Network Security (ACNS '05)*, pp. 442–455, June 2005.

[17] G. Eu-Jin, "Secure Indexes. Cryptology ePrint Archive," Report 2003/216, 2003, http://eprint.iacr.org/2003/216/.

[18] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology-Eurocrypt 2004*, pp. 506–522, Springer, Berlin, Germany, 2004.

[19] M. Abdalla, M. Bellare, D. Catalano et al., "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in *Advances in Cryptology—CRYPTO, 2005*, pp. 205–222, Springer, Berlin, Germany, 2005.

[20] F. Han, J. Qin, H. Zhao, and J. Hu, "A general transformation from KP-ABE to searchable encryption," *Future Generation Computer Systems*, vol. 30, pp. 107–115, 2014.

[21] J. W. Byun, H. S. Rhee, H. A. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in *Secure Data Management*, pp. 75–83, Springer, Berlin, Germany, 2006.

[22] I. R. Jeong, J. O. Kwon, D. Hong, and D. H. Lee, "Constructing PEKS schemes secure against keyword guessing attacks is possible?" *Computer Communications*, vol. 32, no. 2, pp. 394–396, 2009.

[23] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *Information Sciences*, vol. 238, pp. 221–241, 2013.

[24] C. Hu and P. Liu, "A secure searchable public key encryption scheme with a designated tester against keyword guessing attacks and its extension," in *Advances in Computer Science, Environment, Eco-Informatics, and Education*, pp. 131–136, Springer, Berlin, Germany, 2011.

[25] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2266–2277, 2012.

[26] A. Beimel, *Secure schemes for secret sharing and key distribution [Ph.D. thesis]*, Israel Institute of Technology Technion, Haifa, Israel, 1996.