Challenges and Trends on Predicate Encryption—A Better Searchable Encryption in Cloud

Liang Hu, Yuanmo Zhang, Hongtu Li, Yicheng Yu, Fangming Wu, and Jianfeng Chu
Jilin University, Changchun 130012, China
Email: {hul, chujf}@jlu.edu.cn, {yuanmozhang, yicheng_yu}@126.com, li_hongtu@hotmail.com, wfm227@yeah.net

Abstract —As cloud storage becomes widely used, sensitive data is usually required to be encrypted before stored in the cloud. Searchable encryption schemes provide an important mechanism to cryptographically protect data and make it available to be searched and accessed. Predicate encryption, a recently developed cryptographic primitive, offers a new solution to search on encrypted data and fine-grained access control over the encrypted data. It makes ciphertext related to the attribute and user's secret key and token associated with the predicate. This paper reviews the development of provably secure schemes and some states of the most recent researches. There remain open problems in before works like security issues and lacking of efficiency, which guides us to the future directions.

Index Terms—Predicate encryption, cloud storage, access control, data security

I. Introduction

With the rapid development of the cloud, users begin to store their data in the cloud. Considering data security and user privacy, it is necessary for users to encrypt their sensitive data before moving data to the cloud server. However, it becomes inconvenient when the users attempt to retrieve the documents by some keywords.

In order to solve this problem, searchable encryption (SE) is proposed and attracts researchers' attention to study [1]-[5]. SE saves huge network bandwidth and computation capacity for uses by supporting keyword search over encrypted data in the cloud server. Among different kinds of SE, as a new cryptographic primitive, predicate encryption (PE) provides fine-grained control over the accesses to encrypted data [6]. In a predicate encryption scheme, messages can be encrypted with a set of attributes. A secret token, generated by the secret key owner corresponding to a predicate, can be given to a person as a search privilege. This person can make a search query through this secret token [7]. The cloud server receives the search query from the secret key owner or the above person, and then searches the matched ciphertexts if and only if the set of attributes of the ciphertexts satisfies the predicate of the secret token.

Manuscript received June 23, 2014; revised December 24, 2014.
This work was supported by the Deep exploration instrumentation and equipment development (SinoProbe-09-01-03) under Grant No.201011078.
Corresponding author email: chujf@jlu.edu.cn.
doi:10.12720/jcm.9.12.908-915

Predicate encryption provides a function to search encrypted data and fine-grained access control. That makes a new direction to solve traditional problems. The enhanced functionality and flexibility provided by PE systems are very attractive for many practical applications: network audit logs [8], sharing of medical records [9], un-trusted remote storage [10] and so on. More applied research is needed to build predicate encryption into real-world systems. Since PE mechanism originated in theoretical research, considering its high complexity, it is unable to be widely used in the industry. As a result of this, many fascinating open problems remain. An efficient and flexible mechanism PE plays an important role in promoting the popularity of cloud storage.

The remainder of this paper is organized as follows: Section II presents an overview of some background knowledge. In section III, we describe construction algorithm in public-key and secret-key based PE scheme, then we discuss the classification of security in detail in section IV, present the expressiveness and efficiency of PE schemes in section V and its secret key revocation in section VI. In addition, we make a comparison of some typical schemes in section VII. The final section draws our conclusion and gives future ideas.

II. Preliminaries

Aiming to construct the framework of predicate encryption, much recent work makes contributions. Identity-based encryption (IBE) [11]-[16] can be seen as predicate encryption for the class of equality tests; Attribute-based encryption schemes (ABE) [17]-[20] can also be cast in the framework of predicate encryption, it guarantees a user can receive a private capability that represents a complex access control policy over the attributes of an encrypted record. Hidden vector encryption (HVE) supports the fine-grained conjunctive combination of equality queries, comparison queries, and subset queries on ciphertext [21]-[24], which makes predicate encryption more expressive.

In this section, we proceed from reviewing the brief history and basic concepts of IBE, ABE and HVE.

A. IBE

In an IBE scheme, the sender can use the receiver's identity as a public key to encrypt a message, and the receiver can decrypt the ciphertext by his own private key

obtained from the Private Key Generator (PKG) according to his identity. Since the realization of the first Identity-based encryption schemes by Boneh and Franklin [11], there have been some encryption features provided by the new cryptosystems to increase functionality and expressiveness.

The functions that compose a generic IBE are specified by the following four randomized algorithms:

- Setup: takes a security parameter and returns system master private key MSK and public key PK .
- Extract: takes system parameters, master private key, and an identity as input, and returns a secret private key SK corresponding to the identity.
- Encrypt: takes the master public key, the public key of the receiver node (derived from its identity), and the message as input, and returns the corresponding ciphertext.
- Decrypt: takes the master public key, a ciphertext and the personal private key as input, and returns the decrypted message.

B. ABE

Sahai and Waters propose the first concept of the attribute-based encryption scheme [17]. ABE originally started by generalizing the definition of identity from a string to a set of attributes. The ABE scheme uses an user's identity as attributes, and this set of attributes is used to encrypt and decrypt data.

In 2006, Goyal *et al.* propose a key-policy attribute-based encryption (KP-ABE) scheme that built the access policy into the user's private key and described the encrypted data with user's attributes [18]. The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme.

Bettencourt *et al.* also propose a ciphertext-policy attribute based (CP-ABE) scheme in 2007, and the CP-ABE scheme built the access policy into the encrypted data; a set of attributes is in a user's key [20]. The CP-ABE scheme addresses the problem of KP-ABE that data owner only trusts the key issuer.

The functions that compose a generic ABE are specified by the following four randomized algorithms:

- Setup: takes as input a security parameter and a universe description U , which defines the set of allowed attributes in the system. It outputs the public parameters PK and the master secret key MSK .
- Encrypt: takes as input the public parameters PK , a message and a set of attributes S and outputs a ciphertext associated with the attribute set.
- KeyGen: takes as input the master secret key MSK and an access structure A and outputs a private key SK associated with the attributes.
- Decrypt: takes as input a private key SK associated with access structure A and a ciphertext associated with attribute set S and outputs the message if S satisfies A or the error message otherwise.

C. HVE

The first hidden vector encryption scheme has been given by Boneh and Waters (BW07) which showed that HVE gives efficient encryption schemes supporting conjunctions of equality queries, range queries and subset queries[21]. In a HVE scheme, ciphertexts are associated with binary vectors while private keys are associated with binary vectors with "don't care" entries (denoted by ★). A private key can decrypt a ciphertext if all entries of the key vector that are not ★ agree with the corresponding entries of the ciphertext vector. The later work is extending HVE from bilinear groups of composite order to bilinear groups of prime order. [23,24]

A HVE scheme is a quadruple of probabilistic polynomial-time algorithms such that:

- Setup: takes as input the security parameter and the attribute length n and outputs the master public key PK and the master secret key MSK .
- KeyGen: takes as input the master secret key MSK and string $y \in \{0,1,\bigstar\}^n$ and outputs the decryption key K_y associated with y.
- Encrypt takes as input the public key PK , attribute string $x \in \{0,1\}^n$ and message from the associated message space and returns ciphertext.
- Decrypt: takes as input a secret key K_y and a ciphertext and outputs the message if the two strings must match in positions i where $y_i \neq \bigstar$ and, intuitively, ★ is the "don't care" symbol.

III. PE Construction Algorithm

In IBE, the public key is user's identity. Ciphertext can be decrypted only who has the identity. IBE is not suitable for one-to-many system which ABE is appropriate. In ABE, a data owner just needs to predefine these attributes that he would utilize; he doesn't need to care about the number of users in the system. However, it is disable to encrypt attribute in ABE. PE encrypts the attribute as well as plaintext. The notion of predicate encryption is explicitly presented in KSW08 [25] that covers IBE, ABE and HVE.

In the setting of predicate encryption, secret keys in a predicate encryption scheme correspond to predicates f in some class F , and a sender associates a ciphertext with an attribute in a set Σ ; a ciphertext associated with the attribute can be decrypted by a secret key SK_f corresponding to the predicate $f \in F$ if and only if $f(I)=1$.

Like traditional encryptions, there are two categories in predicate encryption: secret-key predicate encryption schemes [26]-[29] and public-key predicate encryption schemes [30]-[37]. A public-key setting has been proposed for multiple-user applications like broadcast services [38], but its security is weaker than that of a

secret-key setting. On the other hand, a secret-key setting is appropriate for single-user applications. Some secure secret-key schemes are appropriate for simple applications such as remote storage services.

A. Public-Key Predicate Encryption

A public-key predicate encryption scheme for the class of predicates F over the set of attributes Σ consists of four probabilistic polynomial-time algorithms, such that:

- Setup: takes as input the security parameter 1^n; and outputs a public key PK and a master secret key MSK.
- Encrypt: takes as input the public key PK, a plaintext M which in some associated message space, and an attribute $I \in \Sigma$. It returns a ciphertext CT.
- GenKey: takes as input the master secret key MSK and a query predicate $f \in F$. It outputs a key SK.
- Decrypt: takes as input a public key SK, a ciphertext CT. It outputs $f(I)$. Only if $f(I)=1$, it returns a message M. Else it returns $\perp$.

B. Secret-Key Predicate Encryption

Secret-key predicate encryption can be similarly defined as public-key predicate encryption. However, everyone can encrypt using the public-key in public-key encryption. In the secret-key encryption, encryption and decryption are both performed using the secret-key. Hence, only the key owner can encrypt. In both schemes, only the secret-key owner can decrypt.

A secret-key predicate encryption scheme for the class of predicates F over the set of attributes Σ consists of four probabilistic polynomial-time algorithms, such that:

- Setup: takes as input a security parameter 1^n and outputs a secret key SK.
- Encrypt: takes as input a secret key SK and a plaintext $x \in \Sigma$ and outputs a ciphertext CT.
- GenToken: takes as input a secret key SK and a query predicate $f \in F$. It outputs a token TK_f that allows one to evaluate $f(x)$ over an encryption of x.
- Query: takes as input a token TK_f for a predicate f and a ciphertext CT. It outputs either 0 or 1, indicating the value of the predicate f evaluated on the underlying plaintext.

IV. Security

There are several notions of security for predicate encryption schemes. Based on complicated assumptions, PE schemes have different security levels.

A. Payload-Hiding , Attribute-Hiding and Predicate-Hiding

Payload-hiding is the "basic" level of security. It guarantees that adversary cannot obtain anything about the encrypted message. However, it may reveal some information about attributes. I.e., if an adversary A holds keys $SK_{f1}...SK_{fl}$ then A learns nothing about encrypted message by attribute I if $f_1(I)=...=f_l(I)=0$. We refer to this security notion as payload hiding [39].

Attribute-hiding is a stronger notion. It guarantees that no efficient adversary could obtain any information about the attribute which is associated with a ciphertext. Roughly speaking, attribute-hiding requires that a ciphertext conceals not only the plaintext but also the associated attribute. I.e., an adversary holding secret keys learns only the values $f_1(I)...f_l(I)$ [25,40]. There are two levels in attribute hiding. One is weakly attribute-hiding and the other one is fully attribute-hiding. In the fully attribute-hiding security definition [25,33], although the adversary knows SK, he has no idea of the attribute corresponding I to the ciphertext unless that $f(I)=0$. The adversary may obtain some additional information about the attribute, if the algorithm is weakly attribute-hiding.

In FH14 [41], Fan and Huang first propose an extension of predicate encryption, called timed-release predicate encryption. Only after a specified time period, the evaluator can decrypt the ciphertexts that satisfy the predicate. Therefore, FH14 can provide not only ciphertext retrieval with search privacy protection but time trigger. It is proved to be attribute hiding.

In addition to protecting the privacy of plaintexts, it is necessary to defend the description of the predicates encoded by tokens. Prior work on public-key predicate encryption has focused on the notion of plaintext privacy, and ignores the security of tokens. As a result of this, Shen *et al*. present a notion called predicate-hiding in SSW09 [26]. Informally, predicate privacy says that a token hides all information about the encoded predicate other than what is implied by the ciphertexts in one's possession, as we said earlier. Their construction is based on the KSW08 construction [25]. In particular, a token and a ciphertext each encodes a vector in Z_N^n, and the inner product $\langle x, y \rangle$ is commutative. Furthermore, for inner products, ciphertexts and tokens have symmetric roles in the security definitions. One way to interpret this observation is to view a ciphertext as an encryption of a plaintext vector and a token as an encryption of a predicate vector. Their scheme has significant obstacles to practical implementation by using bilinear groups. In addition, its security is based on a variant of the subgroup decision assumption, which implies that it is infeasible to factor a composite order of the bilinear group. Such large composite-order groups, however, result in a heavy load of group operations, markedly reducing the efficiency of the SSW09 scheme. In order to improve the effectiveness, instead of four groups, Yoshino et al. present the symmetric-key inner-product predicate encryption scheme [27] based on three groups. Compared to SSW09, their prime-order group instantiation is asymptotically more than 33% faster and has asymptotically 25% smaller ciphertexts and tokens.

As we said earlier, in the secret-key encryption, only secret-key owner can encrypt. On the contrary, anyone can encrypt data by public-key in the public-key encryption. As a result, an adversary can encrypt any plaintext of his choice and evaluate a token on the resulting ciphertext to know if the plaintext satisfies the predicate associated with the token.

BIP10 is a breakthrough that this is the first time to achieve predicate-hiding in partial public-key based PE [42]. Furthermore, making use of prime order groups greatly improves the efficiency of the resulting encryption schemes. Blundo et al. consider the notion of a partial public key encryption (as suggested in [SSW09]). This scheme is based on BW07 [21]. In order to reach predicate security, BIP10 show that tokens only reveal the positions of the ★-entries in the associated pattern. Because that predicate security is not achievable in a pure public-key scenario, it uses a partial public key model in which the key owner can decide on a policy to generate a subset of the ciphertexts. In the formal definition of predicate secure it requires that an adversary is not able to distinguish between tokens with pattern $\overrightarrow{y_0}$ or $\overrightarrow{y_1}$ with respect to a policy provided that the two patterns have the same value of the predicate Match for all attributes $\vec{x}$ that can be encrypted under policy.

Kawai and Takashima propose a reasonable definition of predicate-hiding inner product encryption (IPE) in a public key setting, which we call inner product encryption with ciphertext conversion (IPE-CC) [34]. In IPE-CC original ciphertexts are converted to predicate-searchable ones by a helper in possession of a conversion key. There are introduced original and converted ciphertexts, and a new conversion key is used as public and secret keys. Each user encrypts an attribute $\vec{x}$ by using the public key, and generates original ciphertext $\mathrm{c}t_{\vec{x}}$. $\mathrm{c}t_{\vec{x}}$ is converted to a predicate-searchable ciphertext $CT_{\vec{x}}$ by a helper who has the conversion key ck. IPE-CC has two types of secret (or trapdoor) keys, sk and ck. An IPE-CC scheme is called fully secure iff it satisfies all the below three security requirements.

- Predicate-hiding of token key $tk_{\vec{v}}$ and attribute-hiding of ciphertexts ($\mathrm{c}t_x, CT_{\vec{x}}$) against any malicious user with no secret key sk or conversion key ck.
- (Fully-)Attribute-hiding of ciphertexts ($\mathrm{c}t_x$, $CT_{\vec{x}}$) against any malicious helper with no secret key sk.
- Predicate-hiding of token key $tk_{\vec{v}}$ and attribute-hiding of ciphertext $\mathrm{c}t_x$ against any malicious private key generate (PKG) with no conversion key.

Predicate-hiding is not achievable in traditional public-key predicate encryption. So IPE-CC progresses a lot to get fully-secure scheme, where all the security properties are proven under the DLIN assumption in the standard model. From the above IPE-CC scheme, it obtains Proposed IPE-CC(variant) scheme and the first fully secure SIPE scheme. However, it is predicate-hiding for tokens from any malicious users except the helper. Therefore, it still faces the risk of leakage.

B. Selectively Secure & Adaptive Secure

In the IBE scheme, selectively secure schemes in the standard model were constructed [13], [38]. Boneh and Boyen [43] and Waters [14] constructed adaptive secure IBE schemes in the standard model. According to these, the selective adaptive secure in predicate encryption scheme is that the advantage of all probabilistic polynomial-time adversaries is negligible in the security parameter. Although some research has achieved the adaptive secure, the majority of the predicate encryption schemes are just proven to be selective secure. The notion of selective secure is the security of a limited model. In this weaker model, before seeing the public parameters of the system, the adversary is obliged to announce the target he intends to attack. This is an unnatural and undesirable restriction on the adversary, but it unfortunately seems to be necessary for the proof techniques used in some works.

The KSW08 IPE scheme is fully attribute-hiding but selectively secure, and the LOS+10[31] and OT10 [32] IPE schemes are adaptively secure but weakly attribute-hiding. In 2012, Okamoto and Takashima propose the first inner product encryption scheme OT12 that is adaptively secure and fully attribute-hiding under the DLIN assumption in the standard model [33]. OT12 extends the dual system encryption technique into a more general manner, in which new forms of ciphertext and secret keys are employed and various forms of ciphertext and secret keys are introduced and new types of information theoretical tricks are employed with several forms of computational reduction. A variant of the OT12 basic scheme with the same security, achieves a shorter master public key and shorter secret keys. This variant also enjoys more efficient decryption.

V. Expressiveness and Efficiency

An important purpose of the predicate capability is designed to support complex query predicate encryption systems. At first, researchers have designed predicate encryption schemes that support an equality test, for example, if we use such a predicate encryption system for the keyword search, the user would be able to make queries of the form: $word = 2014$.

Shi *et al.* propose a searchable encryption scheme that supports multi-dimensional range queries over encrypted data (MRQED) [8]. If the scheme is supporting multi-dimensional range query, it means that we could search range queries on each dimension, like $(\text{age} \in [7,10]) \wedge (grade \in [2,4])$. By assuming that each plaintext entry has D attributes, the query predicates are conjunctions of range queries over a subset of these D attributes. The technique utilizes an interval tree

structure to form a hierarchical representation of intervals along each dimension and stores multiple ciphertexts corresponding to a single data value on the server (one corresponding to each level of the interval tree). This scheme is very similar to the BonehWater06 [35] work in many ways. In such scenarios where T is large and D is small, MRQED is more practical. However, one can also conceive of other applications where T is small and D is large, and in these cases, the BonehWaters06 construction would be more practical.

Although some schemes support conjunctive query such as $(\text{age}=1)\wedge(\text{grade}=2)$ [22], inner-product based on PE is more expressive. By switching it to be an inner product form, it can change $x\in[1,3]$ to $(x=1)\vee(x=2)\vee(x=3)$. Katz *et al*. (KSW08) [25] first focus on predicates corresponding to the computation of inner products. Parameters of inner-product predicates are expressed as vectors $\vec{X}$ (for a ciphertext) and $\vec{V}$ (for a secret key), where $R(\vec{V},\vec{X})$ holds iff $\vec{V}\bullet\vec{X}=0$. (Here, $\vec{V}\bullet\vec{X}$ denotes the standard inner-product.) As far as we know, the widest classes of relations supported by attribute-hiding PE systems are inner-product predicates. Inner-product predicates represent a fairly wide class of relations including equality tests as the simplest case, disjunctions or conjunctions of equality tests, and, more generally, CNF or DNF formulas. To use inner product predicates for such universal relations, we must write formulas in CNF or DNF form, which can cause a super-polynomial blowup in size for arbitrary formulas.

However, predicate encryption mechanisms still need to study how to support more flexible query in the future. Although there is some work to realize searching ciphertexts using range query and subset query, it still no perfect scheme proposed. In the next period of time, proposing a PE algorithm which supports relational operators well remains a hot point.

On the other hand, it is better to have an efficient algorithm. Encryption time, public key size, secret key size, capability size and decryption time, as performance metrics, are used to determine what we mean by efficiency. Some work has done to change from composite-order groups [25], [26] to prime-order groups [27]-[33]. Since KSW08 proposes no delegation functionality. Shi and Waters present a delegation mechanism for a class of PE, but it is a class of equality tests for HVE [22]. That is more restricted than inner-product predicates. In 2009, Okamoto and Takashima present a hierarchical predicate encryption (HPE) scheme for inner-product predicate encryption based on a dual pairing vector spaces (DPVS) [30]. DPVS is extended from bilinear pairing groups into higher dimensional vector spaces. The setup algorithm produces a pair of dual bases (B, B^*) on DPVS. And a part of B (say $\hat{B}$) is used as a public key and the corresponding part of B^* (say $\hat{B}^*$) is used as a secret key or trapdoor. Therefore, the basis, B - $\hat{B}$, is information theoretically concealed against an adversary, i.e., even an infinite power adversary has no idea on which basis is selected as B - B^* when B^* is published. It establishes a framework for information theoretical tricks in the public-key setting. Since the l-th level secret key is consist of a key for decryption and a delegated key, users can give the delegated key to others by their own secret key. So if Alice can decrypt files F_A, as he gives the delegated key to Bob, Bob can decrypt files F_B ($F_A \supseteq F_B$).

VI. Revocation

In the PE scheme, user's secret key and the token are associated with the predicate while ciphertext is linked to the attribute. The dynamic change of attribute and predicate makes the cost and difficulties of secret key revocation increased. The revocation of secret key is drawing attention.

FH13, proposed controllable privacy preserving search by Fan and Huang, makes it possible for the secret key owner to control the lifetime of the delegation. Except SSW09, Blundo *et al*. [26] proposed another symmetric scheme which works in groups of a prime order. This scheme is based on BIP09 [25], which is more efficient than SSW09 for that is performed in the groups of a composed order. Controllable privacy preserving search [29] scheme has two new functions. One is revocable delegated search which makes it possible for the secret key owner to control the lifetime of the delegation. In order to control the lifetime period of delegated search privilege, the secret key owner randomly chooses a time restrictive token. The other one is un-decryptable delegated search. If the secret key owner attaches this functionality to the predicated token, the delegated person will be unable to decrypt the returned matched ciphertexts even though he has the delegated privilege of search. Though it is more efficient for its revocable delegated search, un-decryptable delegated search, and using prime order groups, it cannot support complex queries for this scheme is not based on the inner product. Although FH13 makes it possible for the secret key owner to control the lifetime of the delegation, it must decide the lifetime at the beginning which is not suitable for dynamic changes. Therefore, revocable secret key method is still worthy of researching.

VII. Comparison

Table I compares some typical inner-product predicate encryption schemes introduced in Sections 4. $|G|$ and $|G_T|$ represent size of an element of G and that of G_T. PH, AH, PK, SK, CT, GSD, DSP, C3DH and eDDH stand for predicate-hiding, attribute-hiding, master public key, secret key, ciphertext, general subgroup decision[44],

decisional subspace problem[30], composite 3-party (decisional) Diffie-Hellman[26], and extended decisional Diffie-Hellman [21], respectively.

TABLE I: COMPARISON WITH PE SCHEMES

	Setting	Security		Order of G	Assumption	PK size	SK size	CT size
KSW08	Public key	Selective	Fully-AH	Composite	2 variants of GSD	$O(n)\|G\|$	$(2n+1)\|G\|$	$(2n+1)\|G\|+\|G_T\|$
SSW09	Secret key	Selective	PH & Weakly-AH	Composite	A variant of GSD, C3DH, DLIN	---	$(2n+2)\|G\|$	$(2n+2)\|G\|+\|G_T\|$
OT09	Public key	Selective	Weakly-AH	Prime	2 variants of DSP	$O(n^2)\|G\|$	$(n+3)\|G\|$	$(n+3)\|G\|+\|G_T\|$
LOT10	Public key	Adaptive	Weakly-AH	Prime	n-eDDH	$O(n^2)\|G\|$	$(2n+3)\|G\|$	$(2n+3)\|G\|+\|G_T\|$
OT10	Public key	Adaptive	Weakly-AH	Prime	DLIN	$O(n^2)\|G\|$	$(3n+2)\|G\|$	$(3n+2)\|G\|+\|G_T\|$
OT12 (basic)	Public key	Adaptive	Fully-AH	Prime	DLIN	$O(n^2)\|G\|$	$(4n+2)\|G\|$	$(4n+2)\|G\|+\|G_T\|$
OT12 (variant)	Public key	Adaptive	Fully-AH	Prime	DLIN	$O(n^2)\|G\|$	$11\|G\|$	$(5n+1)\|G\|+\|G_T\|$
Proposed IPE-CC(basic)	Public key	Adaptive	PH & Fully-AH	Prime	DLIN	$O(n^2)\|G\|$	$6n\|G\|$	$6n\|G\|+\|G_T\|$
Proposed IPE-CC(variant)	Public key	Adaptive	PH & Fully-AH	Prime	DLIN	$O(n)\|G\|$	$6n\|G\|$	$6n\|G\|+\|G_T\|$
Proposed SIPE	Secret key	Adaptive	PH & Fully-AH	Prime	DLIN	---	$6n\|G\|$	$6n\|G\|+\|G_T\|$

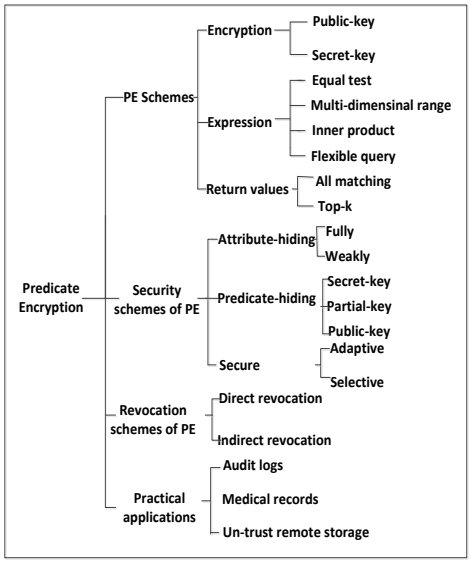

Fig. 1. Research of PE schemes

VIII. CONCLUSION AND FUTURE WORK

As showed in Fig. 1, the main research contents of PE focus on encryption schemes, the effect of support search statement, the security of PE, the practical applications and so on. Some research on predicate encryption mechanism for a more comprehensive presentation and discussion is also shown in Fig. 1. As more data is saved in the cloud server, user' awareness of sensitive data security and personal privacy is growing. How to retrieve efficiently, accurately and safely of ciphertext in the cloud server will be the direction we continue to explore. The researchers believe that further research is mainly focused on solving the following problems:

- Supporting for more flexible query like relational operators (>, <, ==, etc.). Though inner product acquires some achievement, it is still not perfect in expression in PE. In the ensuing period of time, proposing a PE algorithm which supports relational operators well remains a hot point.
- PE scheme is based on either composite-order groups or prime-order. It is difficult to apply to the scenarios with huge users and massive data. Only the design of efficient PE algorithm is the fundamental way to speed up the efficiency of today's search.
- The security of all known predicate encryption schemes is based on many different and often complex assumptions. Taking into account these assumptions, PE schemes have different security levels. Although it is hardly to realize predicate-hiding in public-key predicate encryption schemes, we hope a public-key PE scheme could be proven fully secure under a simple assumption in a standard model for everyone even if with the help of a third party.
- Previous works have realized that cloud returns all messages without integration. In order to avoid users processing every file in order to find one matching their interests, we should return top-k matching files in a ranked order regarding to certain relevant criteria. (e.g., keyword weight or keyword frequency). This method can make users find their interesting files fast and save user's decryption cost and bandwidth. However, we may take attention to support for multiple keywords and conjunctive keywords and avoid cloud learning more messages about the relevancy of keywords.
- As ciphertext is related to the attribute and user's secret key and token are associated with the predicate, it is hard to revoke the secret key. By controlling of the lifetime of the delegation, it has to connect to data owner and decide the lifetime at the beginning, it

takes a lot to communicate between data users and cloud about the secret key updating time, what's worse, it is hard to revoke secret key dynamically. Therefore, revocable secret key search is still worthy for researching.

ACKNOWLEDGMENT

This work was supported in part from Deep exploration instrumentation and equipment development (SinoProbe-09-01-03).

REFERENCES

[1] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Proc. 2nd International Conference Applied Cryptography and Network Security*, Berlin, 2004, pp. 31−45.

[2] C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. IEEE 30th International Conference Distributed Computing Systems*, Genoa, 2010, pp. 253−262.

[3] J. Li, Q. Wang, C. Wang, M. Cao, K. Ren, and W. J. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. IEEE INFOCOM Mini-Conf. IEEE Computer Society*, San Diego, 2010, pp. 1−5.

[4] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. on Parallel and Distributed Systems*, vol. 25, pp. 222-233, Jan 2014.

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in *Proc. 13th ACM Conf. on Computer and Communications Security*, New York, 2006, pp. 79−88.

[6] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Proc. 8th Conference on Theory of Cryptography*, Providence, 2011, pp. 253-273.

[7] S. Agrawal, D. M Freeman, and V. Vaikuntanathan, "Functional encryption for inner product predicates from learning with errors," in *Proc. 17th International Conference on the Theory and Application of Cryptology and Information Security*, Seoul, 2011, pp. 21-40.

[8] E. Shi, J. Bethencourt, T. H. H. Chan, D. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, 2007, pp. 350-364.

[9] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proc. IEEE 31st Int'l Conf. Distributed Computing Systems*, Minneapolis, 2011, pp. 383-392.

[10] B. Zhu, B. Zhu, and K. Ren, "PEKSrand: Providing predicate privacy in public-key encryption with keyword search," in *Proc. IEEE International Conference on Communications*, Kyoto, 2011, pp. 1-6.

[11] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. 21st Annual International Cryptology Conference*, Santa Barbara, 2001, pp. 213-229.

[12] D. Boneh, Di. G Crescenzo, R. Ostrovsky, and G. Persiano, "Public-key encryption with keyword search," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques*, Interlaken, 2004, pp. 506-522.

[13] D. Boneh and X. Boyen, "Efficient selective-ID identity based encryption without random oracles," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques*, Interlaken, 2004, pp. 223-238.

[14] B. Waters, "Efficient identity-based encryption without random oracles," in *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, 2005, pp. 114-127.

[15] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in *Proc. 26th Annual International Cryptology Conference*, Santa Barbara, 2006, pp. 290-307.

[16] C. Clifford, "An identity based encryption scheme based on quadratic residues," in *Proc. 8th IMA International Conference*, Cirencester, 2001, pp. 360–363.

[17] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic*, Aarhus, 2005, pp. 457-473.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine grained access control of encrypted data," in *Proc. 13th ACM Conference on Computer and Communications Security*, Alexandria, 2006, pp. 89-98.

[19] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. 14th ACM Conference on Computer and Communications Security*, Alexandria, 2007, pp. 195-203.

[20] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, 2007, pp. 321-334.

[21] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory of Cryptography Conference*, Amsterdam, 2007, pp. 535-554.

[22] E. Shi and B. Waters, "Delegating capability in predicate encryption systems," in *Proc. 35th International Colloquium on Automata*, Languages and Programming, Reykjavik, 2008, pp. 560-578.

[23] V. Iovino and G. Persiano, "Hidden-vector encryption with groups of prime order," in *Proc. 2nd International Conference on Pairing-Based Cryptography*, Egham, 2008, pp. 75-88.

[24] J. H. Park, "Efficient hidden vector encryption for conjunctive queries on encrypted data," *IEEE Trans. on Knowledge and Data Engineering*, vol. 23, no. 10, pp. 1483-1497, Oct. 2011.

[25] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Proc. 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Istanbul, 2008, pp. 146-162.

[26] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Proc. 6th Theory of Cryptography Conference*, San Francisco, 2009, pp. 457-473.

[27] M. Yoshino, N. Kunihiro, K. Naganuma, and H. Sato, "Symmetric inner-product predicate encryption based on three groups," in *Proc. 6th International Conference on Provable Security*, Chengdu, 2012, pp. 215-234.

[28] C. Blundo, V. Iovino, and G. Persiano, "Private-key hidden vector encryption with key confidentiality," in *Proc. 8th International Conference on Cryptology and Network Security*, Kanazawa, 2009, pp. 259-277.

[29] C. I. Fan and S. Y. Huang, "Controllable privacy preserving search based on symmetric predicate encryption in cloud storage," in *Proc. 3rd International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Beijing, 2011, pp. 269-273.

[30] T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," in *Proc. 15th International Conference on the Theory and Application of Cryptology and Information Security*, Tokyo, 2009, pp. 214-231.

[31] A. Lewko, T. Okamoto, A. Sahai, T. Katsuyuki, and W. Brent, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. 29th Annual*

International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, 2010, pp. 62-91.
[32] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Proc. 30th Annual International Cryptology Conference*, Santa Barbara, 2010, pp. 191-208.
[33] T. Okamoto and K. Takashima, "Adaptively attribute-hiding (hierarchical) inner product encryption," in *Proc. 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cambridge, 2012, pp. 591-608.
[34] Y. Kawai and K. Takashima, "Predicate-and attribute-hiding inner product encryption in a public key setting," in *Proc. 6th International Conference on Pairing-Based Cryptography*, Beijing, 2014, pp. 113-130.
[35] D. Boneh and B. Waters, "A fully collusion resistant broadcast, trace, and revoke system," in *Proc. 13th ACM Conference on Computer and Communications Security*, Alexandria, 2006, pp. 211-220.
[36] R. Wei and D. Ye, "Delegate predicate encryption and its application to anonymous authentication," in *Proc. 4th International Symposium on ACM Symposium on Information, Computer and Communications Security*, Sydney, 2009, pp. 372-375.
[37] D. Sun, C. Boyd, and J. M. G. Nieto, "Predicate encryption for multi-inner-products," *Security and Communication Networks*, vol. 6, no. 3, pp. 325–339, 2013.
[38] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in *Proc. 8th International Workshop on Theory and Practice in Public Key Cryptography*, Les Diablerets, 2005, pp. 380-397.
[39] J. Katz and A. Yerukhimovich, "On black-box constructions of predicate encryption from trapdoor permutations," in *Proc. 15th International Conference on the Theory and Application of Cryptology and Information Security*, Tokyo, 2009, pp. 197-213.
[40] B. Dan and W. Brent, "A fully collusion resistant broadcast trace and revoke system with public traceability," in *Proc. 13th ACM Conference on Computer and Communications Security*, Alexandria, 2006, pp. 211-220.
[41] C. I. Fan and S. Y. Huang, "Timed-release predicate en-cryption and its extensions in cloud computing," *Journal of Internet Technology*, vol. 15, no. 3, pp. 413-426, 2014.
[42] C. Blundo, V. Iovino, and G. Persiano, "Predicate encryption with partial public keys," in *Proc. 9th International Conference on Cryptology and Network Security*, Kuala Lumpur, 2010, pp. 298-313.
[43] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Proc. 24th Annual International Cryptology Conference*, Santa Barbara, 2004, pp. 443-459.
[44] M. Bellare, B. Waters, and S. Yilek, "Identity-based encryption secure against selective opening attack," in *Proc. 8th Theory of Cryptography Conference*, Providence in Yuval Ishai, 2011, pp. 235-252.

Liang Hu had his BEng on Computer Systems Organization in 1993 and his PhD on Computer Software and Theory in 1999. He is a Professor and PhD supervisor of College of Computer Science and Technology, Jilin University, China. His main research interest includes network security and distributed computing.

Yuanmo Zhang was born in Jilin, China in 1989. She received the B.S. degree from the College of Computer Science and Technology, Jilin University in 2012, and she is currently working toward the M.S. degree at Jilin University. Her research interest includes computer networks and information security.

Hongtu Li was born in Siping of Jilin, China on Mar. 17 1984. Now he is the teacher of the College of Computer Science and Technology, Jilin University, Changchun, China. He received the Ph.D. degree in computer structure from Jilin University in 2012. His current research interests focus on network security and cryptology.

Yicheng Yu was born in Jilin, China in 1989. He received the B.S. degree from the College of Computer Science and Technology, Jilin University in 2012, and he is currently working toward the M.S. degree at Jilin University. His research interest includes computer networks and cloud computing security.

Fangming Wu received his B.S. degree from the PLA Information Engineering University in 2007. He is currently pursuing in the College of Computer Science and Technology, Jilin University. His research interest is the communication of WSN, computer networks and information security.

Jianfeng Chu* was born in 1978, Ph.D., Now he is the teacher of the College of Computer Science and Technology, Jilin University, Changchun, China. He received the Ph.D. degree in computer structure from Jilin University in 2009. His current research interests focus on information security and cryptology.

