entropy

MDPI

Article

Public Key Encryption with Keyword Search in Cloud: A Survey

Yunhong Zhou [1], Na Li [1], Yanmei Tian [1], Dezhi An [2] and Licheng Wang [1,*]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; hongdixin@126.com (Y.Z.); 15011177558@163.com (N.L.); tianym0213@163.com (Y.T.)

[2] School of Cyber Security, Gansu University of Political Science and Law, Lanzhou 730070, China; adz6199@gsli.edu.cn

* Correspondence: wanglc@bupt.edu.cn

Received: 5 March 2020; Accepted: 5 April 2020; Published: 8 April 2020

Abstract: With the popularization of cloud computing, many business and individuals prefer to outsource their data to cloud in encrypted form to protect data confidentiality. However, how to search over encrypted data becomes a concern for users. To address this issue, searchable encryption is a novel cryptographic primitive that enables user to search queries over encrypted data stored on an untrusted server while guaranteeing the privacy of the data. Public key encryption with keyword search (PEKS) has received a lot of attention as an important branch. In this paper, we focus on the development of PEKS in cloud by providing a comprehensive research survey. From a technological viewpoint, the existing PEKS schemes can be classified into several variants: PEKS based on public key infrastructure, PEKS based on identity-based encryption, PEKS based on attribute-based encryption, PEKS based on predicate encryption, PEKS based on certificateless encryption, and PEKS supporting proxy re-encryption. Moreover, we propose some potential applications and valuable future research directions in PEKS.

Keywords: cloud computing; searchable encryption; search query; public key encryption with keyword search; data privacy

1. Introduction

In recent years, with the speedy development of computation and communication, cloud computing [1] is becoming more and more popular, and cloud storage services are becoming more and more mature, such as Baidu Cloud, Amazon simple storage service, Widows Azure, Google Cloud, etc. [2]. As a new type of network storage technology, cloud storage saves user data on the cloud server. Cloud server provider performs corresponding operations on the user data through the online network environment, and charges a fee for use of the hardware resources and service time by the user.

Cloud storage services [3] are widely used in different applications due to its many advantages as follows. It includes data scalability, data accessibility, data shareability, and consistent back up of massive data. Many advantages of cloud storage services improve the quality of the user experience [4] and service, which users are allowed to remotely access data in cloud using any devices from anywhere and at any time instead of having to use fixed machines. Cloud storage is adopted by a large number of individuals and companies in order to reduce the heavy burden of local storage and the management costs.

Despite cloud storage services provide users with a lot of convenience, there are still remaining enormous issues and challenges. When the user outsources their sensitive data to the cloud storage, the transmitted data is vulnerable to intrusion [5,6] by illegal entities especially under critical

infrastructures. Meanwhile, the user lost their capabilities to control the data effectively. By accessing the data, the cloud server and the illegal user can try to acquire the information contained in the data, and the privacy security problem of the user is faced with great challenges. In order to protect the security of sensitive data, a straightforward method is used to encrypt the user data before outsourcing it to the cloud [7]. However, when the user wants to search for related files containing a certain keyword, how to process and search on the encrypted data becomes an intractable problem. In the past, there are two methods to solve it. One is to download all encrypted data to the local and then decryption query. This method needs to download a large number of files that are unneeded, which wastes network overhead and requires a lot of computational cost for decryption. This way is not feasible in practice. Another extreme method is user sends the secret key to the cloud server to decrypt the query, but the cloud server is not fully trusted.

In order to better solve the above problems, Goldreich [8] first proposed the ciphertext search mechanism in 1996, but the client and the server needed a large number of interactions, which is not efficient in practical use. In 2000, Song [9] first provided a practical searchable encryption technology, which became a milestone in the development of searchable encryption. Searchable encryption (SE) is a new technology that a user has the capability to selectively search on encrypted data outsourced to the cloud server. From the perspective of cryptography, SE technology mainly includes two types, one is symmetric searchable encryption (SSE), and the other is public key encryption with keyword search (PEKS). At present, an number of SSE schemes [10–14] have been proposed due to high efficiency. However, users have to securely share key for data encryption in SSE, and it is not suitable for multi-user data sharing scenarios. PEKS solved the problem of secret key distribution yielded by SSE. Compared with SSE, PEKS has a broader application prospect. Although there are many survey studies over searchable encryption [15–19], there are few complete survey researches on PEKS. In this article, we seek to complement these existing surveys by presenting a comprehensive study for PEKS schemes.

The remainder of this paper is organized as follows. Section 2 introduces the general framework of PEKS. Section 3 provides a comprehensive taxonomy of existing PEKS schemes in terms of technology view. Section 4 discusses the application area of PEKS. Finally, Section 5 summarizes the paper and provides valuable research directions in this area for future.

2. General Framework of PEKS

In 2004, Boneh et al. [20] first proposed the framework of PEKS. PEKS is mainly based on public key encryption algorithms. The PEKS consists of three entities: data sender, data receiver, and cloud server provider. A data sender encrypts their documents and index with the public key and uploads to the remote server provider. A data receiver who has gained corresponding private key can perform the search operation. He generates the trapdoor he wants to search the keyword with the private key and sends it to the server. After receiving trapdoor, the server provider enable test whether a given ciphertext contains the search keyword without knowing the plaintext message of the encrypted data and the keyword. Then, the server provider returns the query results to the data receiver. Finally, the receiver can decrypt the ciphertext which the server sends. PEKS is more suitable for use in some insecure networks. It does not require the encryption party and the decryption party to negotiate the key in advance. Figure 1 shows the model of PEKS system.

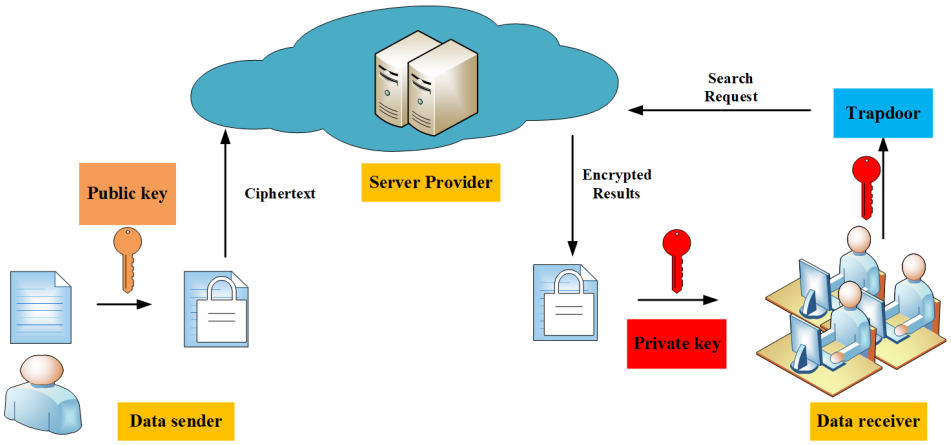

Figure 1. Model of public key encryption with keyword search (PEKS) system.

2.1. Algorithm Description

A general PEKS scheme mainly includes four probabilistic polynomial-time algorithms [20].

- `KeyGen(`λ`)`: a key generation algorithm run by the **data receiver**. It takes a security parameter λ as input, and outputs public key pk and private key sk .
- `PEKS(`pk`,`W`)`: an encryption algorithm run by the **data sender**. It takes public key pk and a keyword W as inputs, outputs a keyword ciphertext S of W.
- `Trapdoor(`sk`,`W`)`: a keyword trapdoor generation run by the **data receiver**. It takes his/her own private key sk and a query keyword W as inputs, and outputs the trapdoor T_W for the query keyword W.
- `Test(`pk`,`S`,`T_W`)`: a test algorithm run by the **server provider**. It takes public key pk, a ciphertext S of keyword W', and a trapdoor T_W of query keyword W as inputs, if $W = W'$, this algorithm outputs "yes"; otherwise, it outputs "no".

2.2. Security Model

Boneh et al. [20] introduced the first PEKS construction which was based on Boneh and Franklin's work on IBE [21,22]. They defined the security of PEKS scheme which was indistinguishably secure against an adaptive chosen keyword attack (**IND-CKA**) [20].

We give the following game to definition IND-CKA security between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

- **Setup:** The challenger $\mathcal{C}$ runs the key generation algorithm to generate public key pk and private key sk. It sends pk to the adversary $\mathcal{A}$ and keeps private key sk.
- **Phase 1:** The adversary $\mathcal{A}$ can adaptively ask the challenger $\mathcal{C}$ for trapdoors corresponding to keywords of its choice.
- **Challenge:** The adversary $\mathcal{A}$ sends the challenger $\mathcal{C}$ two keywords W_0, W_1 on which it wishes to be challenged. Note that W_0, W_1 have not been requested before in Phase 1; otherwise, it is a trivial attack that the adversary always wins the game. The challenger $\mathcal{C}$ randomly picks a bit $b \in \{0,1\}$ and gives the adversary $\mathcal{A}$ ciphertext $C = PEKS(pk, W_b)$.
- **Phase 2:** The adversary $\mathcal{A}$ can continue to ask for more trapdoors like in Phase 1 for any keyword of his choice except for the W_0,W_1.
- **Guess:** The adversary $\mathcal{A}$ outputs its guess of b' and wins the game if $b = b'$.

The advantage of an adversary $\mathcal{A}$ in winning the game is

$$Adv_{\mathcal{A}}(s) = |Pr[b = b'] - 1/2| \quad (1)$$

In a short, a PEKS scheme is IND-CKA security if an adversary $\mathcal{A}$ has a negligible advantage to win the game.

2.3. Attack Model

We investigate the attack model of the PEKS. Although a user can outsource a set of encrypted data to the server provider while maintaining the ability to selectively search over them, most of the existing PEKS schemes are vulnerable to the keyword guessing attack, in addition, there is file injection attack.

2.3.1. Keyword Guessing Attack

Keyword guessing attack (KG) is an important issue for public key searchable encryption. Byun et al. [23] first launched the keyword guessing attack on some PEKS schemes. This attack is originated from the low-entropy property of the keyword space. By performing this attack, an attacker is able to correctly guess the keyword encoded in a given keyword trapdoor. In KG attack, the attacker can be classified into two different types of adversaries, namely, the outside attacker and the inside attacker [24].

- **Outside attacker:** the outside attack is a malicious entity who has no relationship with the server provider and can eavesdrop on a public channel between the server provider and the receiver. Baek et al. [25] first constructed a secure channel free PEKS scheme. If the trapdoor is transmitted over public channel, the outsider attacker can gain the keyword ciphertexts but can not excute the text algorithm.
- **Inside attacker:** the inside attacker usually refers to the malicious server provider. The malicious server can obtain the encrypted keywords from any sender. Meanwhile, it can gain the information about the trapdoor from the receiver. Even worse, if the PEKS scheme is secure channel-free, the malicious server can perform the test algorithm to verify the relation between an encrypted keyword and a trapdoor by using its private key. Obviously it is very difficult to resist inside attacker.

2.3.2. File Injection Attack

File injection attack (FI) is another important issue for public key searchable encryption. Zhang et al. [26] first observed the file injection attack in searchable encryption. A malicious server can obtain query information of the keywords by injecting a set of injected files to the client. File injection attack is devastating for query privacy due to leaking access pattern, it is easy for attacker to recover a significate amount of sensitive data. Therefore, it is imperative to design efficient PEKS schemes to mitigate this critical attack.

2.4. Search Functionalities of PEKS

The PEKS is a promising technique in cloud, and it has attracted considerable attentions from cryptographic researchers. In such a case, it is difficult to search over the encrypted data. PEKS is working hard to support information query of various functions in ciphertext like plaintext information retrieval. Up to now, PEKS can support to use various keyword searches, such as single keyword search, conjunctive keyword search, fuzzy keyword search, multi-keyword search, ranking keyword search, verifiable keyword search, similarity keyword search, semantic keyword search, range query, subset query, etc.

3. Taxonomy of Existing PEKS Schemes

Since the PEKS was proposed, we have discovered that researchers working in the domain of PEKS use search functionality for the classification of the existing schemes (see, e.g., in [16]). The goal of this section is to give a comprehensive taxonomy of the current PEKS schemes and provide a general overview of the conducted research. In this paper, existing PEKS schemes mainly can be broadly classified into six variants from the technology view, such as PEKS on public key

infrastructure, PEKS based on identity-based encryption, PEKS based on attribute-based encryption, PEKS based on predicate encryption, PEKS based on certificateless encryption, and PEKS supporting proxy re-encryption.

3.1. PEKS Based on Public Key Infrastructure (PEKS-PKI)

To resolve secret key management and distribution in symmetric searchable encryption, the PEKS was proposed. At current, most PEKS schemes have been established on PKI with the certificate management. The sender has a authority to check the legitimacy of a receiver's public key and then encrypts the data and keywords under the receiver's public key; thereafter, it uploads encrypted data to the server provider. The receiver generates the trapdoor under its private key for providing a capability to the server provider to test if a given encrypted data contains the keyword it would like to search. The public key is originated from the third authority namely the public key infrastructure.

3.1.1. PEKS-PKI Research and Progress

Boneh et al. [20] proposed the framework of PEKS based on public key infrastructure using bilinear pairing. Each user in this scheme can be allowed to create searchable content with the receiver's public key, but only the private key holder can generate a keyword trapdoor to query. Their scheme needs a secure channel to transform the search trapdoor; however, it is expensive to build the secure channel. Baek et al. [25] proposed a PEKS scheme removed the limit for a secure channel. Their construction requires a server public key and private key, and only the server chosen by the sender can search. It was proved security in the random oracle model under the BDH problems. Next, Rhee et al. [27] proposed a new PEKS scheme based on PKI, which enhanced Baek's model [25] and allowed an attacker to obtain the relation between ciphertexts and a trapdoor.

Park et al. [28] proposed the first PEKS scheme supporting conjunctive keyword search by public key encryption and presented the two constructions based on DBDH problem and DBDHI problem. However, their schemes need amounts of communication and storage overhead. Hwang and Lee [29] improved Park et al. [28] schemes and proposed a new concept called multiuser public key encryption with conjunctive keyword search to save the communication and storage space. Subsequently, Zhang et al. [30] proposed a PEKS scheme supporting conjunctive with subset keyword search and improved Park et al. [28] work that can only support conjunctive keyword search. Lv et al. [31] proposed an expressive and secure PEKS scheme supporting conjunctive, disjunctive and negation search operations based on composite order groups. It was secure in the standard model and can be extended to support range search.

Tang and Chen [32] proposed a PEKS scheme named public key encryption with registered keyword search, which allowed a sender to build searchable content only for the keywords that the sender registered keyword with a receiver first. Their construction was more robust against an offline keyword guessing attack. Hu et al. [33] proposed a decryptable searchable public key encryption with a designated tester construction enhanced security against keyword guessing attacks, and it can decrypt the keyword from keyword ciphertext.

Fang et al. [34] provided a formal model of SCF-PEKS secure against chosen keyword attacks, ciphertext attacks, and keyword guessing attacks. They proposed a secure channel free PEKS scheme without random oracle under the well known assumptions. Next, Shao and Yang [35] enhanced the security model against keyword guessing attacks based on the work of Fang et al. [34] and solved the problem that the attacker is the malicious server. Recently, Lu et al. [24] demonstrated Shao and Yang's work [35] cannot resist inside keyword guessing attacks and proposed a new improvement of Fang et al. [34] scheme resisted against inside and outside attackers.

Zhang et al. [36] proposed a novel PEKS framework supporting verifiable keyword search and provided two concrete constructions which can maintain the strong security property and have a high efficiency for search over outsourced encrypted data. Huang and Li [37] proposed a public key authenticated encryption with keyword search scheme, in which the data sender not only encrypted

keyword but also authenticated it. Their scheme was secure against the inside keyword guessing attack. Recently, Wu et al. [38] proposed a new PEKS construction-based Diffie–Hellman shared secret key to achieve strong security resistance of the file-injected attack and inside keyword guessing attack in existing PEKS systems.

3.1.2. Summary

In Table 1, we compare the several representative PEKS-PKI schemes. Table 2 shows the efficiency of compared PEKS-PKI schemes, and the notations in the Table 3. As usual, the cost of the general cryptographic hash operations are ignored. Although the works in [37,38] fully consider the outside and inside attacks, the method in [37] is more efficient. Therefore, the method in [37] is more suitable for cloud services than other existing PEKS-PKI schemes. The PEKS-PKI scheme needs a certificate to generate a validate public key to prevent public key replacement attacks. However, this will inevitably bring heavy certificate management problems, such as generation, distributions, storage, verification, and revocation.

Table 1. Comparison of several PEKS-PKI schemes.

Scheme	Search Functionality	Security		Attack Model				
		Definition	Assumption	ROM	SCF	OKG	IKG	FI
Boneh et al. [20]	Single	IND-CKA	BDH	✓				
Park et al. [28]-I	Conjunctive	IND-CKA	DBDH	✓				
Park et al. [28]-II	Conjunctive	IND-CKA	DBDHI	✓				
Hwang et al. [29]	Conjunctive	IND-CKA	DLDH	✓				
Baek et al. [25]	Single	IND-CKA	BDH	✓	✓			
Rhee et al. [27]	Single	IND-CKA	BDH,BDHI	✓	✓			
Tang et al. [32]	Single	IND-CKA	DBDH	✓	✓	✓		
Zhang et al. [30]	Conjunctive, subset	TU,AC	DDHI	-		✓		
Hu et al. [33]	Single	IND-CKA	DLP,HDH		✓	✓		
Shao et al. [35]	Single	IND-KGAs	-	-	✓	✓		
Huang et al. [37]	Single	SS	DBDH,mDLIN	✓		✓	✓	✓
Wu et al. [38]	Single	IND-CKA	DBDH,CDH			✓	✓	✓

ROM denotes random oracle model. (ROM [39] is an ideal oracle for modelling a cryptographic hash function.) SCF denotes secure channel free. OKG denotes outside keyword guessing attack. IKG denotes inside keyword guessing attack and FI denotes file injection attack. BDH refers to Bilinear Diffie–Hellman assumption. DBDH refers to Decisional Bilinear Diffie–Hellman assumption. DBDHI refers to Decisional Bilinear Diffie–Hellman Inversion assumption. DLDH refers to Decision Linear Diffie–Hellman assumption. BDHI refers to Bilinear Diffie–Hellman Inversion assumption. DDHI refers to Decisional Diffie–Hellman Inversion assumption. DLP refers to Discrete Logarithm Problem. HDH refers to Hash Diffie–Hellman assumption. mDLIN refers to modified Decision Linear assumption. CDH refers to Computational Diffie–Hellman assumption. We write SS for sematic security, TU for trapdoor unforgetable, AC for anonymous of the ciphertext, and IND-KGAs for IND-KGA-server.

Table 2. Efficiency of the compared PEKS-PKI schemes.

Scheme	Computation Cost			Communication Cost	
	Encrypt	Trapdoor	Test	Ciphertext Size	Trapdoor Size
Boneh et al. [20]	$2T_{exp}+T_{\hat{e}}$	T_{exp}	$T_{\hat{e}}$	$log\|G_1\|+\|\lambda\|$	$log\|G_1\|$
Park et al. [28]-I	$(l+2)T_{exp}+lT_{\hat{e}}$	T_{exp}	$T_{exp}+T_{\hat{e}}$	$2log\|G_1\|+llog\|G_t\|$	$log\|G_1\|+log\|Z_p\|$
Park et al. [28]-II	$(3l+2)T_{exp}$	$2T_{exp}$	$T_{exp}+2T_{\hat{e}}$	$(2l+3)log\|G_1\|$	$2log\|G_1\|+log\|Z_p\|$
Hwang et al. [29]	$(2l+2)T_{exp}$	$3T_{exp}$	$3T_{\hat{e}}$	$(l+2)log\|G_1\|$	$3log\|G_1\|$
Baek et al. [25]	$2T_{exp}+2T_{\hat{e}}$	T_{exp}	$T_{exp}+T_{\hat{e}}$	$log\|G_1\|+\|\lambda\|$	$log\|G_1\|$
Rhee et al. [27]	$2T_{exp}+9T_{\hat{e}}$	T_{exp}	$T_{exp}+T_{\hat{e}}$	$log\|G_1\|+\|\lambda\|$	$log\|G_1\|$
Tang et al. [32]	$3T_{exp}+T_{\hat{e}}$	T_{exp}	$T_{\hat{e}}$	$log\|G_1\|+log\|G_t\|$	$log\|G_1\|$
Zhang et al. [30]	$(2l+2)T_{exp}+T_{\hat{e}}$	$3lT_{exp}$	$(2+2l)T_{exp}+(2l+1)T_{\hat{e}}$	$(l+1)log\|G_1\|+$ $(l+2)log\|G_t\|+log\|Z_p\|$	$(l+2)log\|G_1\|+log\|G_t\|$
Hu et al. [33]	$2T_{exp}+3T_{\hat{e}}$	$3T_{exp}$	$2T_{exp}+T_{\hat{e}}$	$log\|G_1\|+log\|Z_p\|$	$2log\|G_t\|$
Shao et al. [35]	$9T_{exp}+3T_{\hat{e}}$	$2T_{exp}$	$5T_{exp}+4T_{\hat{e}}$	$5log\|G_1\|+3log\|G_t\|$	$3log\|G_1\|$
Huang et al. [37]	$3T_{exp}$	$T_{exp}+T_{\hat{e}}$	$2T_{\hat{e}}$	$2log\|G_1\|$	$log\|G_t\|$
Wu et al. [38]	$5T_{exp}+T_{\hat{e}}$	$5T_{exp}$	$6T_{exp}+3T_{\hat{e}}$	$2log\|G_1\|+log\|G_t\|$	$2log\|G_1\|$

Table 3. Notations for PEKS-PKI schemes.

Notation	Description
T_{exp}	The time of a modular exponentiation
$T_{\hat{e}}$	The time of a bilinear pairing
$\|G_1\|$	The number of elements in G_1
$\|G_t\|$	The number of elements in G_t
$\|Z_p\|$	The number of elements in Z_p
λ	The security parameter
$\|\lambda\|$	The bit length of security parameter
l	The number of the keywords

3.2. PEKS Based on Identity-Based Encryption (PEKS-IBE)

The identity-based encryption (IBE) was firstly proposed by Shamir [40] in 1984, which simplifies the management of public key and certificate in traditional public key encryption based on PKI. In an identity-based encryption system, a user's public key can be an arbitrary string such as email address, IP address, telephone number, ID, etc. The private key generation (PKG) can generate the private key according to the user's authentication and request. Suppose Alice wants to send a message to Bob, the communication step of the two parties using identity-based encryption is shown in Figure 2. In a PEKS-IBE scheme, a data sender uploads ciphertexts to a server provider, then the receiver contacts PKG using its identity to get a corresponding private key and generates a search trapdoor using its private key to send the server provider. Finally, the server provider conducts a keyword search.

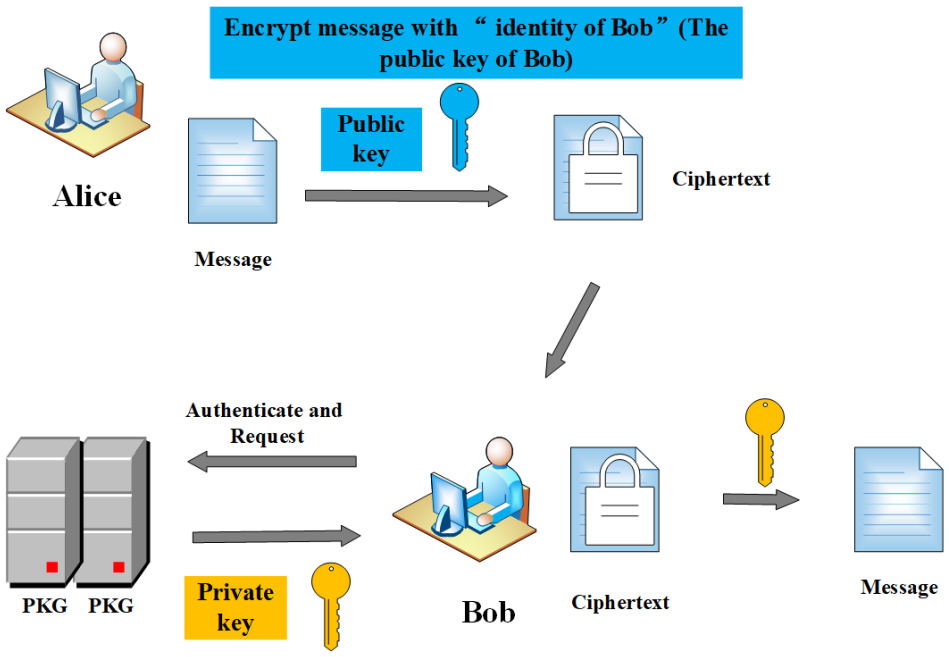

Figure 2. The communication between Alice and Bob.

3.2.1. PEKS-IBE Research and Progress

Boneh et al. [20] provided the first PEKS scheme based on IBE, in which the keyword acted as the identity. Crescenzo and Saraswat [41] proposed the first PEKS scheme without bilinear maps transformed by the Cocks' identity-based encryption scheme [42] based on Jacobi symbols and the quadratic residual problem. Their scheme is security in the random oracle model, but it needs secure channels and high storages. Next, Tian et al. [43] improved computation and communication, and proposed an ID-based encryption with keyword search scheme from bilinear pairings which can remove secure channel and be proved secure in random oracle under the appropriate computational

assumptions. Subsequently, Camenisch et al. [44] presented an extended notion of PEKS based on blind and anonymous identity-based encryption to improve security. In their scheme, a user is able to obtain a search token from the secret key holder without revealing the keyword.

Abdalla et al. [45] proposed a generic PEKS construction supporting conjunctive keyword from an anonymous IBE scheme and a hierarchical IBE scheme. The server provider performs test algorithm only in a specific time interval, so it cannot use the search trapdoor in the past or future outside the time interval. Next, Khader [46] proposed a PEKS scheme based on k-resilient IBE and presented two construction for conjunctive keyword search and no secure channel to transform trapdoor. Their scheme is secure in the standard oracle under the DDH assumption. However, it needs complex computation and communication space. Subsequently, Wu et al. [47] proposed a novel PEKS secure channel-free scheme with a designated server based on identity-based encryption resisted offline keyword guessing attacks. Recently, Lu et al. [48] pointed out that Wu et al. [47] fails in achieving the ciphertext indistinguishability, and proposed a designated server identity-based encryption scheme supporting conjunctive keyword search removed secure channel and resisted the offline keyword guessing attack.

Said [49] provided a generic transformation from an anonymous IBE to an anonymous (n, t)-IBE in order to implement a novel threshold PEKS deployed on a public key encrypted database. Emura et al. [50] proposed a PEKS scheme supporting keyword revocable based on partially-anonymous identity-based encryption. In their scheme, a keyword trapdoor is generated even if the keyword is revoked, which can resist the security risks caused by the keyword trapdoor. Recently, Wang et al. [51] proposed a secure channel-free identity-based searchable encryption scheme in a peer-to-peer group, which allowed multiple users to share in a peer-to-peer group and search the private data in the cloud.

3.2.2. Summary

In Table 4, we compare several representative PEKS-IBE schemes. Table 5 shows the efficiency of the compared PEKS-IBE schemes, and the notations in the Table 6. Although the methods in [47,48] can resist the outside keyword guessing attack, the method in [47] has more efficiency. Therefore, the method in [47] is more suitable for cloud services than other existing PEKS-IBE schemes. The PEKS-IBE scheme overcomes the certificate management problem based on PKI; however, the current PEKS-IBE schemes have the key escrow issues because a completely trusted private key generator can know all users' private key.

Table 4. Comparison of several PEKS-IBE schemes.

Scheme	Search Functionality	Security				Attack Model		
		Definition	Assumption	ROM	SCF	OKG	IKG	FI
Boneh et al. [20]	Single	IND-CKA	BDH	✓				
Khader et al. [46]	conjunctive	IND-CKA	DDH		✓			
Crescenzo et al. [41]	Single	IND-CKA	QIP	✓				
Tian et al. [43]	Single	IND-CKA	DLP	✓	✓			
Wu et al. [47]	Conjunctive	IND-CKA	BDH,CDH	✓	✓	✓		
Wang et al. [51]	Multi-user	IND-CKA	DBDH	✓	✓	✓		
Lu et al. [48]	Conjunctive	IND-CKA	DBDH,CDH	✓	✓	✓		

BDH refers to Bilinear Diffie–Hellman assumption. DBDH refers to Decisional Bilinear Diffie–Hellman assumption. DDH refers to Decisional Diffie–Hellman assumption. QIP refers to Quadratic Indistinguishability Problem. DLP refers to Discrete Logarithm Problem. CDH refers to Computational Diffie–Hellman assumption.

Table 5. Efficiency of the compared PEKS-IBE schemes.

Scheme	Computation Cost			Communication Cost	
	Encrypt	Trapdoor	Test	Ciphertext Size	Trapdoor Size
Boneh et al. [20]	$2T_{exp} + T_{\hat{e}}$	T_{exp}	$T_{\hat{e}}$	$log\|G_1\| + \|\lambda\|$	$log\|G_1\|$
Khader et al. [46]	$(3l\lambda + 3l + 3)T_{exp}$	-	$5T_{exp}$	$(3 + 2l)log\|G_1\|$	$(4 + l)log\|Z_p\|$
Crescenzo et al. [41]	$4\lambda J$	$4\lambda T_{exp}$	$4\lambda(J + T_{exp})$	$4\|\lambda\|log\|Z_p\|$	$4\|\lambda\|log\|Z_p\|$
Tian et al. [43]	$3T_{exp}$	T_{exp}	$2T_{\hat{e}}$	$3log\|G_1\|$	$log\|G_1\|$
Wu et al. [47]	$(l + 2)T_{exp} + T_{\hat{e}}$	$2T_{exp}$	$2T_{exp} + 2T_{\hat{e}}$	$(l + 1)log\|G_1\| + \|\lambda\|$	$2log\|G_1\|$
Wang et al. [51]	$(5 + n^2)T_{exp} + T_{\hat{e}}$	$5T_{exp} + T_{\hat{e}}$	$nT_{exp} + 4T_{\hat{e}}$	$(n + 3)log\|G_1\| + log\|G_t\|$	$3log\|G_1\|$
Lu et al. [48]	$(l + 4)T_{exp} + T_{\hat{e}}$	$3T_{exp} + T_{\hat{e}}$	$3T_{exp} + 3T_{\hat{e}}$	$(l + 3)log\|G_1\| + 2log\|Z_p\|$	$2log\|G_1\| + log\|Z_p\|$

Table 6. Notations for PEKS-IBE schemes.

Notation	Description
T_{exp}	The time of a modular exponentiation
$T_{\hat{e}}$	The time of a bilinear pairing
$\|G_1\|$	The number of elements in G_1
$\|G_t\|$	The number of elements in G_t
$\|Z_p\|$	The number of elements in Z_p
λ	The security parameter
$\|\lambda\|$	The bit length of security parameter
l	The number of the keywords
J	The Jacobi symbol
n	The number of the users share the data

3.3. PEKS Based on Attribute-Based Encryption (PEKS-ABE)

Attribute-based encryption (ABE) was originally proposed by Sahai and Waters [52] in 2005, and is also known as fuzzy identity-based encryption. It regards the identity as a series of attribute sets; attributes are the information elements of the user. We compare traditional public key encryption (PKE) and attribute-based encryption in a multi-user setting. From Figure 3, in PKE, the sender encrypts a document using each receiver's public key to generate multiple ciphertexts, and each receiver decrypts ciphertexts by using its private key. However, in ABE the sender only needs to formulate an access policy that can be satisfied by multiple users, and then encrypts a document once to generate the only ciphertext. The ciphertext and the user's private key are associated with the attributes. When user's attributes match the corresponding access policies, he can decrypt ciphertexts. According to whether the private key or ciphertext is associated with the access control policy, the attribute-based encryption can be further divided into the key-policy attribute-based encryption (KP-ABE) and the ciphertext-policy attribute-based encryption (CP-ABE). In the PEKS-ABE scheme, a data sender allows to grant its search capabilities to receivers by applying an access control policy over the outsourced ciphertexts.

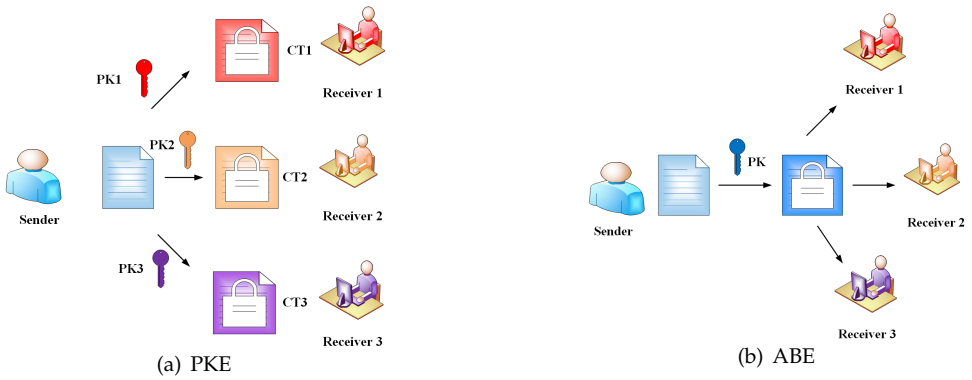

Figure 3. Comparison between public key encryption (PKE) and attribute-based encryption (ABE).

3.3.1. PEKS-ABE Research and Progress

Zhao et al. [53] first considered using the attribute-based signature to realize multi-user keyword search for secure data sharing with fine-grained access control. Han et al. [54] presented a notion based on weak anonymous ABE and considered a transformation ABE into PEKS-ABE. They constructed a concrete PEKS-ABE scheme based on KP-ABE in multi-user setting, but the efficiency was not high. Subsequently, Wang et al. [55] first combined PEKS with CP-ABE and proposed a ciphertext-policy attributed-based encryption scheme to support keyword search functionality. This scheme allows the data sender to control his data access policy, and only legitimate data receivers who meet the policy can retrieve the keyword and decrypt the ciphertext.

Zheng et al. [56] introduced a verifiable attribute-based keyword search scheme, in which the data user can control the search and use of the encrypted data and verify whether the server provider conducts correct keyword search. However, their scheme needs a secure channel and the verification cost is expensive. Liu et al. [57] improved Zheng et al.'s [56] work and proposed a relatively efficient PEKS-ABE scheme based on key policy attribute keyword search removed a secure channel. Subsequently, Li et al. [58] devised a fine-grained access control system to decrease the computation resources in PEKS-ABE, and the server provider can perform partial decryption operations without learning any information related to plaintext.

Yang et al. [59] provided a PEKS-ABE scheme based on bilinear pairing to support fine-grained access control and semantic keyword search in the multi-user settings that enable convenient user revocation mechanism, but it cannot consider traceability. Next, Ning et al. [60] proposed a PEKS-ABE scheme based on CP-ABE supporting traceability by embedding their identity information in the secret keys to prevent dishonest data users from leaking their secret keys to others. Subsequently, Sun et al. [61] proposed a PEKS-ABE scheme supporting efficient user revocation allowed multiple senders to encrypt and outsource the data to the server provider independently. The receivers are able to generate their own search abilities without relying on an trusted authority that is always online. Recently, Zhu et al. [62] proposed a PEKS-ABE scheme based on ciphertext policy attribute-based encryption in order to support with access control over ciphertext and fuzzy keyword search.

Miao et al. [63] proposed a basic attribute-based keyword search over hierarchical data scheme by using CP-ABE technique. Because the basic scheme cannot satisfy the desirable requirements in cloud, they provided two improved schemes supporting multi-keyword search and user revocation. However, they can not consider attack models. Next, Cao et al. [64] enhanced the security that can resist the collision attacks of the server provider and the data user. They proposed a PKES-ABE scheme based on blinded CP-ABE in cloud, which blinded the access attributes of the users. The server provider not only performs the keyword search but also conducts pre-decryption operation. In shared multi-owner setting, Miao et al. [65] recently proposed a privacy preserving PEKS-ABE system by using CP-ABE technology with hidden access policy achieved selective security in the generic bilinear group model, and it can resist the offline keyword guessing attack.

3.3.2. Summary

In Table 7, we compare the several representative PEKS-ABE schemes. Table 8 shows the efficiency of compared PEKS-ABE schemes, and the notations in the Table 9. The method in [64] has relatively high efficiency, but it cannot resist the keyword guessing attack. Therefore, the method in [65] is more suitable for cloud services than other existing PEKS-ABE schemes. The attribute-based encryption method is widely adopted in PEKS due to its efficient data sharing and searching ability. However, the PEKS-ABE scheme also brings the key escrow problem simultaneously because all users' private keys are known by the PKG.

Table 7. Comparison of several PEKS-ABE schemes.

Scheme	Search Functionality	Security				Attack Model		
		Definition	Assumption	ROM	SCF	OKG	IKG	FI
Wang et al. [55]	Single	SeS	q-DBDH	-		✓	✓	
Zheng et al. [56]-I	Verifiable	IND-CKA	DLIN	✓				
Zheng et al. [56]-II	Verifiable	IND-CKA	DLIN					
Sun et al. [61]	Verifiable	IND-CKA	DBDH					
Li et al. [58]	Single	CPA	DBDH	✓			✓	
Miao et al. [63]	Multi-keyword	IND-CKA	DBDH	✓				
Cao et al. [64]	Single	IND-CKA	BDH	✓				
Miao et al. [65]	Single	SeS	DBDH			✓		

BDH refers to Bilinear Diffie–Hellman assumption. DBDH refers to Decisional Bilinear Diffie–Hellman assumption. q-DBDH refers to q-parallel Decisional Bilinear Diffie–Hellman assumption. DLIN refers to Decisional Linear assumption. We write SeS for selective security and CPA for choose plaintext attack.

Table 8. Efficiency of the compared PEKS-ABE schemes.

Scheme	Computation Cost			Communication Cost	
	Encrypt	Trapdoor	Test	Ciphertext Size	Trapdoor Size
Wang et al. [55]	$(3N+2)T_{exp}+T_{\hat{e}}$	$(S+2)T_{exp}$	$NT_{exp}+(2N+1)T_{\hat{e}}$	$(2N+1)log\|G_1\|+log\|G_t\|$	$(S+2)log\|G_1\|$
Zheng et al. [56]-I	$(S+4)T_{exp}$	$(2N+2)T_{exp}$	$ST_{exp}+(2S+2)T_{\hat{e}}$	$(S+3)log\|G_1\|$	$(2N+2)log\|G_1\|$
Zheng et al. [56]-II	$(2N+4)T_{exp}$	$(2S+4)T_{exp}$	$NT_{exp}+(2N+3)T_{\hat{e}}$	$(2N+3)log\|G_1\|$	$(2S+3)log\|G_1\|$
Li et al. [58]	$(2+S)T_{exp}+T_{\hat{e}}$	$(3+3N)T_{exp}$	$2T_{exp}$	$(S+1)log\|G_1\|+log\|G_t\|$	$4log\|G_1\|$
Sun et al. [61]	$(N+2)T_{exp}$	$(2N+1)T_{exp}$	$T_{exp}+(N+1)T_{\hat{e}}$	$(2N+1)log\|G_1\|+log\|G_t\|$	$(2N+1)log\|G_1\|+log\|Z_p\|$
Miao et al. [63]	$(2N+1)T_{exp}$	$(2S+4)T_{exp}$	$T_{exp}+(2S+3)T_{\hat{e}}$	$log\|G_1\|+2log\|G_t\|$	$(2S+3)log\|G_1\|$
Cao et al. [64]	$(3+S)T_{exp}+T_{\hat{e}}$	$2T_{exp}$	$4T_{\hat{e}}$	$(3+N)log\|G_1\|$	$2log\|G_1\|$
Miao et al. [65]	$(2+2N)T_{exp}+T_{\hat{e}}$	$(2N+1)T_{exp}$	$T_{exp}+(2N+1)T_{\hat{e}}$	$(N+1)log\|G_1\|+log\|G_t\|$ $+log\|Z_p\|$	$(2N+1)log\|G_1\|+log\|Z_p\|$

Table 9. Notations for PEKS-ABE schemes.

Notation	Description
T_{exp}	The time of a modular exponentiation
$T_{\hat{e}}$	The time of a bilinear pairing
$\|G_1\|$	The number of elements in G_1
$\|G_t\|$	The number of elements in G_t
$\|Z_p\|$	The number of elements in Z_p
S	The number of a data user's attribute
N	The number of attributes that are involved in a data owner's access control policy

3.4. PEKS Based on Predicate Encryption (PEKS-PE)

The notion of predicate encryption was first proposed by Katz et al. [66] in 2008. Predicate encryption is a new public key encryption allowing users to search on ciphertext without a private key corresponding to a public key, and it can be achievable to fine-grained access control on encrypted data. Secret keys are associated with predicates and ciphertexts are associated with attributes in the predicate encryption system. According to access control, predicate encryption can achieve high flexibility supporting attribute-hiding and payload-hiding. Therefore, predicate encryption might be applied to search over encrypted data. In a PEKS-PE scheme, the server provider can perform the test algorithm to match ciphertexts with the trapdoor supplied on particular predicates. Finally, the server provider returns the query results to the receiver without revealing any information to the server. Corresponding to a predicate, the receiver owning the secret key can decrypt the resulting ciphertexts associated with attributes and recover the message.

3.4.1. PEKS-PE Research and Progress

Blundo et al. [67] proposed a predicate encryption scheme with partial public key by the need for predicate privacy in PEKS. They defined token security to ensure the privacy of attributes from a token. To reduce the communication cost between the receiver and sender, Zhu et al. [68] provided a extend PEKS scheme based on predicate encryption to support predicate privacy, and it based on the idea of randomization without requiring interaction between the receiver and sender. Next, Katz et al. [69] proposed a PEKS-PE scheme supporting disjunctive keyword search, and provided the approach of converting a predicate encryption scheme into a PEKS. Zhang et al. [70] proposed a PEKS-PE scheme, which can not only support disjunctive keyword search, but also conjunctive keyword search over encrypted data. Kim et al. [71] proposed an efficient predicate encryption with constant pairing computations supporting the evaluations of polynomials, disjunctions, conjunctions, CNF formulas, and threshold. Recently, Zhang et al. [72] proposed an efficient PEKS-PE scheme to support conjunctive and disjunctive keyword search, and it needs less time and storage consumption.

Gay et al. [73] proposed a lattice-based PEKS-PE scheme for multidimensional range and multidimensional subset queries, and it was selectively secure and weakly attribute-hiding under the standard learning with errors assumption. Recently, Zhang et al. [74] constructed a PEKS to support semantic multi-keyword search through applying an efficient predicate encryption. In their scheme, the semantic index and query keyword set can be converted into an attribute and a predict vector by utilizing a keyword conversion method.

3.4.2. Summary

In Table 10, we compare the several representative PEKS-PE schemes. Table 11 shows the efficiency of compared PEKS-PE schemes, and the notations in the Table 12. The scheme of Zhang et al. [74] can resist the keyword guessing attack and has relatively strong efficiency. It is more applicable to the cloud environment. Predicate encryption is a new paradigm that covering identity-based encryption, attribute-based encryption, and hidden vector encryption. Attribute information is public in attribute-based encryption, whereas attribute information is hidden in predicate encryption.

Table 10. Comparison of several PEKS-PE schemes.

Scheme	Search Functionality	Security				Attack Model		
		Definition	Assumption	ROM	SCF	OKG	IKG	FI
Zhu et al. [68]	Single	PP,SP	ECDLP	-				
Zhang et al. [70]	Disjunctive,conjunctive	CPA	-	-				
Zhang et al. [74]	Semantic	CPA,IND-CKA	-	-		✓		
Zhang et al. [72]	Conjunctive,disjunctive	IND-CKA	BDHI,DLIN	✓				

ECDLP refers to Elliptic Curve Discrete Logarithm Problem, BDHI refers to Bilinear Diffie–Hellman Inversion assumption, DLIN refers to Decision Linear assumption. We write PP for predicate privacy, SP for statistics privacy and CPA for choose plaintext attack.

Table 11. Efficiency of the compared PEKS-PE schemes.

Scheme	Computation Cost			Communication Cost	
	Encrypt	Trapdoor	Test	Ciphertext Size	Trapdoor Size
Zhu et al. [68]	$2T_{exp} + T_{\hat{e}}$	T_{exp}	$T_{\hat{e}}$	$log\|G_1\| + \|\lambda\|$	$log\|G_1\|$
Zhang et al. [70]	$(4l^2 + 3l)T_{exp}$	$(4l + 2)T_{exp}$	$2l(2l + 1)T_{\hat{e}}$	$(4l^2 + 2l)log\|G_1\| + log\|G_t\|$	$(4l + 2)log\|G_1\|$
Zhang et al. [74]	$(2l + 4)T_{exp}$	$(l + 4)T_{exp}$	$(l + 1)T_{exp} + 3T_{\hat{e}}$	$(l + 3)log\|G_1\|$	$3log\|G_t\| + (l + 1)log\|Z_p\|$
Zhang et al. [72]	$(3l^2 + 4l + 1)T_{exp}$	$(2l + 2)T_{exp}$	$2l(l + 1)T_{\hat{e}}$	$(2l^2 + 4l)log\|G_1\| + log\|G_t\|$	$(2l + 2)log\|G_1\| + log\|Z_p\|$

Table 12. Notations for PEKS-PE schemes.

Notation	Description
T_{exp}	The time of a modular exponentiation
$T_{\hat{e}}$	The time of a bilinear pairing
$\|G_1\|$	The number of elements in G_1
$\|G_t\|$	The number of elements in G_t
$\|Z_p\|$	The number of elements in Z_p
l	The number of the keywords
$\|\lambda\|$	The bit length of security parameter

3.5. PEKS Based on Certificateless Encryption (PEKS-CLE)

AI-Riyami and Paterson [75] first proposed certificateless encryption in 2003, which is a new type of public key cryptosystem based on the identity-based public key cryptosystem. The private key in certificateless public key encryption is no longer independently generated by the PKG, but is jointly generated by the PKG and the user. In a PEKS-CLE scheme, a data sender encrypts both a keyword and data using a receiver's public key and identity, then it sends encrypted data to the server provider. The receiver first obtains a partial private key from the PKG. A complete private key combines a partial private key and a secret value chosen by the receiver. Thereafter, the receiver generates the search trapdoor using its complete private key to send the server provider in order to conduct search keyword. Certificateless encryption overcomes the problem of key escrow in identity-based encryption because the secret key is only known by the receiver and the PKG does not know it.

3.5.1. PEKS-CLE Research and Progress

Peng et al. [76] first introduced certificateless encryption into PEKS and constructed an secure channel free PEKS-CLE scheme, and it was secure against chosen keyword attack and keyword guessing attack. Subsequently, Wu et al. [77] demonstrated that the certificateless searchable public key encryption scheme of Peng et al. [76] cannot resist a malicious PKG attack and an offline keyword guessing attack.

Zheng et al. [78] integrated the certificateless cryptography with keyword search and proposed a PEKS-CLE scheme that was provably secure in the standard model under the decisional linear assumption, but it cannot consider attack model. Next, Ma et al. [79] proposed a new PEKS-CLE scheme supporting multiple keyword search for industrial Internet of Things deployment removed secure channel, and it was proved security in the random oracle model against a malicious PKG attack and public key replacement attack. Subsequently, Ma et al. [80] proposed an efficient PEKS-CLE scheme for mobile health care system to remove the key management problem and key escrow problem, and it can resist the chosen keyword and keyword guessing attack in the random oracle model.

Islam et al. [81] proposed a PEKS-CLE with designated server scheme that was secure under the bilinear Diffie–Hellman assumption and computational Diffie–Hellman assumption. Next, Wu et al. [82] enhanced the security resisted various types of attacks, and they constructed a new certificateless public key authenticated encryption with keyword search utilizing designated tester for cloud-assisted mIoT. Recently, Lu et al. [83] proposed a pairing-free PEKS-CLE scheme to improve the efficiency problems caused by the use of bilinear pairing, and this scheme was formally proved its security under the complexity assumption of the CDH problem in the random oracle model.

3.5.2. Summary

In Table 13, we compare the several representative PEKS-CLE schemes. Table 14 shows the efficiency of compared PEKS-CLE schemes, and the notations in the Table 15. The method in [83] has greater efficiency but it cannot resist the keyword guessing attack; the method in [82] can resist all kinds of attacks. Therefore, the method in [82] is more suitable for cloud services than other existing PEKS-CLE schemes. The PEKS-CLE scheme not only overcomes certificate management

problems based on PKI, but also resolves the key escrow problem based on IBE and ABE. In other words, certificateless encryption lies between conventional public key encryption and identity-based encryption, but preserves the certificateless advantages.

Table 13. Comparison of several PEKS-CLE schemes.

Scheme	Search Functionality	Security				Attack Model		
		Definition	Assumption	ROM	SCF	OKG	IKG	FI
Peng et al. [76]	Single	IND-CKA	BDH	✓	✓	✓		
Zheng et al. [78]	Single	CI	DLIN					
Islam et al. [81]	Single	CI,DI	CDH,BDH	-	✓	✓		
Ma et al. [80]	Single	IND-CKA	BDH	✓		✓		
Wu et al. [82]	Single	SS	CBDH	✓	✓	✓	✓	
Lu et al. [83]	Single	IND-CKA	CDH	✓				

BDH refers to Bilinear Diffie–Hellman assumption. DLIN refers to Decisional Linear assumption. CDH refers to Computational Diffie–Hellman assumption. CBDH refers to Computational Bilinear Diffie–Hellman assumption. We write CI for ciphertext indistinguishability, DI for trapdoor indistinguishability, and SS for semantically secure.

Table 14. Efficiency of the compared PEKS-CLE schemes.

Scheme	Computation Cost			Communication Cost	
	Encrypt	Trapdoor	Test	Ciphertext Size	Trapdoor Size
Peng et al. [76]	$4T_{exp} + 7T_{\hat{e}}$	$4T_{exp}$	$2T_{exp} + T_{\hat{e}}$	$log\|G_1\| + log\|Z_p\|$	$3log\|G_1\|$
Zheng et al. [78]	$5T_{exp}$	$8T_{exp}$	$4T_{\hat{e}}$	$4log\|G_1\|$	$4log\|G_1\|$
Islam et al. [81]	$5T_{exp}$	T_{exp}	$3T_{exp} + 2T_{\hat{e}}$	$3log\|G_1\|$	$log\|G_1\|$
Ma et al. [80]	$5T_{exp} + 3T_{\hat{e}}$	$2T_{exp}$	$3T_{exp} + T_{\hat{e}}$	$log\|G_1\| + log\|Z_p\|$	$log\|G_1\|$
Wu et al. [82]	$10T_{exp}$	$11T_{exp} + T_{\hat{e}}$	$5T_{exp} + 2T_{\hat{e}}$	$2log\|G_1\|$	$2log\|G_1\| + log\|G_t\|$
Lu et al. [83]	$3T_{exp}$	T_{exp}	T_{exp}	$2log\|G_t\|$	$log\|Z_p\|$

Table 15. Notations for PEKS-CLE schemes.

Notation	Description
T_{exp}	The time of a modular exponentiation
$T_{\hat{e}}$	The time of a bilinear pairing
$\|G_1\|$	The number of elements in G_1
$\|G_t\|$	The number of elements in G_t
$\|Z_p\|$	The number of elements in Z_p

3.6. PEKS Supporting Proxy Re-Encryption (PEKS-PRE)

Proxy re-encryption (PRE) was first proposed by Blaze, Bleumer, and Strauss [84] in Eurocrypt'98. In a proxy re-encryption mechanism, a semi-trusted third party called a proxy is responsible for the ciphertext conversion. In some situations, a sender that acts as a delegator is allowed to delegate their search right to a delegatee through re-encrypting the ciphertext, without revealing his own private key. The ciphertext conversion requires to generate re-encryption key using delegator's private key and delegatee's public key. In this process, the proxy cannot obtain relevant plaintext information. Suppose Alice is a delegator and Bob is a delegatee, the proxy re-encryption model is shown in Figure 4. PEKS-PRE is a cryptographic primitive for searching on encrypted information without decrypting it while supporting a proxy re-encryption system. The server provider plays role in a proxy that could convert the encrypted data into a re-encrypted ciphertext searched by the delegatee. A data sender allows the authorization of the search ability to the other receiver. The proxy cloud server is given a trapdoor which it can use to test whether or not a ciphertext contains a keyword without knowing anything else about the contents of data and keyword.

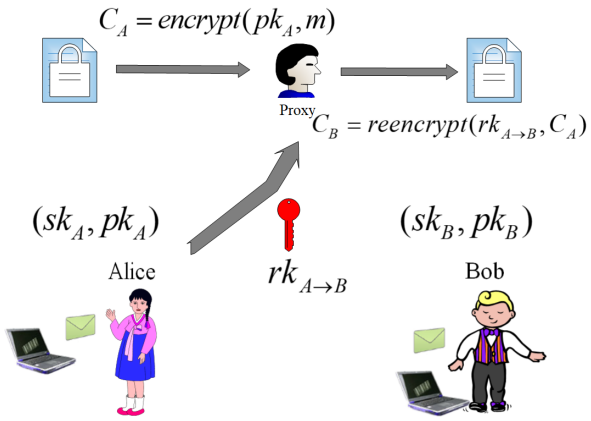

Figure 4. PRE model.

3.6.1. PEKS-PRE Research and Progress

Shao et al. [85] first integrated proxy-encryption and PEKS, which a data user allowed to delegate keyword search ability to another user. They provided a bidirectional PEKS-PRE scheme that was secure in the random oracle model. Yao et al. [86] proposed a novel PEKS-PRE scheme with a designated tester that extended original PEKS model by adding algorithms of re-encrytion key generation and re-encryption of keyword ciphertext to satisfy the requirements of applications. Subsequently, Zhong et at. [87] proposed PEKS from anonymous conditional proxy re-encryption ensured the privacy and security of ciphertext.

Wang et al. [88] proposed a PEKS-PRE scheme supporting conjunctive keyword search constrained single-hop unidirectional proxy re-encryption under the bilinear pairing, and it was secure in the random oracle model. Guo et al. [89] enhanced the security, and they proposed a new searchable bidirectional proxy re-encryption with a designer server without resorting to random oracle model supported verifiable correctness of the keyword results. Next, Yang et al. [90] proposed a PEKS-PRE scheme with a designated tester for electronic health record system supporting secure conjunctive keyword search. The patients enable delegate partial access rights to others to operate search functions over their records in a limited time period. Recently, Yang et al. [91] proposed a novel semantic keyword searchable proxy re-encryption scheme resisted quantum attack, and this scheme was proven secure in the standard model under the learning with errors hardness problem.

Shi et al. [92] combined attribute-based encryption and proxy re-encryption with keyword search and provided two construction schemes based on KP-ABE and CP-ABE. The data user is allowed to delegate the keyword search ability to multiple users. Next, Chen et al. [93] proposed a restricted proxy re-encryption with keyword search scheme for fine-grained data access control to restrict the capability of the proxy cloud server. Subsequently, Hong et al. [94] proposed an attribute-based proxy re-encryption scheme with keyword search, and it fully took advantage of the attribute-based re-encryption and keyword search supporting flexible data access control among users in data sharing scenario. Recently, Chen et al. [95] also combined proxy re-encryption with the attribute-keyword search and provided an attribute-based keyword search with proxy re-encryption scheme that achieved the functions of the data search and fine-grained access control.

3.6.2. Summary

In Table 16, we compare the several representative PEKS-PRE schemes. Table 17 shows the efficiency of the compared PEKS-PRE schemes, and the notations in the Table 18. The methods in [89,90] can resist the keyword guessing attack. However, the method in [90] has more efficiency applying to conjunctive keyword search in cloud. Therefore, the method in [90] is more suitable for

cloud services than other existing PEKS-PRE schemes. Proxy re-encryption provides convenience on encrypted data search improved the functions of revocation, update and deletion of ciphertext data.

Table 16. Comparison of several PEKS-PRE schemes.

Scheme	Search Functionality	Security		Attack Model			
		Definition	Assumption	ROM	SCF	OKG	CA
Yau et al. [86]-I	Single	IND-CKA	BDH	✓			
Yau et al. [86]-II	Single	IND-CKA	BDH	✓	✓		
Wang et al. [88]	Conjunctive	wIND-CCA	q-BDHI	✓			
Guo et al. [89]	Verifiable	IND-CKA	QDBDH,DBDH,HDH		✓	✓	
Yang et al. [90]	Conjunctive	IND-CKA	DBDH,DDH		✓	✓	
Chen et al. [95]	Single	IND-CKA	q-BDHE	✓			✓

BDH refers to Bilinear Diffie–Hellman assumption. DBDH refers to Decisional Bilinear Diffie–Hellman assumption. q-BDHI refers to q-Bilinear Diffie–Hellman Inversion assumption. QDBDH refers to Quotient Decisional Bilinear Diffie–Hellman assumption. HDH refers to Hash Diffie–Hellman assumption. DDH refers to Decisional Diffie–Hellman assumption. q-BDHE refers to q-parallel Bilinear Diffie–Hellman Exponent assumption. CA denotes Collusion Attack, namely the proxy colluded with the delegate. We write wIND-CCA for weakly IND-CCA(chosen ciphertext attack).

Table 17. Efficiency of the compared PEKS-PRE schemes.

Scheme	Computation Cost			Communication Cost	
	Encrypt	Trapdoor	Test	Ciphertext Size	Trapdoor Size
Yau et al. [86]-I	$2T_{exp} + T_{\hat{e}}$	T_{exp}	$T_{\hat{e}}$	$log\|G_1\| + \|\lambda\|$	$log\|G_1\|$
Yau et al. [86]-II	$3T_{exp} + T_{\hat{e}}$	$3T_{exp}$	$2T_{exp} + T_{\hat{e}}$	$log\|G_1\| + \|\lambda\|$	$2log\|G_1\|$
Wang et al. [88]	$(4l+3)T_{exp}$	T_{exp}	$2T_{\hat{e}}$	$(2l+4)log\|G_1\|$	$3log\|G_1\|$
Guo et al. [89]	$3T_{exp} + T_{\hat{e}}$	$3T_{exp}$	$2T_{exp} + T_{\hat{e}}$	$log\|G_1\| + log\|G_t\|$	$2log\|G_1\|$
Yang et al. [90]	$(l+4)T_{exp}$	$(l+1)T_{exp}$	$(l+2)T_{\hat{e}}$	$(l+3)log\|G_1\|$	$(l+3)log\|G_1\|$
Chen et al. [95]	$(2N+4)T_{exp}$	$(S+4)T_{exp}$	$NT_{exp} + (2N+1)T_{\hat{e}}$	$(N+3)log\|G_1\|$	$(S+2)log\|G_1\|$

Table 18. Notations for PEKS-PRE schemes.

Notation	Description
T_{exp}	The time of a modular exponentiation
$T_{\hat{e}}$	The time of a bilinear pairing
$\|G_1\|$	The number of elements in G_1
$\|G_t\|$	The number of elements in G_t
$\|Z_p\|$	The number of elements in Z_p
l	The number of the keywords
$\|\lambda\|$	The bit length of security parameter
S	The number of a data user's attribute
N	The number of attributes that are involved in a data owner's access control policy

4. Application Area

PEKS is a hot research topic of searchable encryption that has great potential for use in many applications where confidential data is outsourced to the third party server provider without affecting the usage of the data stored in the cloud. This section mainly provides some applications of PEKS, such as e-mail routing, health care, and smart grid etc.

4.1. E-mail Routing

Boneh et al. [20] proposed the first PEKS scheme in the e-mail routing scenario. Suppose Bob sends an e-mail containing certain keyword to Alice through an untrusted mail server. It is required that the server cannot obtain the email content and related keyword information, but it needs to route the email to the corresponding terminal device of Alice according to the keyword information. For example, when the keyword information is "urgent", the server forwards the message to Alice's

mobile phone. When the keyword information is "lunch", the server forwards the message to Alice's laptop. Alice is able to read the message on whatever device he/she wants. To protect the privacy of emails, the sender encrypts e-mail with receiver's public key. PEKS might be achievable to search over encrypted email.

4.2. Health Care

For medical practices, an increasing number of health care providers tend to deploy the electronic medical record storage and application services into a third party cloud in order to reduce the cost of huge data storage and maintenance. When medical data are stored on a cloud server that is not fully trusted, patient privacy and security becomes critical issues. To protect the confidentiality of sensitive data, the health care providers prefers to encrypt the medical data before uploading to the cloud. In electronic health care systems, the details of a patient are utilized by the doctors for diagnosis of the disease shared with other doctors. PEKS can provide searching the encrypted data and sharing with authorized user, there are many researches for health care [96–100].

4.3. Smart Grid

In the power system world, smart grid is a new revolution using the IoT technology that it increasingly attracts the attention of many organizations. The smart grid system can not only measure and collect energy usage data through sensors and smart meters, but also store and utilize energy usage data through a powerful cloud computing platform. As the power information uploads to the cloud, security, and privacy of these data become vital. A professional controller prefers to encrypt the sensitive information before outsourcing to cloud, which makes PEKS applicable to smart grid system [101–104].

5. Conclusions and Future Directions

PEKS has been researched for years and has made great progress in recent years. Nevertheless, there are still many drawbacks or problems to be resolved. Various PEKS researches focus on three main influencing factors, namely, query expressiveness, efficiency, and security.

- **Query expressiveness.** The existing PEKS schemes have been improved in order to make them more practical for deployment in different application devices, which not only can support single keyword search but also support conjunctive keyword search, fuzzy keyword search, semantic keyword search, rank search, range search, and subset search. However, this needs to be achieved at the cost of efficiency and security.
- **Efficiency.** A large number of existing PEKS schemes are constructed based on bilinear pairings that are inefficient due to a lot of computational overhead. How to construct a scheme without bilinear map to improve the efficiency of PEKS becomes an important issue that needs to be solved. At the same time, existing multi-user PEKS schemes are not practical in real-world applications and cannot scale well for large constructions. Thus, one of the goal of PEKS schemes should reduce the computational complexity.
- **Security.** Most of existing PEKS schemes are proved security under the random model. However, the random model has its limitations. Security can be proven under the random model, but it may not be secure in practical applications. Although there are some schemes that can be proved security under the standard model, they are usually inefficient and require a large amount of computation costs and space storage. In addition, most PEKS schemes are vulnerable to keyword guessing attacks and file injection attacks.

The research of PEKS still requires to concentrate on improving the query expressiveness and the trade-off between the efficiency and security at the same time. With recent research progress, the future development direction of public key searchable encryption includes the following aspects.

- **Multi-Source Data.** With the rapid development of the social network, multimedia information has grown at an explosive speed, especially multimedia information represented by videos and images. To protect the data privacy, the data information containing sensitive content needs to be encrypted before uploading to the cloud. However, how to query the required video or image on encrypted data has become an intractable problem. In the future, we can consider how to apply PEKS to deal with such problems.
- **Lattice-Based PEKS.** With the growth of the quantum computing, traditional cryptographic algorithms based on hardness assumption will face a huge challenge that can easily be attacked by the quantum computer. Consequently, it is necessary to design a cryptographic algorithm that can resist quantum attack. Lattice-based cryptosystems are becoming increasingly popular in the post-quantum algorithms due to their efficiency and conceptual simplicity. Some researches have evolved [105–108], and it is urgent to construct an efficient and secure lattice-based PEKS scheme in the future.
- **Blockchain-Based PEKS.** As an emerging integrated technology, the blockchain plays an important role in new technological innovation, and nowadays it is increasing attracting attention from all walks of life. Specially, the data requires to be encrypt so as to achieve confidentiality before storing on the blockchain. However, it becomes difficult to conduct keyword search over the blockchain. PEKS can help the effective utilization of the encrypted data while protecting the data privacy. Several studies [109–111] have been proposed for PEKS based on blockchain. For future progress in this field, more research efforts are required.

Author Contributions: Conceptualization, Y.Z.; methodology, Y.Z.; software, N.L.; validation, L.W. and D.A.; formal analysis, Y.Z. and N.L.; investigation, Y.Z., N.L., and Y.T; data curation, Y.Z., N.L., and Y.T.; writing—original draft preparation, Y.Z. and N.L.; writing—review and editing, Y.Z., N.L. , Y.T., and D.A.; visualization, Y.T.; supervision, L.W. and D.A.; project administration, L.W. and D.A.; funding acquisition, L.W. and D.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Shandong Provincial Key Research and Development Program of China (2018CXGC0701), the National Natural Science Foundation of China (NSFC) (No. 61972050), the Team Project of Collaborative Innovation in Universities of Gansu Province (No.2017-16), and the Major Project of Gansu University of Political Science and Law(No.2016XZD12).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PEKS	Public key encryption with keyword search
PEKS-PKI	Public key encryption with keyword search based on public key infrastructure
PEKS-IBE	Public key encryption with keyword search based on identity-based encryption
PEKS-ABE	Public key encryption with keyword search based on attribute-based encryption
PEKS-PE	Public key encryption with keyword search based on predicate encryption
PEKS-CLE	Public key encryption with keyword search based on certificateless encryption
PEKS-PRE	Public key encryption with keyword search supporting proxy re-encryption
ROM	Random oracle model
SCF	Secure channel free
OKG	Outside keyword guessing attack
IKG	Inside keyword guessing attack
FI	File injection attack

References

1. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
2. Buyya, R.; Yeo, C.S.; Venugopal, S.; Broberg, J.; Brandic, I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Gener. Comput. Syst.* **2009**, *25*, 599–616.
3. Konstantopoulos, M.; Diamantopoulos, P.; Chondros, N.; Roussopoulos, M. Distributed Personal Cloud Storage without Third Parties. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 2434–2448.
4. Aloqaily, M.; Kantarci, B.; Mouftah, H.T. A generalized framework for quality of experience (QoE)-based provisioning in a vehicular cloud. In Proceedings of the 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, QC, Canada, 4–7 October 2015; pp. 1–5.
5. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, *90*, 101842.
6. Otoum, S.; Kantarci, B.; Mouftah, H.T. Detection of known and unknown intrusive sensor behavior in critical applications. *Ieee Sens. Lett.* **2017**, *1*, 1–4.
7. Kamara, S.; Lauter, K. Cryptographic cloud storage. In Proceedings of the 2010 International Conference on Financial Cryptography and Data Security, Tenerife, Canary Islands, Spain, 25–28 January 2010; pp. 136–149.
8. Goldreich, O.; Ostrovsky, R. Software protection and simulation on oblivious RAMs. *J. ACM (JACM)* **1996**, *43*, 431–473.
9. Song, D.X.; Wagner, D.; Perrig, A. Practical techniques for searches on encrypted data. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, S&P 2000, Berkeley, CA, USA, 14–1 7 May 2000; pp. 44–55.
10. Goh, E.J.; others. Secure indexes. *IACR Cryptol. Eprint Arch.* **2003**, *2003*, 216.
11. Chang, Y.C.; Mitzenmacher, M. Privacy preserving keyword searches on remote encrypted data. In Proceedings of the International Conference on Applied Cryptography and Network Security, New York, NY, USA, 7–10 June 2005; pp. 442–455.
12. Curtmola, R.; Garay, J.; Kamara, S.; Ostrovsky, R. Searchable symmetric encryption: Improved definitions and efficient constructions. *J. Comput. Secur.* **2011**, *19*, 895–934.
13. Kamara, S.; Papamanthou, C.; Roeder, T. Dynamic searchable symmetric encryption. In Proceedings of the 2012 ACM conference on Computer and communications security, Raleigh, NC, USA, 16–18 October 2012; pp. 965–976.
14. Kamara, S.; Papamanthou, C. Parallel and dynamic searchable symmetric encryption. In Proceedings of the International Conference on Financial Cryptography and Data Security, Okinawa, Japan, 1–5 April 2013; pp. 258–274.
15. Bösch, C.; Hartel, P.; Jonker, W.; Peter, A. A survey of provably secure searchable encryption. *Acm Comput. Surv. (Csur)* **2014**, *47*, 1–51.
16. Wang, Y.; Wang, J.; Chen, X. Secure searchable encryption: A survey. *J. Commun. Inf. Netw.* **2016**, *1*, 52–65.
17. Pham, H.; Woodworth, J.; Salehi, M.A. Survey on secure search over encrypted data on the cloud. *Arxiv* **2018**, Arxiv:1811.09767.
18. Handa, R.; Krishna, C.R.; Aggarwal, N. Searchable encryption: A survey on privacy-preserving search schemes on encrypted outsourced data. *Concurr. Comput. : Pract. Exp.* **2019**, *31*, e5201.
19. Han, F.; Qin, J.; Hu, J. Secure searches in the cloud: A survey. *Future Gener. Comput. Syst.* **2016**, *62*, 66–75.
20. Boneh, D.; Di Crescenzo, G.; Ostrovsky, R.; Persiano, G. Public key encryption with keyword search. In Proceedings of the 2004 International conference on the theory and applications of cryptographic techniques, Interlaken, Switzerland, 2–6 May 2004; pp. 506–522.
21. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. In Proceedings of the 2001 Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
22. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. *SIAM J. Comput.* **2003**, *32*, 586–615.
23. Byun, J.W.; Rhee, H.S.; Park, H.A.; Lee, D.H. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In Proceedings of the 2006 Workshop on Secure Data Management, Seoul, Korea, 10–11 September 2006; pp. 75–83.
24. Lu, Y.; Wang, G.; Li, J. Keyword guessing attacks on a public key encryption with keyword search scheme without random oracle and its improvement. *Inf. Sci.* **2019**, *479*, 270–276.

25. Baek, J.; Safavi-Naini, R.; Susilo, W. Public key encryption with keyword search revisited. In Proceedings of the International conference on Computational Science and Its Applications, Perugia, Italy, 1–4 July 2008; pp. 1249–1259.
26. Zhang, Y.; Katz, J.; Papamanthou, C. All your queries are belong to us: The power of file-injection attacks on searchable encryption. In Proceedings of the 25th {USENIX} Security Symposium ({USENIX} Security 16), Austin, TX, USA, 10–12 August 2016; pp. 707–720.
27. Rhee, H.S.; Park, J.H.; Susilo, W.; Lee, D.H. Improved searchable public key encryption with designated tester. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 10–12 March 2009; pp. 376–379.
28. Park, D.J.; Kim, K.; Lee, P.J. Public key encryption with conjunctive field keyword search. In Proceedings of the 2004 International Workshop on Information Security Applications, Jeju Island, Korea, 23–25 August 2004; pp. 73–86.
29. Hwang, Y.H.; Lee, P.J. Public key encryption with conjunctive keyword search and its extension to a multi-user system. In Proceedings of the 2007 International Conference on Pairing-Based Cryptography, Tokyo, Japan, 2–4 July 2007; pp. 2–22.
30. Zhang, B.; Zhang, F. An efficient public key encryption with conjunctive-subset keywords search. *J. Netw. Comput. Appl.* **2011**, *34*, 262–267.
31. Lv, Z.; Hong, C.; Zhang, M.; Feng, D. Expressive and secure searchable encryption in the public key setting. In Proceedings of the 2014 International Conference on Information Security, Hong Kong, China, 12–14 October 2014; pp. 364–376.
32. Tang, Q.; Chen, L. Public-key encryption with registered keyword search. In Proceedings of the 2009 European Public Key Infrastructure Workshop, Pisa, Italy, 10–11 September 2009; pp. 163–178.
33. Hu, C.; Liu, P. An enhanced searchable public key encryption scheme with a designated tester and its extensions. *J. Comput.* **2012**, *7*, 716–723.
34. Fang, L.; Susilo, W.; Ge, C.; Wang, J. Public key encryption with keyword search secure against keyword guessing attacks without random oracle. *Inf. Sci.* **2013**, *238*, 221–241.
35. Shao, Z.Y.; Yang, B. On security against the server in designated tester public key encryption with keyword search. *Inf. Process. Lett.* **2015**, *115*, 957–961.
36. Zhang, R.; Xue, R.; Yu, T.; Liu, L. PVSAE: A public verifiable searchable encryption service framework for outsourced encrypted data. In Proceedings of the 2016 IEEE International Conference on Web Services (ICWS), San Francisco, CA, USA, 27 June–2 July 2016; pp. 428–435.
37. Huang, Q.; Li, H. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. *Inf. Sci.* **2017**, *403*, 1–14.
38. Wu, L.; Chen, B.; Zeadally, S.; He, D. An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage. *Soft Comput.* **2018**, *22*, 7685–7696.
39. Bellare, M.; Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. In Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA, USA, 3–5 November 1993; pp. 62–73.
40. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of the 1984 Workshop on the Theory and Application of Cryptographic Techniques. Paris, France, 9–11 April 1984; pp. 47–53.
41. Di Crescenzo, G.; Saraswat, V. Public key encryption with searchable keywords based on Jacobi symbols. In Proceedings of the 2007 International Conference on Cryptology in India, Chennai, India, 9–13 December 2007; pp. 282–296.
42. Cocks, C. An identity based encryption scheme based on quadratic residues. In Proceedings of the 2001 IMA International Conference on Cryptography and Coding, Cirencester, UK, 17–19 December 2001; pp. 360–363.
43. Tian, X.; Wang, Y. ID-based encryption with keyword search scheme from bilinear pairings. In Proceedings of the 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 12–17 October 2008; pp. 1–4.
44. Camenisch, J.; Kohlweiss, M.; Rial, A.; Sheedy, C. Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data. In Proceedings of the 2009 International Workshop on Public Key Cryptography, Irvine, CA, USA, 18–20 March 2009; pp. 196–214.
45. Abdalla, M.; Bellare, M.; Catalano, D.; Kiltz, E.; Kohno, T.; Lange, T.; Malone-Lee, J.; Neven, G.; Paillier, P.; Shi, H. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions.

In Proceedings of the 2005 Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005; pp. 205–222.
46. Khader, D. Public key encryption with keyword search based on K-resilient IBE. In Proceedings of the 2007 International Conference on Computational Science and Its Applications, Kuala Lumpur, Malaysia, 26–29 August 2007; pp. 1086–1095.
47. Wu, T.Y.; Tsai, T.T.; Tseng, Y.M. Efficient searchable ID-based encryption with a designated server. *Ann. Telecommun.* **2014**, *69*, 391–402.
48. Lu, Y.; Wang, G.; Li, J.; Shen, J. Efficient designated server identity-based encryption with conjunctive keyword search. *Ann. Telecommun.* **2017**, *72*, 359–370.
49. Siad, A. Anonymous identity-based encryption with distributed private-key generator and searchable encryption. In Proceedings of the 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), Istanbul, Turkey, 7–10 May 2012; pp. 1–8.
50. Emura, K.; Watanabe, Y. Keyword revocable searchable encryption with trapdoor exposure resistance and re-generateability. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 167–174.
51. Wang, X.F.; Mu, Y.; Chen, R.; Zhang, X.S. Secure channel free id-based searchable encryption for peer-to-peer group. *J. Comput. Sci. Technol.* **2016**, *31*, 1012–1027.
52. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Proceedings of the 2005 Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; pp. 457–473.
53. Zhao, F.; Nishide, T.; Sakurai, K. Multi-user keyword search scheme for secure data sharing with fine-grained access control. In Proceedings of the 2011 International Conference on Information Security and Cryptology, Seoul, Korea, 30 November–2 December 2011; pp. 406–418.
54. Han, F.; Qin, J.; Zhao, H.; Hu, J. A general transformation from KP-ABE to searchable encryption. *Future Gener. Comput. Syst.* **2014**, *30*, 107–115.
55. Wang, C.; Li, W.; Li, Y.; Xu, X. A ciphertext-policy attribute-based encryption scheme supporting keyword search function. In *Cyberspace Safety and Security*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 377–386.
56. Zheng, Q.; Xu, S.; Ateniese, G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, Canada, 27 April–2 May 2014; pp. 522–530.
57. Liu, P.; Wang, J.; Ma, H.; Nie, H. Efficient verifiable public key encryption with keyword search based on KP-ABE. In Proceedings of the 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications, Guangdong, China. 8–10 November 2014; pp. 584–589.
58. Li, J.; Lin, X.; Zhang, Y.; Han, J. KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage. *IEEE Trans. Serv. Comput.* **2016**, *10*, 715–725.
59. Yang, Y. Attribute-based data retrieval with semantic keyword search for e-health cloud. *J. Cloud Comput.* **2015**, *4*, 10.
60. Ning, J.; Dong, X.; Cao, Z.; Wei, L.; Lin, X. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1274–1288.
61. Sun, W.; Yu, S.; Lou, W.; Hou, Y.T.; Li, H. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *27*, 1187–1198.
62. Zhu, H.; Mei, Z.; Wu, B.; Li, H.; Cui, Z. Fuzzy keyword search and access control over ciphertexts in cloud computing. In *Proceedings of the 2017 Australasian Conference on Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 248–265.
63. Miao, Y.; Ma, J.; Liu, X.; Li, X.; Jiang, Q.; Zhang, J. Attribute-based keyword search over hierarchical data in cloud computing. *IEEE Trans. Serv. Comput.* **2017**, doi:10.1109/TSC.2017.2757467.
64. Cao, L.; Zhang, J.; Dong, X.; Xi, C.; Wang, Y.; Zhang, Y.; Guo, X.; Feng, T. A based on blinded CP-ABE searchable encryption cloud storage service scheme. *Int. J. Commun. Syst.* **2018**, *31*, e3566.
65. Miao, Y.; Liu, X.; Choo, K.K.R.; Deng, R.H.; Li, J.; Li, H.; Ma, J. Privacy-preserving attribute-based keyword search in shared multi-owner setting. *IEEE Trans. Dependable Secur. Comput.* **2019**, doi:10.1109/TDSC.2019.2897675.

66. Katz, J.; Sahai, A.; Waters, B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer: Berlin/Heidelberg, Germany, 2008; pp. 146–162.
67. Blundo, C.; Iovino, V.; Persiano, G. Predicate encryption with partial public keys. In *Proceedings of the 2010 International Conference on Cryptology and Network Security*. Springer: Berlin/Heidelberg, Germany, 2010, pp. 298–313.
68. Zhu, B.; Zhu, B.; Ren, K. PEKSrand: Providing predicate privacy in public-key encryption with keyword search. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–6.
69. Katz, J.; Sahai, A.; Waters, B. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *J. Cryptol.* **2013**, *26*, 191–224.
70. Zhang, Y.; Lu, S. POSTER: Efficient method for disjunctive and conjunctive keyword search over encrypted data. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1535–1537.
71. Kim, I.; Hwang, S.O.; Park, J.H.; Park, C. An efficient predicate encryption with constant pairing computations and minimum costs. *IEEE Trans. Comput.* **2016**, *65*, 2947–2958.
72. Zhang, Y.; Li, Y.; Wang, Y. Secure and efficient searchable public key encryption for resource constrained environment based on pairings under prime order group. *Secur. Commun. Netw.* **2019**, *2019*, 5280806.
73. Gay, R.; Méaux, P.; Wee, H. Predicate encryption for multi-dimensional range queries from lattices. In *Proceedings of the 2015 IACR International Workshop on Public Key Cryptography*. Springer: Berlin/Heidelberg, Germany, 2015; pp. 752–776.
74. Zhang, Y.; Wang, Y.; Li, Y. Searchable Public Key Encryption Supporting Semantic Multi-Keywords Search. *IEEE Access* **2019**, *7*, 122078–122090.
75. Al-Riyami, S.S.; Paterson, K.G. Certificateless public key cryptography. In *Proceedings of the 2003 International Conference on the Theory and Application of Cryptology and Information Security*. Springer: Berlin/Heidelberg, Germany, 2003; pp. 452–473.
76. Yanguo, P.; Jiangtao, C.; Changgen, P.; Zuobin, Y. Certificateless public key encryption with keyword search. *China Commun.* **2014**, *11*, 100–113.
77. Wu, T.Y.; Meng, F.; Chen, C.M.; Liu, S.; Pan, J.S. On the security of a certificateless searchable public key encryption scheme. In *Proceedings of the 2016 International Conference on Genetic and Evolutionary Computing*. Springer: Berlin/Heidelberg, Germany, 2016; pp. 113–119.
78. Zheng, Q.; Li, X.; Azgin, A. CLKS: Certificateless keyword search on encrypted data. In *Proceedings of the 2015 International Conference on Network and System Security*. Springer: Berlin/Heidelberg, Germany, 2015; pp. 239–253.
79. Ma, M.; He, D.; Kumar, N.; Choo, K.K.R.; Chen, J. Certificateless searchable public key encryption scheme for industrial internet of things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 759–767.
80. Ma, M.; He, D.; Khan, M.K.; Chen, J. Certificateless searchable public key encryption scheme for mobile healthcare system. *Comput. & Electr. Eng.* **2018**, *65*, 413–424.
81. Islam, S.H.; Obaidat, M.S.; Rajeev, V.; Amin, R. Design of a certificateless designated server based searchable public key encryption scheme. In *Proceedings of the 2007 International Conference on Mathematics and Computing*. Springer: Berlin/Heidelberg, Germany, 2017; pp. 3–15.
82. Wu, L.; Zhang, Y.; Ma, M.; Kumar, N.; He, D. Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things. *Ann. Telecommun.* **2019**, *74*, 423–434.
83. Lu, Y.; Li, J.g. Constructing pairing-free certificateless public key encryption with keyword search. *Front. Inf. Technol. & Electron. Eng.* **2019**, *20*, 1049–1060.
84. Blaze, M.; Bleumer, G.; Strauss, M. Divertible protocols and atomic proxy cryptography. In *Proceedings of the 1998 International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1998, pp. 127–144.
85. Shao, J.; Cao, Z.; Liang, X.; Lin, H. Proxy re-encryption with keyword search. *Inf. Sci.* **2010**, *180*, 2576–2587.
86. Yau, W.C.; Phan, R.C.W.; Heng, S.H.; Goi, B.M. Proxy re-encryption with keyword search: New definitions and algorithms. In *Security Technology, Disaster Recovery and Business Continuity*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 149–160.

87. Zhong, W.; Wang, X.A.; Wang, Z.; Ding, Y. Proxy re-encryption with keyword search from anonymous conditional proxy re-encryption. In Proceedings of the 2011 Seventh International Conference on Computational Intelligence and Security,Hainan, China, 3–4 December 2011; pp. 969–973.
88. Wang, X.A.; Huang, X.; Yang, X.; Liu, L.; Wu, X. Further observation on proxy re-encryption with keyword search. *J. Syst. Softw.* **2012**, *85*, 643–654.
89. Guo, L.; Lu, B.; Li, X.; Xu, H. A verifiable proxy re-encryption with keyword search without random oracle. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, China, 14–15 December 2013; pp. 474–478.
90. Yang, Y.; Ma, M. Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 746–759.
91. Yang, Y.; Zheng, X.; Chang, V.; Tang, C. Semantic keyword searchable proxy re-encryption for postquantum secure cloud storage. *Concurr. Comput. : Pract. Exp.* **2017**, *29*, e4211.
92. Shi, Y.; Liu, J.; Han, Z.; Zheng, Q.; Zhang, R.; Qiu, S. Attribute-based proxy re-encryption with keyword search. *PloS one* **2014**, *9*, e116325.
93. Chen, Z.; Li, S.; Huang, Q.; Wang, Y.; Zhou, S. A restricted proxy re-encryption with keyword search for fine-grained data access control in cloud storage. *Concurr. Comput. : Pract. Exp.* **2016**, *28*, 2858–2876.
94. Hong, H.; Sun, Z. Towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search. In Proceedings of the 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 28–30 April 2017; pp. 218–223.
95. Chen, Y.; Hu, Y.; Zhu, M.; Yang, G. Attribute-Based Keyword Search with Proxy Re-Encryption in the Cloud. *IEICE Trans. Commun.* **2018**, *101*, 1798–1808.
96. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *24*, 131–143.
97. Guo, L.; Yau, W.C. Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage. *J. Med Syst.* **2015**, *39*, 11.
98. Wu, Y.; Lu, X.; Su, J.; Chen, P. An efficient searchable encryption against keyword guessing attacks for sharable electronic medical records in cloud-based system. *J. Med Syst.* **2016**, *40*, 258.
99. Liu, Z.; Weng, J.; Li, J.; Yang, J.; Fu, C.; Jia, C. Cloud-based electronic health record system supporting fuzzy keyword search. *Soft Comput.* **2016**, *20*, 3243–3255.
100. Lu, Y.; Li, J. Efficient searchable public key encryption against keyword guessing attacks for cloud-based EMR systems. *Cluster Comput.* **2019**, *22*, 285–299.
101. Wen, M.; Lu, R.; Zhang, K.; Lei, J.; Liang, X.; Shen, X. PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid. *IEEE Trans. Emerg. Top. Comput.* **2013**, *1*, 178–191.
102. Li, H.; Yang, Y.; Wen, M.; Luo, H.; Lu, R. Emrq: An efficient multi-keyword range query scheme in smart grid auction market. *KSII Trans. Int. Inf. Syst.* **2014**, *8*, 3937–3954.
103. Eltayieb, N.; Elhabob, R.; Hassan, A.; Li, F. An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. *J. Syst. Archit.* **2019**, *98*, 165–172.
104. Uwizeye, E.; Wang, J.; Cheng, Z.; Li, F. Certificateless public key encryption with conjunctive keyword search and its application to cloud-based reliable smart grid system. *Ann. Telecommun.* **2019**, *74*, 435–449.
105. Gu, C.; Guang, Y.; Zhu, Y.; Zheng, Y. Public key encryption with keyword search from lattices. *Int. J. Inf. Technol.* **2013**, *19*, 1–10.
106. Gu, C.; Zheng, Y.; Kang, F.; Xin, D. Keyword search over encrypted data in cloud computing from lattices in the standard model. In *Proceedings of the 2015 Second International Conference on Cloud Computing and Big Data in Asia*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 335–343.
107. Yang, Y.; Ma, M. Semantic searchable encryption scheme based on lattice in quantum-era. *J. Inf. Sci. Eng.* **2016**, *32*, 425–438.
108. Zhang, X.; Xu, C. Trapdoor security lattice-based public-key searchable encryption with a designated cloud server. *Wirel. Pers. Commun.* **2018**, *100*, 907–921.

109. Tahir, S.; Rajarajan, M. Privacy-preserving searchable encryption framework for permissioned blockchain networks. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1628–1633.
110. Tang, Q. Towards Blockchain-enabled Searchable Encryption. *Arxiv* **2019**, Arxiv:1908.09564.
111. Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429.