Hindawi
International Journal of Mathematics and Mathematical Sciences
Volume 2022, Article ID 3223509, 10 pages
https://doi.org/10.1155/2022/3223509

Review Article

A Survey on Public Key Encryption with Keyword Search: Taxonomy and Methods

M.H. Noorallahzade,[1] **R. Alimoradi**,[2] **and A. Gholami**[3]

[1]*Faculty of Mathematical Sciences, Qom University, Qom, Iran*
[2]*Department of Computer Science, Faculty of Science, Qom University, Qom, Iran*
[3]*Faculty of Science, Qom University, Qom, Iran*

Correspondence should be addressed to R. Alimoradi; r.alimoradi@qom.ac.ir

Received 25 December 2021; Accepted 7 February 2022; Published 11 March 2022

Academic Editor: Ram N. Mohapatra

Given the many benefits that cloud computing brings, organizations tend to outsource most of their data to reduce a large portion of their costs, but concern about the privacy of data is a major obstacle to outsourcing sensitive data. To solve this problem, public key encryption with keyword search (PEKS) is suggested, which is a widely used method. Addressing this issue separately is beneficial because PEKS does not require a secure communication channel and key distribution. Therefore, at first glance, it seems that PEKS schemes should be used more in practical applications. Thus, reviewing and categorizing PEKS schemes are very important and necessary. In this article, we have tried to help reviewing the public key searchable encryption and categorizing these designs.

1. Introduction

Today, cloud storage services are very well known and common. Many people and businesses use these services and outsource their data to reduce a large portion of their costs. Some cloud storage providers such as Amazon, Windows Azure, and Google Cloud are well known to quickly offer searchable encryption services to succeed in attracting more customers. Cloud storage services [1] are popular because of the many benefits that are popular and enable users to view their data from anywhere and anytime and get the information they need. However, users still do not have the confidence in cloud servers to outsource their sensitive data. Most cloud servers are assumed to be honest but curious. Cloud storage should provide practical and reliable solutions to ensure the security of these data and maintain the ability to search for users. Data sent against infiltration [2, 3] by illegal institutions is very vital, especially in critical infrastructures. To protect sensitive data, a simple way is to encrypt data before outsourcing, but when the user intends to search a keyword among the data, it will be difficult to search. During the time, two solutions were used; both of which today are rejected. First, the user receives all the data, decrypts them, does the search, then re-encrypts the data, and saves the cloud server. This is considered in contradiction with the use of cloud services. The second way is to provide encryption key to the cloud server, which does not logically work because the server cannot be reliable. The first solution was suggested by Goldreich and Ostrovsky [4], but their scheme needs a lot of connection between the server and the user and has low performance. Song et al. [5] proposed a practical plan for the first time. The Song scheme [5] is based on symmetric encryption (SSE). You can see several efficient schemes in this category in [6, 7]. The key management of such schemes is difficult when it comes to multiuser scheme. To solve this problem, PEKS plans were suggested. Therefore, PEKS plans are used more compared to SSE schemes. Also, most of these schemes require a secure communication channel to send sensitive data between users, which in practical applications is very difficult to achieve. To solve this problem, PEKS plans were proposed. Therefore, it seems that PEKS schemes are used more than

SSE schemes. Of course, to conclude about this, the solutions offered by service providers should be considered. Types of PEKS schemes offer different search functionalities. If we want to mention the total search functionalities for these schemes, things such as conjunctive keyword search, single keyword search, fuzzy keyword search, ranking keyword search, multikeyword search, verifiable keyword search, semantic keyword search, similarity keyword search, subset query, and range query can be mentioned.

There are many overviews such as given in [8, 9] in this area. In this article, we try to first categorize this field from different perspectives and then provide a complete classification for readers. To compare different schemes, it should be noted that each scheme is presented to solve one or more problems, so this scheme should be compared with its own categories to get the correct results from this comparison. In general, according to the usage scenario, the schemes can be compared in terms of security, performance, and functionality.

The remainder of this article is organized as follows: Section 2 provides some applications of PEKS; Section 3 provides a PEKS framework; Section 4 provides classification of existing PEKS schemes; Section 5 deals with the conclusion.

2. Some Applications of PEKS

2.1. PEKS Can Be Used for Healthcare. To reduce their costs, healthcare providers and large hospitals tend to store their patients' electronic medical records on a cloud server that provides cloud computing services. Because the cloud server is not completely trustworthy, patient privacy and security may be compromised. Therefore, to solve this problem, large hospitals prefer to encrypt their patients' medical data before sending it to the cloud server. Given that physicians need details of a patient's previous illness to correctly diagnose a disease, it is best for them to be able to use the details of opinions shared with other physicians. The proposed solution could be PEKS, which allows searching for encrypted data and sharing it with other users who are allowed to search. There are many articles and documents for healthcare [10, 11].

2.2. PEKS Can Be Used in Electronic Banking. Large banks tend to store their customers' electronic records on a cloud server that provides cloud computing services to reduce costs and improve their computing power in the e-banking sector. Because the cloud server is not completely trustworthy, the privacy and security of bank customers (such as bank account balances) may be compromised. Therefore, to solve this problem, large banks prefer to encrypt their customers' bank account information before sending it to the cloud server. The proposed solution could be PEKS, which would allow banks to safely and worry-free search operations on encrypted data.

2.3. PEKS Can Be Used in Internet of Things. Today, the Internet of Things (IoT) is widely used by the public and is a popular trend among researchers. Given that a huge amount of data is generated by sensors and stored on cloud servers and since users should be able to access the data they want through search, the proposed solution could be PEKS, which with its help, users will be able to perform search operations on encrypted data securely and without any disclosure of information.

2.4. PEKS Can Be Used for Big Data. Big data means a huge amount of structured and unstructured data that have the potential to help companies improve their operations and make faster and smarter decisions. The amount of the data is so large that it is difficult to process it with traditional databases and existing software. In most organizations, the amount of data is too large or moving too fast and organizations do not have the capacity. Of course, organizations have decided to use cloud computing services since they encountered big data, but to do so, they must either have complete confidence in the cloud servers or they must first encrypt their data and then send it to the cloud server. Since organizations never fully trust cloud servers and after encrypting their data with current methods, they lose the ability to search their data and they will certainly turn to cloud service providers to cover searchable encryption. Currently, cloud computing service providers are looking for suitable encryption schemes to protect the privacy of their customers.

3. General PEKS Framework

The PEKS general framework was first proposed in 2004 by Boneh et al. [12]. The framework combination of three entities (user, data owner (DO), and cloud server) together creates PEKS. The DO encrypts the documents, encrypts the index with the user's public key, and finally sends them to the cloud server for storage. The user who has the private key corresponding to the public key can send the search request to the cloud server. He generates a suitable trapdoor with the help of a private key and sends it to the cloud server. After receiving the trapdoor, the cloud server checks whether the search query matches the index. If matched, the cloud server sends encrypted documents to the user as search results. The user can decrypt encrypted documents. PEKS is more suitable for open networks (insecure networks). The PEKS model can be seen in Figure 1.

3.1. PEKS Algorithms. Each PEKS scheme usually includes the following four algorithms [12]:

KeyGen(): this is a key generation algorithm that receives a security parameter as input and provides a public key and private key (PK, SK) as output. The user who receives the search results runs the key generation algorithm.

PEKS (PK, W): this encryption algorithm receives the PK user's public key and a W keyword as input and presents the S code as output. Note that the PEKS algorithm is always run by the data owner.

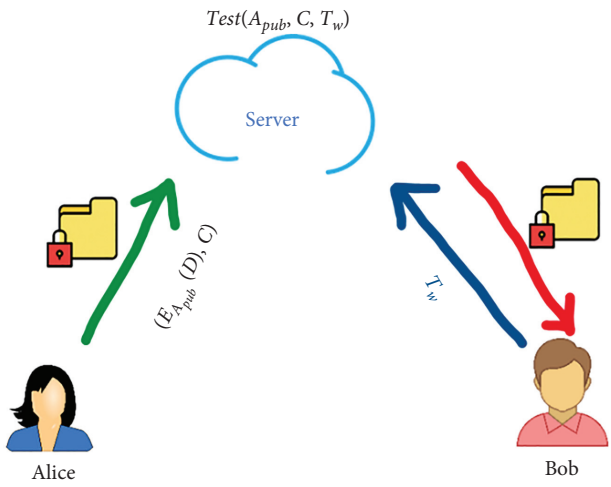

Figure 1: The PEKS model.

Trapdoor (SK, W): this algorithm, to generate trapdoor, receives SK user's private key as input, a W query keyword, and TW as output to send to the server. The user who receives the search results runs the trapdoor algorithm.

Test (PK, S, TW): this search algorithm receives as input public PK key, ciphertext S, and TW. If W was matched in the search process, the output of the algorithm is "Yes," and the corresponding documents are provided to the user. Otherwise, the answer of the test algorithm will be "No."

3.2. PEKS Security Models. For the first time, indistinguishable against a chosen keyword attack (IND-CKA) was introduced by Boneh et al. [12] by playing a game between adversary A and challenger C. This game is fully described below.

Setup: first the KeyGen() is run by challenger C, and he receives the key pair (PK, SK) as the output of this algorithm. He gives PK to adversary A but keeps SK's private key to himself.

Step 1. Adversary A can adaptively ask challenger C for the results of the keywords of his choice.

Challenge: adversary A sends two keywords, W_0 and W_1, which he has never sent to challenger C before. Challenger C randomly selects the bit b and calculates and sends a C = PEKS (PK, Wb) ciphertext to the adversary A.

Step 2. Adversary A can send any keyword of his choice except W_0 and W_1, as additional requests in Phase 1 to the challenger.

Adversary A guesses the bit b_0, and if $b = b_0$, he will win the game. $\mathrm{Adv}A(s) = \Pr[b = b_0] - 1/2$ (absolute value of probability is considered). If adversary A has a negligible advantage to win the game, the result is that the PEKS IND-CKA scheme is secure.

3.3. Attack Models. According to attack models published for PEKS schemes, existing PEKS schemes are vulnerable to keyword guessing and file injection attacks. In the following, we describe the attack models for PEKS schemes.

3.3.1. File Injection Attack. File injection (FI) attack has also attracted the attention of many researchers and is now an important issue to consider when designing a PEKS scheme.

Zhang and Zhang [13] were the first to launch a file injection attack on searchable encryption. This attack is dangerous when there is a malicious cloud server (internal attacker) that can inject certain data to get good information about the keyword query. The access pattern is leaked by executing the file injection attack, so by executing this attack, privacy is violated because this attack provides a significant amount of sensitive data to the attacker. Therefore, it is very important to design PEKS schemes that are resistant to this attack and at the same time have good performance.

3.3.2. Keyword Guessing Attack. If we want to point out one of the most important attacks on PEKS schemes, we must mention the keyword guess attack. Boneh et al. [12] first applied a keyword guess attack on some PEKS schemes. Because of the small space of keywords, this attack is applicable. This attack enables the attacker to retrieve the encrypted keyword correctly. KG attack is divided into two categories: external attack when there is an external attacker and internal attack when there is an internal attacker [14]. External attack: in this attack, we have an external attacker who is out of our scheme. This attacker carries out an attack through a public channel between the server and the user. For example, Baek et al. [15] proposed a PEKS scheme in which there is no secure communication channel. In their scheme, the trapdoor is transmitted through a public channel, so that an external attacker can view or store encrypted keywords through this channel. Internal attack: in this attack, the internal attacker is usually considered a malicious cloud server. If there is a malicious cloud server, each user (without worries) sends encrypted keywords to that server. This server can also receive trapdoor information from the user. It should be noted that a malicious cloud server can even communicate between an encrypted keyword and a trapdoor by running a TEST algorithm. From what has been said, it is very difficult to build resistance against an internal attacker.

4. Classification of Existing PEKS Schemes

Since most work environments are not closed, symmetric searchable encryption schemes may not always be possible. Asymmetric searchable encryption was designed and

introduced for open environments. To address key management in SSE, the PEKS was introduced. The purpose of this section is to provide a comprehensive overview of the PEKS schemes that have been published so far and to provide an overview of the research and documentation published so far. First, to achieve the desired goals, we divide PEKS schemes into six classes (see Figure 2).

4.1. PEKS Based on Public Key Infrastructure (PEKS-PKI). According to Section 2, it is natural that most PEKS schemes are based on PKI with digital certificate management. In these schemes, the sender (Alice) can verify the receiver's public key from the digital certificate before encryption and then encrypt the keywords and data with the public key in the certificate. Finally, he sends the encrypted document and data to the cloud server. The receiver (Bob) sends the trapdoor to the cloud server with his secret key to test whether the encrypted data matched the keyword he wants. The digital public key certificate is produced in a public key infrastructure by a trusted third party.

The first scheme was proposed by Boneh et al. [12] based on the public key infrastructure using a bilinear pairing map. Because of the existence of the receiver's digital certificate, the user who has this certificate is allowed to create index with the public key, but only the private key holder can create a trapdoor for the query. It should be noted that their scheme requires a secure communication channel to transmit the trapdoor. However, creating a secure communication channel is difficult and expensive. Baek et al. [15] introduced a PEKS scheme that did not require a secure communication. In their scheme, the server also needs a pair of public and private keys. It should be noted that the server selected by the sender can perform the test algorithm. The security of this scheme is in the oracle random model under BDH problem. Tang and Chen [16] introduced a new PKI-based PEKS scheme to improve the scheme by Baek et al. [15] that the attacker can obtain the relationship between the trapdoor and ciphertext.

The PEKS scheme, which supported linked keyword search in two structures with public key encryption introduced by Park et al. [17], was based on the DBDH problem and the DBDHI problem. Their scheme requires many connections between the user and the server and has a storage overhead. Huang and Li [18] were able to improve the scheme of Park et al. [17]. The scheme introduces multiuser public key encryption with conjunctive keyword search to save the number of user-server connections and storage. Zhang and Zhang [13], to improve the scheme of Park et al. [17], introduced a scheme that offers the ability to search for subset keywords. Lv et al. [19] introduced an expressive and secure PEKS scheme that offers the ability to search for disjunctive, conjunctive, and negation based on hybrid order groups. The security of this scheme can be proven in the standard model, and the range search feature can also be added to this scheme.

Tang and Chen [16] introduced a scheme with a specific condition for producing searchable content. This scheme is resistant to offline guessing keyword attacks. Hu and Liu [20] introduced a scheme that can decrypt the keyword.

Fang et al. [21] developed a scheme that is resistant to keyword guess attacks, ciphertext attacks, and chosen keyword attacks, and it is SCF-PEKS secure. Their PEKS scheme does not require a secure communication or channel. Shao and Yang [22] improved the scheme of Fang et al. in terms of resistance to keyword guessing attacks. Therefore, without compromising the security of the scheme, the server can be considered an attacker. Lu et al. [14] argued that Shao and Yang's scheme [22] was not resistant to keyword guessing attacks, so they came up with a new scheme to improve Fang et al.'s scheme [21]. This scheme has good resistance against both internal and external adversaries.

Zhang and Zhang [13] introduced a scheme, which was a new scheme that supported keyword verification functionality. This scheme has a structure that can be highly efficient and maintain a strong security feature. Huang and Li [18] introduced a scheme, in which the data sender not only encrypts the keyword but also authenticates it. The scheme is still secure when a malicious server is considered. Wu et al. [23] introduced a scheme to achieve optimal resistance to file-injected attacks and KGA attacks.

4.2. PEKS Based on Identity-Based Encryption (PEKS-IBE). Shamir [24] first introduced IBE encryption in 1984. This method simplifies certificate management (public key management) based on PKI. In IBE, the public key holder can be an e-mail address, an IP address, a phone number, an ID, and any field. In this method, generating a private key (PKG) can be in accordance with the user authentication. In a PEKS-IBE scheme, a sender encrypted text to a cloud server and then the receiver identifies himself to PKG. He generates a trapdoor with his private key and then sends trapdoor to cloud server. Finally, the cloud server performs the keyword search operation.

Boneh et al. [12] introduced the first PEKS-IBE scheme in which the keyword acted as an identity. Di Crescenzo and Saraswat [25] introduced the first PEKS-IBE scheme based on Jacobi symbols and the quadratic residual problem without bilinear maps [26]. The scheme needs high storages and secure communication channel. Of course, the security of this scheme has been proven in the random oracle model. Next, Camenisch et al. [27] were able to improve computations and possible communication, although their scheme contained bilinear maps but did not require a secure communication channel. The security of this scheme has been proven in the random oracle model. Camenisch et al. [27] used the concept of anonymous and

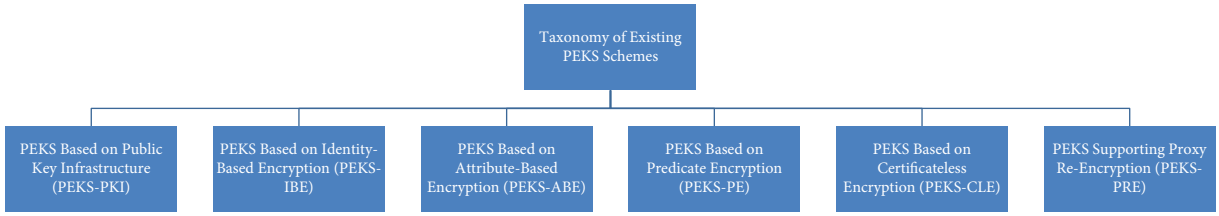

Figure 2: Classification of existing PEKS schemes.

blind identity encryption to improve security. In the scheme, the user can receive a search token from someone who has a private key without revealing more information.

Abdalla et al. [28] achieved a general PEKS structure for a hierarchical IBE scheme and an anonymous IBE scheme. The cloud server cannot use trapdoor in a specific time (the past or future) to execute the test algorithm. Khader [29] proposed a robust IBE-based PEKS scheme and provided a structure for a linked keyword search and a second structure without a secure communication channel for trapdoor conversion. The security of their scheme has been proven in oracle standard and under the assumption of DDH. This scheme requires complex communication space and calculations. Wu et al. [30] proposed a new PEKS scheme that did not require a secure communication channel and was resistant to offline KGA attacks. Lu et al. [31] introduced an IBE server scheme that removes the secure communication channel, can search for a conjunctive keyword, and is resistant to offline KGA attack.

4.3. PEKS Based on Attribute-Based Encryption (PEKS-ABE). Sahay and Waters [32] proposed attribute-based encryption (ABE) in 2005 that considers identity as a series of attribute sets. These attributes are user information parameters. In PKE, if a sender wants to encrypt a document using the public keys of several receivers, it must generate multiple ciphertexts from that document, and each receiver decrypts his or her own text using his or her private key. However, in ABE, the sender has only one access policy with which multiple users decrypt an encrypted document, so in this way, he encrypts a document once to generate only one ciphertext. The private key holder has attributes associated with this access policy. Decryption is allowed if the user's attributes comply with the relevant access policies. Attribute-based encryption can be divided into two parts: (1) ciphertext-policy attribute-based encryption (CP-ABE) and (2) key-policy attribute-based encryption (KP-ABE).

Zhao et al. [33] introduced a scheme to achieve multiuser keyword search capability with precise access control. They considered using attribute-based signatures. Han et al. [34] introduced a scheme in which the conversion of the ABE algorithm into a PEKS-ABE scheme was considered. They built a PEKS-ABE scheme based on KP-ABE with multiuser search capabilities, but the performance of this scheme did not meet expectations. Wang et al. [35] first introduced PEKS-CP-ABE and introduced a ciphertext-based encryption scheme to enable keyword search. The sender can specify the policy of access to his data so that only the receivers of legal data that comply with this policy can decrypt.

Zheng et al. [36] proposed a verifiable attribute-based PEKS scheme, in which the user can check whether the server is performing the correct keyword search. The disadvantage of this scheme is the need for the cost of expensive verifications and a secure communication channel. Next, Liu et al. [37] were able to improve the work of Zheng et al. [36]. They introduced a PEKS-ABE scheme that increased efficiency and did not require a secure communication channel. Li et al. [38] introduced a new method to reduce computational resources in PEKS-ABE, in which the server can decrypt part of the encrypted data without obtaining information from the original text.

Yang [39] introduced a PEKS-ABE scheme that made it easy to delete a user. The scheme uses bilinear pairing and can search multiple users and search for a semantic keyword but cannot consider traceability. Ning et al. [40] introduced a scheme based on CP-ABE. Sun et al. [41] were able to develop a PEKS-ABE scheme to improve the Yang [39] scheme. Zhu et al. [42] proposed a PEKS-ABE scheme with fuzzy keyword search capability.

Miao et al. [43] presented a PKES-ABE scheme based on hierarchical data, based on CP-ABE. Their original scheme failed to meet the requirements of the cloud, so they came up with two other schemes to improve the original scheme, which can delete the user and search for a multikeywords, but the scheme is still vulnerable to attacks. Cao et al. [44] were able to improve the scheme of Miao et al. [43] and increase security. Their scheme could perform blind operations.

4.4. PEKS Based on Predicate Encryption (PEKS-PE). The concept of predicate encryption was first proposed by Katz et al. [45] in 2008. This encryption method is a new public key encryption that allows users to search without knowing the private key using a special method (precise access control over encrypted data). Depending on the access control method, this encryption method has a high ability to hide hidden

features and shipments. The server run the test algorithm to match a trapdoor with encrypted index. At the end of work, the server returns the results to the receiver without disclosing any more information to the server. In this encryption method, only the private key holder can receive and decrypt the resulting encrypted texts related to the features.

Zhang and Lu [46] developed a PEKS-PE scheme, which in addition to the ability to search for disjunctive keywords can also search for conjunctive keywords. Kim et al. [47] provided an efficient propositional encryption. Recently, Zhang et al. [48] introduced a PEKS-PE scheme that can perform keyword conjunctive and disjunctive, is highly efficient, and requires less storage space. Zhang et al. [49] introduced a scheme of propositions that is highly efficient and capable of searching semantic multikeywords. In this scheme, the query keyword set and semantic index can be converted into an attribute and a prediction vector using a special method.

4.5. PEKS Based on Certificateless Encryption (PEKS-CLE). Certificateless encryption was first proposed in 2003 by Al-Riyami and Paterson [50], a new type of public key encryption system based on IBE. In this method, the secret key is not only generated by PKG but also the user cooperates with PKG in generating the private key. In a PEKS-CLE scheme, a data transmitter encrypts both the keyword and the data, using the public key and the receiver identity, and then sends the encrypted data to the server. The receiver first receives part of a private key from the PKG. A complete private key is a combination of what is received from the PKG and a secret value selected by the receiver. Finally, the receiver generates the trapdoor and sends it to the server. It should be noted that certificateless encryption does not have the problem of storing the key in identity-based encryption because PKG does not know the private key.

Yanguo et al. [51] first proposed a PEKS-CLE scheme without the need for a secure communication channel, after introducing certificateless encryption in PEKS, which was resistant to keyword guessing attack and chosen keyword attack. Wu et al. [52], by expressing the objections of Yanguo et al. [51], showed that this scheme could not be secure against offline key guessing attack and malicious PKG attack.

Zheng et al. [53] added keyword search to certificateless cryptography and succeeded in proposing a new PEKS-CLE scheme. The security of this scheme is proved in the standard model under the decisional linear assumption. Ma et al. [54] proposed a scheme for industrial deployment on the Internet of Things. This scheme is a new PEKS-CLE scheme that can search for a few keywords and does not require a secure communication channel, and in oracle's random model, its security is proven and is protected against public key replacement attack and PKG malicious attack. Also, Ma et al. [55], in their work for mobile healthcare systems, developed and published an efficient PEKS-CLE scheme to eliminate the key storage problem and key management problem. In addition, this scheme can resist the keyword guessing attack.

Recently, Lu and Li [56] introduced a PEKS-CLE scheme that did not use pairing. Since the use of bilinear pairing reduces the efficiency of the scheme, this scheme was proposed to improve the performance problems, and the security of this scheme can be proved assuming the complexity of the CDH problem in the random oracle model.

4.6. PEKS Supporting Proxy Re-Encryption (PEKS-PRE). This encryption method was first proposed by Blaze et al. [57] in EUROCRYPT'98. In this method, the proxy is a semitrusted third party and is responsible for converting ciphertext. It should be noted that the sender of the data may delegate its search right to a delegate after re-encrypting key without giving him his private key. This method is designed in such a way that the proxy cannot obtain the relevant plaintext information. PEKS-PRE is a proxy re-encrypting system that allows you to search for encrypted data without decrypting it. The server acts as a proxy that can convert encrypted data back into encrypted text that can be searched by the delegate. The sender has data that allow the other receiver to search. The proxy server is given a trapdoor that it can use for the test algorithm.

Shao [58] first combined PEKS and proxy encryption, with the goal of allowing one user to delegate keyword search to another. After presenting the bidirectional PEKS-PRE scheme, they proved its security in the oracle random model. Yau et al. [59] introduced a novel PEKS-PRE scheme that extended the original PEKS model (by adding re-encryption of keyword ciphertext and re-encryption key generation).

Wang et al. [60] introduced a PEKS-PRE scheme, which includes conjunctive keyword search, proxy re-encryption, and bilinear pairing, and proved the security of this scheme in a random oracle model. Guo et al. [61] increased the security of the previous scheme, and they introduced a new proxy re-encryption. Yang and Ma [62] introduced a PEKS-RE scheme for an electronic health record system. In this scheme, patients can, if necessary, delegate partial access to other users for a limited time so that they can search their records. Yang et al. [63] introduced a new PEKS-RE encryption scheme that covers semantic keyword search capabilities. This scheme is resistant to quantum attack.

Shi et al. [64] introduced for the first time the construction schemes based on CP-ABE and KP-ABE by combining proxy re-encryption and attribute-based encryption. According to this scheme, the user can assign the ability to search for the keyword to several users, if necessary. Chen et al. [65] combined attribute-keyword search with proxy re-encryption and introduced a new scheme that achieved fine-grained access control and data search functions.

Table 1 compares several PEKS schemes based on search functionality, security, and attack models.

Table 1: Comparison of several PEKS schemes.

	No.	Scheme	Search functionality	Security		Attack models				
				Model	Assumption	ROM	SCF	OKG	IKG	FI
PEKS-PKI schemes	1	Boneh et al. [40]	Single	IND-CKA	BDH	✓				
	2	Park et al. [17]-I	Conjunctive	IND-CKA	DBDH	✓				
	3	Park et al. [17]-II	Conjunctive	IND-CKA	DBDHI	✓				
	4	Hwang and Lee [66]	Conjunctive	IND-CKA	DLDH	✓				
	6	Rhee et al. [67]	Single	IND-CKA	BDH, BDHI	✓				
	7	Tang and Chen [16]	Single	IND-CKA	DBDH	✓	✓	✓		
	8	Zhang and Zhang [13]	Conjunctive, subset	TU, AC	DDHI			✓		
	9	Hu and Liu [20]	Single	IND-CKA	DLP, HDH		✓	✓		
	10	Shao and Yang [22]	Single	IND-KGAs	—		✓	✓		
	11	Huang and Li [18]	Single	SS	DBDH, mDLIN	✓		✓	✓	✓
	12	Wu et al. [23]	Single	IND-CKA	DBDH, CDH			✓	✓	✓
PEKS-IBE schemes	13	Khader [29]	Conjunctive	IND-CKA	DDH		✓			
	14	Di Crescenzo and Saraswat [25]	Single	IND-CKA	QIP	✓				
	16	Wu et al. [30]	Conjunctive	IND-CKA	BDH, CDH	✓	✓	✓		
	17	Wang et al. [68]	Multiuser	IND-CKA	DBDH	✓	✓	✓		
	18	Lu et al. [31]	Conjunctive	IND-CKA	DBDH, CDH	✓	✓	✓		
PEKS-ABE schemes	19	Wang et al. [35]	Single	SS	QDBDH			✓	✓	
	22	Sun et al. [41]	Verifiable	IND-CKA	DBDH					
	23	Li et al. [38]	Single	CPA	DBDH	✓			✓	
	24	Miao et al. [43]	Multikeyword	IND-CKA	DBDH	✓				
	25	Cao et al. [44]	Single	IND-CKA	BDH	✓				
	26	Miao et al. [69]	Single	SS	DBDH			✓		
PEKS-PE schemes	27	Zhu et al. [70]	Single	PP,SP	ECDLP					
	28	Zhang and Lu [46]	Disjunctive, conjunctive	CPA	—					
	29	Zhang et al. [49]	Semantic	CPA,IND-CKA	—			✓		
	30	Zhang et al. [48]	Conjunctive, disjunctive	IND-CKA	BDHI, DLIN	✓				
PEKS-CLE schemes	31	Yanguo et al. [51]	Single	IND-CKA	BDH	✓	✓	✓		
	32	Zheng et al. [53]	Single	CI	DLIN					
	33	Islam et al. [71]	Single	CI,DI	CDH, BDH		✓	✓		
	34	Ma et al. [55]	Single	IND-CKA	BDH	✓		✓		
	35	Wu et al. [72]	Single	SS	CBDH	✓	✓	✓	✓	
	36	Lu and Li [56]	Single	IND-CKA	CDH	✓				
PEKS-PRE schemes		Yau et al. [59]-I	Single	IND-CKA	BDH	✓				
		Yau et al. [59]-II	Single	IND-CKA	BDH	✓	✓			
		Wang et al. [60]	Conjunctive	wIND-CCA	q-BDHI	✓				
		Guo et al. [61]	Verifiable	IND-CKA	QDBDH, DBDH, HDH		✓	✓		
		Yang [62]	Conjunctive	IND-CKA	DBDH, DDH		✓	✓		
		Chen et al. [65]	Single	IND-CKA	q-BDHE	✓				

CPA, choose plaintext attack; ROM, random oracle model; OKG, outside keyword guessing attack; SCF, secure communication channel free; IKG, inside keyword guessing attack; DLDH, decision linear Diffie–Hellman assumption; DLP, discrete logarithm problem; mDLIN, modified decision linear assumption; SS, sematic security; CDH, computational Diffie–Hellman assumption; TU, trapdoor unforgettable; IND-KGAs, IND-KGA-server; AC, anonymous of the ciphertext; QIP, quadratic indistinguishability problem; QDBDH, quotient decisional bilinear Diffie–Hellman assumption; q-BDHI, q-bilinear Diffie–Hellman inversion assumption; HDH, hash Diffie–Hellman assumption; DLIN, decisional linear assumption; DDH, decisional Diffie–Hellman assumption; CI, ciphertext indistinguishability; CBDH, computational bilinear Diffie–Hellman assumption; DI, trapdoor indistinguishability; PP, predicate privacy; SP, statistics privacy.

5. Conclusion

In this article, we have tried to compare PEKS schemes from all possible aspects. It is expected that due to the expansion of this field and many kinds of research that are done in this field, we have been able to create the necessary familiarity by expressing various evaluation criteria from different perspectives of security, efficiency, and performance.

There are three main factors under which SE schemes are categorized: security, performance, and functionality. We hope that novice readers will better understand the concepts of PEKS by reading this article and find appropriate criteria for evaluating different schemes. For this purpose, we have

mentioned the content in a way that there are several criteria for selecting the appropriate security requirements, appropriate capabilities, appropriate performance, and appropriate solutions.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Konstantopoulos, P. Diamantopoulos, N. Chondros, and M. Roussopoulos, "Distributed personal cloud storage without third parties," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 11, pp. 2434–2448, 2019.

[2] M. Aloqaily, S. Otoum, I. AlRidhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, Article ID 101842, 2019.

[3] S. Otoum, B. Kantarci, and H. T. Mouftah, "Detection of known and unknown intrusive sensor behavior in critical applications," *IEEE Sensors Letters*, vol. 1, no. 5, pp. 1–4, 2017.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," *Journal of the ACM*, vol. 43, no. 3, pp. 431–473, 1996.

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of the 2000 IEEE symposium on security and privacy. S&P , 2000*, May 2000.

[6] E.-J. Goh, "Secure indexes," *IACR Cryptol. ePrint Arch.*vol. 2003, p. 216, 2003.

[7] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Proceedings of the International conference on financial cryptography and data security*, Okinawa, Japan, April 2013.

[8] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1–51, 2014.

[9] R. Handa, C. R. Krishna, and N. Aggarwal, "Searchable encryption: a survey on privacy-preserving search schemes on encrypted outsourced data," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 17, Article ID e5201, 2019.

[10] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, and C. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search," *Soft Computing*, vol. 20, no. 8, pp. 3243–3255, 2016.

[11] Y. Lu and J. Li, "Efficient searchable public key encryption against keyword guessing attacks for cloud-based EMR systems," *Cluster Computing*, vol. 22, no. 1, pp. 285–299, 2019.

[12] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proceedings of the International conference on the theory and applications of cryptographic techniques*, May 2004.

[13] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 262–267, 2011.

[14] Y. Lu, G. Wang, and J. Li, "Keyword guessing attacks on a public key encryption with keyword search scheme without random oracle and its improvement," *Information Sciences*, vol. 479, pp. 270–276, 2019.

[15] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *Proceedings of the International conference on Computational Science and Its Applications*, Perugia, Italy, July 2008.

[16] Q. Tang and L. Chen, "Public-key encryption with registered keyword search," in *Proceedings of the European Public Key Infrastructure Workshop*, Pisa, Italy, September 2009.

[17] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in *Proceedings of the International Workshop on Information Security Applications*, Jeju Island, Republic of Korea, August 2004.

[18] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," *Information Sciences*, vol. 403, pp. 1–14, 2017.

[19] Z. Lv, C. Hong, M. Zhang, and D. Feng, "Expressive and secure searchable encryption in the public key setting," in *Proceedings of the International Conference on Information Security*, Hong Kong, China, October 2014.

[20] C. Hu and P. Liu, "An enhanced searchable public key encryption scheme with a designated tester and its extensions," *Journal of Computers*, vol. 7, no. 3, pp. 716–723, 2012.

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

[22] Z.-Y. Shao and B. Yang, "On security against the server in designated tester public key encryption with keyword search," *Information Processing Letters*, vol. 115, no. 12, pp. 957–961, 2015.

[23] L. Wu, B. Chen, S. Zeadally, and D. He, "An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage," *Soft Computing*, vol. 22, no. 23, pp. 7685–7696, 2018.

[24] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, Santa Barbara, CA, USA, August 1984.

[25] G. Di Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on Jacobi symbols," in *Proceedings of the International Conference on Cryptology in India*, Chennai, India, December 2007.

[26] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proceedings of the IMA International Conference on Cryptography and Coding*, Cirencester, UK, December 2001.

[27] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in *Proceedings of the International Workshop on Public Key Cryptography*, March 2009.

[28] M. Abdalla, M. Bellare, D. Catalano et al., "Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions," in *Proceedings of the Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 2005.

[29] D. Khader, "Public key encryption with keyword search based on K-resilient IBE," in *Proceedings of the International Conference on Computational Science and its Applications*, Glasgow, UK, May 2006.

[30] T.-Y. Wu, T.-T. Tsai, and Y.-M. Tseng, "Efficient searchable ID-based encryption with a designated server," *annals of telecommunications-annales des télécommunications*, vol. 69, no. 7, pp. 391–402, 2014.

[31] Y. Lu, G. Wang, J. Li, and J. Shen, "Efficient designated server identity-based encryption with conjunctive keyword search," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 359–370, 2017.

[32] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, May 2005.

[33] F. Zhao, T. Nishide, and K. Sakurai, "Multi-user keyword search scheme for secure data sharing with fine-grained access control," in *Proceedings of the International Conference on Information Security and Cryptology*, Seoul, Rebulic of Korea, December 2011.

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

[35] C. Wang, W. Li, Y. Li, and X. Xu, "A ciphertext-policy attribute-based encryption scheme supporting keyword search function," in *Proceedings of the International Symposium on Cyberspace Safety and Security*, Zhangjiajle, China, November 2013.

[36] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: verifiable attribute-based keyword search over outsourced encrypted data," in *Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, Toronto, Canada, May 2014.

[37] P. Liu, J. Wang, H. Ma, and H. Nie, "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, November 2014.

[38] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 715–725, 2016.

[39] Y. Yang, "Attribute-based data retrieval with semantic keyword search for e-health cloud," *Journal of Cloud Computing*, vol. 4, no. 1, pp. 1–6, 2015.

[40] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1274–1288, 2015.

[41] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1187–1198, 2014.

[42] H. Zhu, Z. Mei, B. Wu, H. Li, and Z. Cui, "Fuzzy keyword search and access control over ciphertexts in cloud computing," in *Proceedings of the Australasian Conference on Information Security and Privacy*, Auckland, New Zealand, July 2017.

[43] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attribute-based Keyword Search over Hierarchical Data in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 13, 2017.

[44] L. Cao, J. Zhang, X. Dong et al., "A based on blinded CP-ABE searchable encryption cloud storage service scheme," *International Journal of Communication Systems*, vol. 31, no. 10, p. e3566, 2018.

[45] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," *Journal of Cryptology*, vol. 26, no. 2, pp. 191–224, 2013.

[46] Y. Zhang and S. Lu, "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, November 2014.

[47] I. Kim, S. O. Hwang, J. H. Park, and C. Park, "An efficient predicate encryption with constant pairing computations and minimum costs," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2947–2958, 2016.

[48] Y. Zhang, Y. Li, and Y. Wang, "Secure and Efficient Searchable Public Key Encryption for Resource Constrained Environment Based on Pairings under Prime Order Group," *Security and Communication Networks*, vol. 2019, Article ID 5280806, 14 pages, 2019.

[49] Y. Zhang, Y. Wang, and Y. Li, "Searchable public key encryption supporting semantic multi-keywords search," *IEEE Access*, vol. 7, Article ID 122078, 2019.

[50] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, Taipei, Taiwan, December 2003.

[51] P. Yanguo, C. Jiangtao, P. Changgen, and Y. Zuobin, "Certificateless public key encryption with keyword search," *China Communications*, vol. 11, no. 11, pp. 100–113, 2014.

[52] T.-Y. Wu, F. Meng, C.-M. Chen, S. Liu, and J.-S. Pan, "On the security of a certificateless searchable public key encryption scheme," in *Proceedings of the International Conference on Genetic and Evolutionary Computing*, Fuzhou, China, November 2016.

[53] Q. Zheng, X. Li, and A. Azgin, "CLKS: certificateless keyword search on encrypted data," in *Proceedings of the International Conference on Network and System Security*, New York, NY, USA, November 2015.

[54] M. Ma, D. He, N. Kumar, K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 759–767, 2017.

[55] M. Ma, D. He, M. K. Khan, and J. Chen, "Certificateless searchable public key encryption scheme for mobile healthcare system," *Computers & Electrical Engineering*, vol. 65, pp. 413–424, 2018.

[56] Y. Lu and J.-G. Li, "Constructing pairing-free certificateless public key encryption with keyword search," *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 8, pp. 1049–1060, 2019.

[57] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, Espoo, Finland, June 1998.

[58] J. Shao, "Proxy re-encryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576–2587, 2010.

[59] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Proxy re-encryption with keyword search: new definitions and algorithms," in *Security Technology, Disaster Recovery and Business Continuity*, pp. 149–160, Springer, Berlin, Germany, 2010.

[60] X. A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, "Further observation on proxy re-encryption with keyword search," *Journal of Systems and Software*, vol. 85, no. 3, pp. 643–654, 2012.

[61] L. Guo, B. Lu, X. Li, and H. Xu, "A verifiable proxy re-encryption with keyword search without random oracle," in *Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security*, Emeishan, China, December 2013.

[62] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," *IEEE Transactions on*

Information Forensics and Security, vol. 11, no. 4, pp. 746–759, 2015.

[63] Y. Yang, X. Zheng, V. Chang, and C. Tang, "Semantic keyword searchable proxy re-encryption for postquantum secure cloud storage," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 19, p. e4211, 2017.

[64] Y. Shi, J. Liu, Z. Han, Q. Zheng, R. Zhang, and S. Qiu, "Attribute-based proxy re-encryption with keyword search," *PloS one*, vol. 9, no. 12, Article ID e116325, 2014.

[65] Y. Chen, Y. Hu, M. Zhu, and G. Yang, "Attribute-based keyword search with proxy re-encryption in the cloud," *IEICE-Transactions on Communications*, vol. 101, no. 8, pp. 1798–1808, 2018.

[66] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in *Proceedings of the International Conference on Pairing-Based Cryptography*, July 2007.

[67] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in *Proceedings of the Fourth International Symposium on Information, Computer, and Communications Security*, Sydney Australia, March 2009.

[68] X.-F. Wang, Y. Mu, R. Chen, and X.-S. Zhang, "Secure communication channel free id-based searchable encryption for peer-to-peer group," *Journal of Computer Science and Technology*, vol. 31, no. 5, pp. 1012–1027, 2016.

[69] Y. Miao, X. Liu, K.-K. R. Choo et al., "Privacy-preserving attribute-based keyword search in shared multi-owner setting," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, 2019.

[70] B. Zhu, B. Zhu, and K. R. Peksrand, "Providing predicate privacy in public-key encryption with keyword search," in *Proceedings of the 2011 IEEE International Conference on Communications (ICC)*, Kyoto, Japan, June 2011.

[71] S. H. Islam, M. S. Obaidat, V. Rajeev, and R. Amin, "Design of a certificateless designated server based searchable public key encryption scheme," in *Proceedings of the International Conference on Mathematics and Computing*, Haldia, India, January 2017.

[72] L. Wu, Y. Zhang, M. Ma, N. Kumar, and D. He, "Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things," *Annals of Telecommunications*, vol. 74, no. 7, pp. 423–434, 2019.