SCIENCE CHINA
Information Sciences

• REVIEW •

October 2022, Vol. 65 201301:1–201301:34
https://doi.org/10.1007/s11432-021-3393-x

A survey on cryptographic techniques for protecting big data security: present and forthcoming

Siqi LU[1,2*], Jianhua ZHENG[3], Zhenfu CAO[4,5,6], Yongjuan WANG[1,2] & Chunxiang GU[1,2]

[1]*School of Cyberspace Security, Information Engineering University, Zhengzhou* 450001, *China;*
[2]*Henan Key Laboratory of Network Cryptography Technology, Zhengzhou* 450001, *China;*
[3]*Institute of Security Technology, Beijing* 100191, *China;*
[4]*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai* 200062, *China;*
[5]*Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen* 518055, *China;*
[6]*Shanghai Institute of Intelligent Science and Technology, Tongji University, Shanghai* 200062, *China*

Received 17 June 2021/Revised 22 October 2021/Accepted 28 December 2021/Published online 22 September 2022

Abstract Big data drive multidimensional convergence and profound innovations among industries and provide novel ways of exploring the world. As they significantly create economic and social value, big data meaningfully impact the implementation and management of information security and privacy protection. Cryptographic technologies are used to protect the security and entire life cycle of big data. The demand for this technology is multiplied when the data are stored in the cloud. They are stored in the cloud in the form of ciphertext, and the driving requirement for data retrieval, sharing, and manipulation places the security of data at risk. The all-or-nothing approach of traditional cryptography systems cannot realize the release and processing of data information with flexible and increasingly fine granularity. Consequently, dealing with the relationship between privacy protection and data utilization, as well as navigating the blurry boundaries between subverting either plaintext or ciphertext, has become a research focus of the current cryptographic trend for protecting big data security. Presently, there are many studies designed to solve these limitations. First, security requirements and source encryption mode for future big data systems and applications are elaborated. Then, focusing on the practical security and functionality of the big data life cycle, including storage, retrieval, sharing, calculation, statistical analysis, and utilization, the research being conducted based on those functions is reviewed. For each cryptographic technology that meets the requirement of each type of big data security or application, security and efficiency comments and sufficient comparison analyses of cryptography schemes or protocols are provided; moreover, the current general problems and development trends are expounded. Because the current innovative research on cryptographic technology was primarily based on the development or improvement of a single solution, the study on the security of the entire big data life cycle from a holistic perspective is extremely limited. Finally, based on surveys and integration of cryptographic techniques, a compatible and comprehensive reference cryptographic architecture for big data security (Z-CABDS) is proposed, which can be used to guide each sub-direction to cooperate with each other to achieve the full life cycle security of big data. Moreover, certain challenges, open problems, and thoughts on future research related to the cryptography of big data security from the viewpoint of the entire big data life cycle are addressed, including views on information theory, the intersection and fusion of technologies, and new technology derivation, which aims to provide a good reference and inspiration for follow-up research.

Keywords big data security, cryptographic techniques, ciphertext-based data sharing and computing, authenticated encryption, functional encryption, homomorphic encryption, secure multi-party computing

Citation Lu S Q, Zheng J H, Cao Z F, et al. A survey on cryptographic techniques for protecting big data security: present and forthcoming. Sci China Inf Sci, 2022, 65(10): 201301, https://doi.org/10.1007/s11432-021-3393-x

1 Introduction

The advent of the Internet of Things (IoT) has led to the advancement of networking devices and their constituent data. By 2019, the total number of global IoT devices had reached 12 billion; it will reach 24.6 billion by 2025[1)]. According to Statista[2)], the total amount of global data reached 47 ZB in 2019, and

* Corresponding author (email: 080lusiqi@sina.com)

1) GSMA. The mobile economy 2021. 2021. https://www.gsma.com/mobileeconomy/.
2) Statista. Digital economy compass 2020. 2020. https://www.statista.com/news/digital-economy-compass/en.

it will reach 2142 ZB by 2035. With the rapid development of global interconnectivity and digitization, global data have exponentially grown, and humans have entered the era of big data.

The boost in computing power and the fast development of artificial intelligence have greatly enhanced the processing, analysis, and mining of large types of data. The attributes of big data have gradually expanded from the 5V characteristics of volume, variety, velocity, value, and veracity to those of multi-fusion, fast aggregation, and high value. The information and knowledge obtained from large-scale and high-quality data analysis are changing our lives and enriching the ways we explore the world. They have indeed driven multidimensional and deep integrations among industries. Data have become a most valuable resource, and their potential value in politics, economy, national security, and other aspects has created concern and attention globally. From the Obama Administration's "Big Data Research and Development Initiative" launched in 2012 to "Data Strategy 2020" released by the United States Department of Defense in October 2020, the USA has built a comprehensive strategy obtaining big data for political, economic, and military purposes. The US government aims to use big data in obtaining knowledge and strategy advantage, promoting the development and availability of public data, and improving public social services. They are also used in the transformation of the United States Department of Defense to a more data-centric organization while implementing the National Defense Strategy of data weaponization. Simultaneously, the British government launched their digital strategy and established the "Open Data Institute". The EU launched its "Open Data Strategy" and finally realized barrier-free information sharing for Pan-European member states. Australia released their "Public Service Big Data Strategy". Korea launched its national big data development plan that aims to train 1000 enterprises regarding big data and cloud computing. Thus, big data have become the basis for many nations to identify, judge, and meet the requirements of public value. Consequently, the conventional wisdom of data sovereignty and national security is evolving. As big data create large economic and social advantages, they pose new challenges to information security and privacy protection. Because of the increasing number of ubiquitous networks, harm now spreads faster and impacts more people. The destruction, leakage, and manipulation of data have a considerable impact on personal privacy, national security, social order, and public interest. From the worldwide blackmail attack, WannaCry, in 2017 to the privacy leaks of Facebook and Uber in 2018, the security risks of big data are monumental. The importance and sensitivity of data involved are directly related to the core interests of users, countries, and society.

In a cloud computing environment where data storage and processing resources are controlled by service providers, users require to control their data content and maintain ownership. As an important tool in protecting big data security, cryptographic measures must provide the first layer of protection both prior to its transfer to the cloud and during its storage in the form of ciphertext. These initiate security requirements and source encryption mode of big data application, as shown in Figure 1. However, the ciphertext of traditional encryption systems can be analyzed, mined, and utilized only after it is decrypted into plaintext, which consumes additional computing and communication costs. Based on new cryptographic technologies, the cloud realizes the sharing, calculation and processing of data on the basis of ciphertext without knowing anything information of the data. Hence, modern big data cryptography research focuses on the fine-grained flexible sharing and processing of ciphertext-based data. Different application requirements have come up with cryptosystems with different characteristics, such as searchable encryption (SE) for ciphertext-based data retrieval, functional encryption (FE) for ciphertext-based data sharing, and multi-party computing (MPC) protocol for ciphertext-based computing. Recent studies on this topic have shown significant theoretical and technical results on this topic.

Inspired by [1,2], this study comprehensively reviews the cryptography technologies from the practical requirements of big data storage and security, fine-grained data security sharing, and ciphertext-based data computing, while determining their essentials and the remaining problems to be solved. It summarizes multiple development statuses and analyzes their practical security and efficiency. Authenticated encryption and data integrity auditing technologies, which protect the confidentiality and integrity of big data during storage, are discussed. Group key agreements (GKA), broadcast encryption (BE), identity-based encryption (IBE), attribute-based encryption (ABE), proxy re-encryption (PRE), and FE are reviewed for fine-grained data sharing and access control. Regarding ciphertext-based retrieval and computing, attribute-preserving encryption and SE are outlined together with the homomorphic encryption and secure MPC techniques. For each cryptographic technology that meets the requirement of each type of big data security or application, we go through the background of the proposed technologies, expound sufficient security and efficiency comments, compare analyses of cryptography schemes or protocols, and summarize current general problems and development trends. After reviewing the status of various

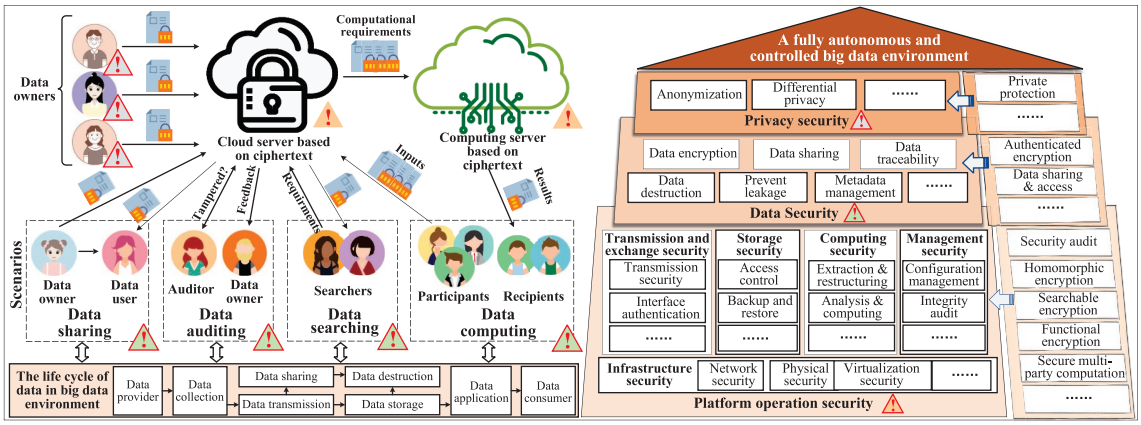

Figure 1 (Color online) Applications and security requirements of big data.

research sub-directions, we identified a problem: researchers are very extensive with their theoretical research on each sub-direction and have proposed multiple solutions; however, when these solutions are combined to solve the big data life cycle security, can it still be safe? Will there be security or efficiency issues in the convergence, combination, and coordination of the various schemes? Therefore, to realize the comprehensive application of schemes and to protect the security of the entire big data life cycle, we present the cryptographic architecture for big data security (Z-CABDS), a compatible and comprehensive reference cryptographic architecture for big data security. Moreover, certain challenges, open problems, and thoughts on future research related to the cryptography of big data security from the viewpoint of the entire big data life cycle are addressed, including the views on information theory, intersection and fusion of technologies, and new technology derivation, which aims to provide a good reference and inspiration for follow-up research.

2 Secure storage of big data

Cloud service providers (CSPs) often provide big data secure storage environments by applying access controls and cryptography technologies with database and system security applications. The goal is to protect the cloud storage system and stored data from illegal access, tampering, and retrieval by adversaries. As with most technologicals, the various implementations of cloud storage and security are driven by marketization. However, many incidents of privacy leakage demonstrate that market forces cannot account for all the risks imposed by service providers. Although service providers deliver their services based on the regulations, they attempt to remain aware of their users' privacy needs. Hence, cloud storage service providers are objectively considered honest but curious. Consequently, data encryption is generally applied at all phases of transfer, storage, and manipulation. Traditionally, efficient symmetric cryptographic algorithms are used to encrypt the data, and a public-key cipher is used to encrypt the symmetric key, thus providing us with a hybrid encryption model. However, the users' requirements for access to cloud services and big data management are rapidly increasing. The disadvantages of traditional hybrid encryption techniques (e.g., high communication costs and lack of flexibility in data sharing and computing) have been attracting considerable attention both academically and industrially. Therefore, for the various applications of big data, an encryption algorithm will often have attributes specialized to the situation, such as authenticated encryption for integrity verification, SE for ciphertext-based searching, PRE for point-to-point ciphertext-based sharing, ABE and FE for fine-grained sharing, and (fully) homomorphic encryption for ciphertext-based calculation. These technologies are explained in subsequent chapters. This chapter focuses on the research overview of authenticated encryption and integrity auditing for secure storage of big data.

2.1 Authenticated encryption

Confidentiality and integrity (authenticity) are important security attributes that must be guaranteed with the storage of big data. Authenticated encryption algorithms are created for the efficient protection of data confidentiality and integrity through symmetric cryptography. If performed well, the database

can resist passive (e.g., eavesdropping) and active attacks (e.g., unauthorized manipulation, modification, and destruction). Early authenticated encryption schemes used cryptographic algorithms to ensure data confidentiality and integrity via message authentication coding (MAC). Classic schemes included Encrypt-then-MAC (EtM), Encrypt-and-MAC (E&M), and MAC-then-Encrypt. However, only EtM is secure and was adopted by the Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission. Because EtM's encryption and authentication algorithms are completely independent, the costs are expensive and efficiency is low. To overcome this, authenticated encryption schemes, whose encryption and authentication algorithms generally share computing resources, have been proposed. In 2014, the National Institute of Standards and Technology initiated the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR competition) to collect and curate secure and efficient authenticated encryption schemes with broad application potential. Finally, in February 2019, the CAESAR competition selected six winning algorithms in three scenarios, such as ASCON [3] for lightweight application scenarios, AEGIS-128 [4] for high-performance application scenarios, and Deoxys-II [5] for defense in depth scenarios. ASCON is based on the sponge operation mode with a customized SPN permutation, the optimized s-box of which can resist side-channel attacks. Its lightweight design enables rapid hardware and software implementation. The AEGIS algorithm uses a number of 128-bit groups as the internal state for calculation. For example, AEGIS-128 updates the state for each step on the 128-bit group by paralleling five advanced encryption standard (AES) round functions without a key addition operation. Based on the AES round function and the tweakable block cipher, the Deoxys-II algorithm uses several sets of parameters to adjust the key and tweak sizes, which is accompanied by a good security margin for all sets of recommended parameters. Furthermore, during the CAESAR competition, a wealth of theoretical research results on authenticated encryption algorithms emerged (e.g., ACORN [6], OCB [7], COLM [8]). The encryption-mode-based COLM comprises two layers of parallelizable encryption connected by a linear mixing functionality. It resists nonce-misuse attacks, and its structure has proven releasing unverified plaintext (RUP) security [9].

Based on the CAESAR competition, the authenticated encryption designs resort under five categories (as shown in Table 1): block cipher, stream cipher, sponge structure, permutation, and compression function. The authenticated encryption mode design based on the block cipher originated from the one-pass mode proposed by Jutla [10]. Subsequently, multiple schemes have been proposed to address diverse practical requirements. For example, the RIV [11], based on the extended synthetic initialization vector (SIV) [12], is designed to resist nonce-misuse attack and is provably secure when RUP. XUBA [13], based on the 128-bit stream cipher, satisfies standard security and is resistant to algebraic, differential, time-memory-data trade-off, MAC forgery, and guessing attacks. The Galois/counter mode (GCM)-based instantiation algorithm GCM-RUP [14] achieves a general construction resisting RUP attacks by adding the tweakable block cipher (TBC). They provided proof of beyond-birthday-bound (BBB) security under the condition that the nonce is not misused. However, when processing each data block, most TBC-based authenticated encryptions with BBB security require two or more block encryption calls. On the basis of the combination of two TBCs, the XKX construction [15] having BBB security with improved efficiency is proposed. Moreover, the stream cipher-based TriviA [16] is presented, which is hardware friendly with high throughput and implements tag calculation via pairwise independent hashing. The pure OMD (p-OMD) [17], which is an OMD authenticated encryption algorithm variant [18], dispenses with the XOR MAC algorithm to improve execution efficiency without security loss, and the security proof is given under the standard assumption (pseudorandomness of the compression function). In 2016, Thomas and Yannick [19] proposed a provably secure reverse-tweakable authenticated encryption mode synthetic counter-in-tweak (SCT), which converted a tweakable block cipher into a random number-based authenticated encryption scheme. It ensures security up to the birthday bound in the strong nonce-misuse resistance sense; it is simple, parallelizable, efficient for short messages, and supportable of incremental updates of associated data. To achieve multiuser security in practical applications, Bellare et al. [20] provided a formal definition of multiuser indistinguishability and key recovery for the authenticated-encryption mode GCM for the transport layer security (TLS) 1.3 protocol and analyzed the multiuser security advantages of the authenticated encryption mode randomized GCM (RGCM), thus comparing it with GCM under the perfect-block cipher assumption. They proposed a more concise optional authenticated encryption mode (named XGCM) and demonstrated that it had higher multiuser security and the same efficiency as RGCM. In the same year, Reyhanitabar et al. [21] analyzed the online encryption and decryption efficiency limitations of the robust authenticated encryption scheme proposed by Hoang et al. [22] in 2015, thus proposing the nonce-based variable-stretch authenticated encryption scheme,

Table 1 Comparison of authenticated encryption schemes

Scheme	Cryptographic primitive	Efficiency	Attack resistance	Properties
COLM [8]	block cipher	Pipelined hardware implementation	nonce misuse	RUP
ASCON [6]	permutation function	Soft- and hardware evaluation	side channel Differential and Linear	Lightweight small state size
RIV [11]	block cipher	Software efficient: 1.5 CPB on Haswell	nonce misuse	Provable security subtle AE (SAE) modular framework
XUBA [13]	stream cipher	No efficiency evaluation	algebraic attack differential attack time-memory-data trade-off attack forgery and MAC guessing attack	Strict avalanche criterion (SAC) collision test
XKX [15]	TBC	One-pass efficient	BBB	Online and parallelizable
TriviA [16]	stream cipher	Hareware performance evaluation 3.8 times better than ASCON	guess-then-find attack Cube-Attack Polynomial Density	Small hardware footprint provable security
SCT [19]	TBC	Efficient for small messages	nonce misuse BBB	Close-to-optimal security simple and parallelizable
XGCM [20]	block cipher	More simple less sessions	threat of mass surveillance	mu (multiuser) indistinguishability mu kr (key recovery) security modular design
nvAE [21]	nonce-based	Not impact significantly	nonce misuse generic forgery attack	Key-equivalent separation by stretch (kess) robustness and online encryption provably achievable
AEZ [22]	AES round function	Software efficient: 0.7 cpb on Haswell	nonce misuse pseudorandom-injection (PRI) security	Provable security prove-then-prune robustness
SIVAT [23]	nonce-based	No efficiency evaluation	side channel protocol leakage nonce misuse	Provable security robustness
Feistel construction [24]	PRI	Only 3 round complexity	key-dependent message attacks related-key attacks nonce misuse	Universal composability (UC) security robustness
FRIET [25]	FRIET-P pseudorandom	Soft- and hardware evaluation	leakage attack: fault/side channel Invariant attack Differential and Linear Propagation	Full diffusion lightweight

which satisfies the key-equivalent separation-by-stretch property. In 2017, Barwell et al. [23] proposed an anti-leakage and anti-misuse authenticated encryption scheme based on a leakage-resilient pseudorandom function and provided a secure and efficient pairing-based instantiation. In 2018, Barbosa and Farshim [24] combined non-differentiable attributes with authenticated encryption to develop a provably secure authenticated encryption scheme based on the Feistel structure, which reduced the complexity of at least six rounds of block ciphers to three. In 2020, Simon et al. [25] proposed a new fault-resistant iterative extended transformation (FRIET) with permutation, which was resistant to fault attacks. They then developed a duplex authenticated encryption FRIET based on it. They analyzed the execution efficiency of the scheme, tested its fault detection capability, and completed a leakage assessment.

The security proof method of the authenticated encryption mode is primarily based on the provable security theory. Assuming that the underlying encryption algorithm is a strong pseudorandom permutation, the security of the authenticated encryption mode is regulated to the algorithm's security. The analysis of authenticated encryption primarily revolves around mixed-integer linear programming technology, which is used to search for block-cipher differential and linear paths. It borrows techniques from the integral distinguisher technology based on bit-level segmentation characters [26] and cube attacks [27]. Moreover, studies on candidate algorithms have been performed for the CAESAR competition, including those of the differential characters of the state-update function and the internal state collision analysis for the MORUS algorithm, differential discrimination cryptanalysis, divide-and-conquer cryptanalysis [28], and differential and rotation cryptanalysis [29] on MORUS-640. The ASCON algorithm includes differential cryptanalysis, impossible differential cryptanalysis, linear character cryptanalysis of its permutation, differential paths generated by collisions based on sponge function-like structures, round-key cube attacks, and differential linear attacks [30]. For the PRIMATEs algorithm, there are differential character cryptanalyses of permutations, linear character cryptanalyses, collision-generating path analyses, impossible differential path analyses, diagonal fault analyses of the authenticated permutation-based encryption mode, and key-recovery cube-like attacks on the HANUMAN mode [31]. In term of the GCM mode, a RUP attack was proposed [32]. In response to the above mentioned cryptanalysis research, multiple resistance schemes have been proposed. In 2016, Bost and Sanders [33] reported a collision of tweakable encryption in the OTR mode and developed attacks on its confidentiality and authentication. Then, they

proposed a collision-resistant construction scheme against the attack. Bay et al. [34] analyzed the security of the encrypt-linear-mix-decrypt (ELmD) authenticated encryption mode based on a block cipher submitted at CAESAR during the second round. They demonstrated common-forgery and key-recovery attacks on the scheme. In 2018, Dodis et al. [35] proposed the sender binding-security problem for the attachment-franking scheme of Facebook and identified that the cause of the problem was that the authenticated encryption did not make a binding commitment to the message content. Consequently, they proposed a new cryptographic primitive called "encryptment" based on hash-function chaining, which, in turn, was based on the ccAEAD scheme [36]. Moreover, they developed an extremely efficient committing authenticated encryption scheme.

Summary and prospect. Based on the overview of the authenticated encryption mentioned above, it can be concluded the following. (1) The CAESAR competition has developed a solid foundation theoretically and practically to improve and apply authenticated encryption. The algorithms introduced in the competition provide important references for designing authenticated encryption. Most of the current research focuses on the security analysis and optimization of the algorithms in the CAESAR competition. (2) The focus of authenticated encryption security is primarily on RUP, BBB, and nonce-misuse security. The analysis methods primarily cover the cube, distinguishing, forgery, zero-sum distinguisher, integral, and key-recovery attacks. (3) Cryptography primitives and encryption modules with special properties need to be examined as the key to algorithm innovation to design a new scheme for authenticated encryption. However, methods based on the ecosystem of mature algorithms can help improve the efficiency of software and hardware implementation; e.g., Intel AES New Instructions (AES-NI) is an important prerequisite for the AEGIS algorithm to be efficient. (4) The current progress informs that authenticated encryption will evolve into a method that will ensure the confidentiality and integrity of big data storage, which has considerable application feasibility and development prospects. Although there have been many studies about authenticated encryption recently, many unsolved problems still remain regarding the protection of big data security in practical applications. (1) In terms of security, current authenticated encryption methods still have open problems, such as birthday-bound-attack resistance, strong model security, multi- and related-key security, multiuser security, leakage resistance, and nonce-reuse/misuse resistance security. (2) As for implementation efficiency and diverse practical applications, the design of authenticated encryption requires considering multiuser scenarios, computing and storage costs, application environments, and software/hardware implementation. (3) The generality of algorithm design will gradually decrease, and personalization and specialization will increase because of the diversification of application scenarios. For instance, suitable lightweight authenticated encryptions in resource-constrained devices or big data application environments will be a focus of future research.

2.2 Integrity audit for big data storage

Usually, cloud storage service providers offer security and reliable storage services for data providers and users; however, because of internal adversaries and operational errors, the destruction, manipulation, and loss of cloud storage data cannot be completely avoided. Furthermore, providers may delete or modify rarely accessed data for their own benefit. Therefore, to ensure the confidentiality and integrity of cloud data, users require to both encrypt data ahead of time and they must conduct regular integrity audits. MAC was originally used to protect storage integrity verification. However, it required additional storage in the cloud environment and high calculation costs. Although the abovementioned authenticated encryption can simultaneously guarantee data confidentiality and integrity, users must download the encrypted data to a local machine to confirm whether they have been tampered with or destroyed during decryption. To efficiently audit the integrity of cloud storage data, Ateniese et al. [37] proposed in 2007 two schemes under the provable data possession (PDP) model. Based on random sampling, users no longer had to download cloud data and randomly select blocks to achieve probabilistic integrity auditing; thus, they reduced computing and communication costs. The scheme was then extended to support public verifiability and third-party integrity. Juels et al. [38] proposed a proof-of-retrievability (POR) scheme, which both verified data integrity, and ensured data retrievability. Shacham and Waters [39] extended the scheme to support public audits. Then, PDP and POR have become mainstream technologies for auditing the integrity of big data cloud storage, and their scalability allows third-party auditor (TPA) integrity checking. This model has become an important part of big data-related security research.

As shown in Figure 2, based on the classic PDP and POR schemes, follow-up studies on the security analysis and design of diversified schemes are conducted, which aims to expand functions and improve

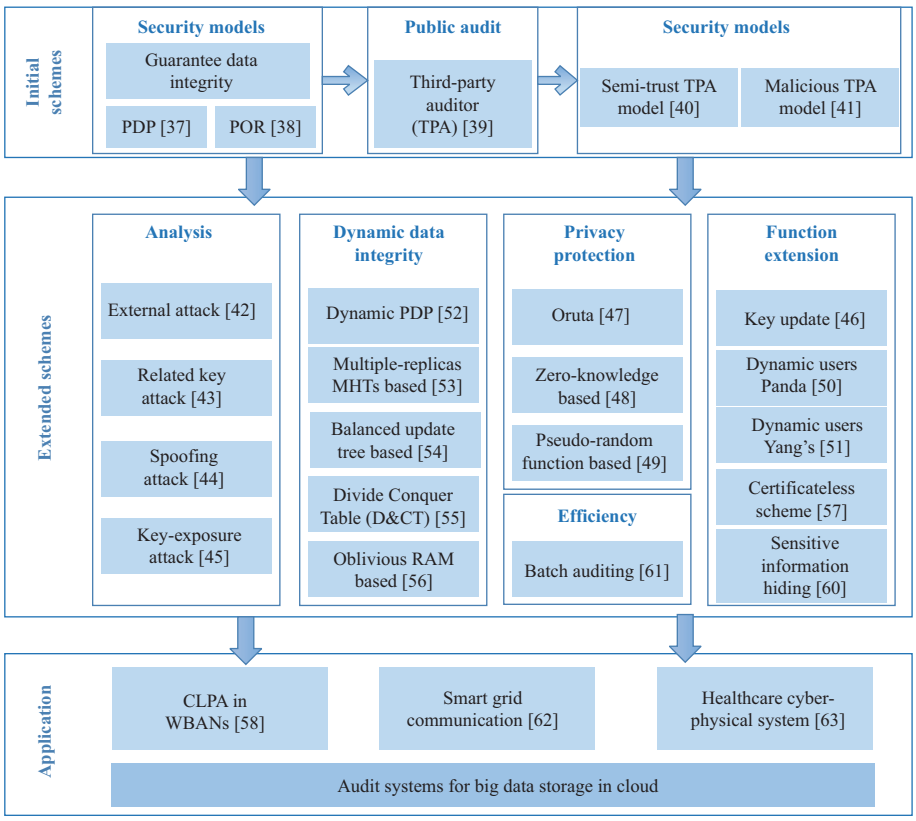

Figure 2 (Color online) Integrity audit for big data storage.

security and efficiency. First, from a trusted third party, the security model has advanced into a semi-trusted or malicious third party. Wang et al. [40] proposed a public auditing scheme using a semi-trusted TPA model based on random hidden patterns. The scheme realized both batch checking of data integrity via TPA and ensured that TPA could not reveal data content. Xu et al. [41] and Worku et al. [42] proposed malicious CSP attacks and external attacks and provided their optimization schemes. Second, related-key, key-exposure, and spoofing attacks were reported and solved, and extended properties were considered, such as privacy preserving, certificateless public auditing, sensitive information hiding, and key updates. Cui et al. [43] discovered a related key attack on the scheme of Shacham et al. [39] and proposed a secure and efficient public POR audit. Liu et al. [44] proposed a spoofing attack in which a CSP could pass the auditing of TPA even if all user data were deleted. Then, they provided a solution to this limitation. Yu et al. [45] proposed the first key-exposure resistance audit scheme. Unfortunately, most key-exposure resistance audit schemes require the client to update secret keys every time period, inevitably giving the client new local burdens. To avoid this limitation, Yu et al. [46] proposed a new paradigm, which is called cloud storage auditing with verifiable outsourcing of key updates having minimal impact on the client. Because privacy protection is often as important as attack protection, the first privacy-preserving public auditing scheme was Oruta [47], which exploited ring signatures to compute verification metadata and realized multiple auditing tasks simultaneously. To achieve security and efficiency improvements based on Oruta, researchers subsequently proposed privacy-preserving remote data integrity auditing based on zero-knowledge privacy and pseudorandom functions [48,49]. In addition to protecting the users' privacy, the design of the schemes considers dynamic users. Based on the idea of proxy re-signatures, Panda [50] was a public auditing scheme for shared data with efficient user revocation, which was able to support batch auditing by simultaneously verifying multiple auditing tasks. Because Panda recalculates the authorization information of all users after the new user joins in order for the user's malicious behavior to be traced to the source, its verification overhead is relatively large. In response to this limitation, Yang et al.'s solution [51] used a group manager to generate authenticators, used two lists to record the members' modification, and achieved data privacy using a blind signature technique, thus finally forming a more efficient scheme supporting identity privacy protection, identity traceability, and malicious user behavior location. Third, in addition to integrity auditing of static data, for practical applications, there is an

urgent requirement for public auditing of dynamic data integrity after data modification, insertion, and deletion. However, the initial lightweight update scheme [52] did not efficiently support data insertion operations. Liu et al. [53] realized complete dynamic data updates and block index authentications based on multiple-replica MHTs. The abovementioned dynamic schemes only operated at the block level and restricted the location of data inserted into a file to fixed block size. To achieve fine-grained dynamic data integrity auditing more efficiently, follow-up schemes [54, 55] based on balanced update tree and divide-and-conquer tables (D&CTs) have been proposed, which aims to break through the restriction of block indexing during data updates by designing novel data structures. Moreover, to prevent the server from identifying and deleting several codeword symbols that belong to any single data block when they are being accessed by the client, Cash et al. [56] used oblivious RAM to hide where the various codeword symbols for any individual data block are stored on the server and proposed a safer dynamic POR scheme. Finally, to get rid of the cost of certificate management in the PKI system, a certificateless scheme [57] was proposed, and He et al. [58] proposed an efficient certificateless public auditing (CLPA) scheme, which was used to address the issue of integrity in cloud-assisted wireless body area networks (WBANs). To avoid incorrect or incomplete response services, the cloud service selection verification (CSSV) scheme and MMBcloud-tree index structures [59] were proposed to determine illegal acts by corrupted or semi-trusted cloud proxy brokers. Shen et al. [60] proposed a remote data integrity audit system with sensitive data hiding using the sanitizer module. Sanitizing sensitive data or files can realize remote auditing and sharing of sensitive data. Yang et al. [61] provided a batch audit scheme based on the short signature and sequence-enforced B+ hash tree structures to improve the audit efficiency and to support dynamic operations and transparent batch auditing.

Summary and prospect. The following results can be concluded from the overview of the abovementioned integrity audit the following. (1) PDP and POR have become mainstream technologies for auditing the integrity of big data cloud storage. Most studies focus on designing customized audit schemes for diversified application scenarios to pursue functional and security extensions such as dynamic data auditing, dynamic user management, privacy preservation, and sensitive data protection. For example, there is remote data auditing scheme with sensitive data hiding to satisfy sensitive data protection requirements or a dynamic auditing scheme for dynamic users with dynamic data operations. (2) Several studies demonstrated that efficiency improvement was achieved through lightweight scheme designs, batch auditing, and proxy auditing. Certain lightweight solutions have been used in the field of smart grids and medical systems [62, 63]. The future development of integrity audit technology in big data application scenarios primarily includes two directions the following. (1) The analysis and design of current schemes still have open problems such as the discovery and defense of attacks, the design of dynamic data integrity audit schemes, privacy-preserving audit schemes, or audit schemes with special properties, and others. (2) Another important research direction is to design customized big data integrity audit schemes for specific application scenarios to satisfy the specific application or security requirements of multiple data structures.

3 Flexible and fine-grained sharing of ciphertext-based data

Users store data on the cloud and share them with others as required, which reflects a basic service provided by CSPs. The data sharing scheme based on access control technology is based on the condition that the CSP is credible and has access control to all plaintext data. The data sharing problem in an honest cloud storage system can be solved only by authentication and access control technologies. However, CSPs are honest but curious. In other words, if the CSP wants to know the user's private information, the user's privacy may be lost; therefore, the user's sensitive data must be encrypted before being uploaded. Obviously, ciphertext-based data in the cloud challenges modes of traditional access control and sharing. Secure data sharing must both ensure that users use cloud storage services safely and transparently, and they must flexibly share ciphertext-based data as per the wishes of the data owner. Based on the application scenario, ciphertext-based data sharing can be divided into one-to-one and one-to-many sharing models, and data owners can share data with one visitor or many on demand. Many encryption algorithms, such as virtual private networks (VPNs) based on protocols, hybrid encryption, identity-based encryption, PRE, GKA, BE, ABE, and FE, meet this demand.

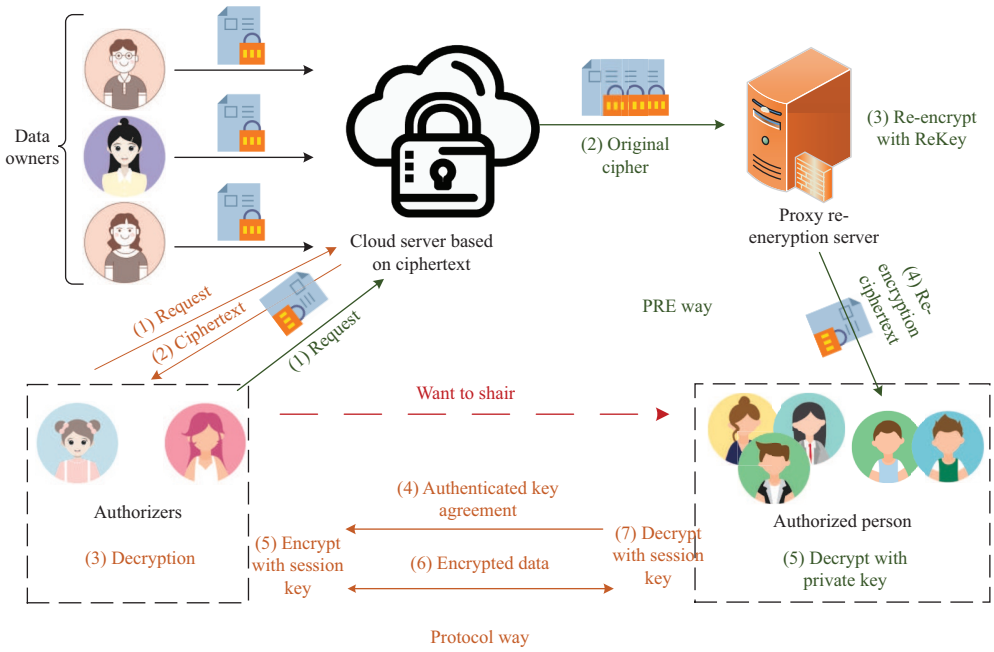

Figure 3 (Color online) One-to-one ciphertext-based data sharing.

3.1 One-to-one ciphertext-based data sharing

As shown in Figure 3, one-to-one ciphertext-based data sharing can be divided into direct and indirect types, which are implemented using VPNs based on protocols, hybrid encryption, identity-based encryption, PRE, and others. Cryptographic protocols usually establish one-to-one secure encryption tunnels via online interaction, and they directly share ciphertext and symmetric encryption keys through the tunnel. This scenario is suitable for one-to-one online data sharing at a high security level. Because each owner-visitor pair must generate a shared symmetric key and perform an encryption operation, this scheme is more secure but less flexible. The primary development trend of cryptographic protocols lies in the pursuit of tight security protocols and smaller computing and communication overhead [64]. Strictly, using cryptographic protocols to achieve data sharing differs from the ciphertext-based sharing scenario in the cloud storage environment; thus, it will not be discussed here. Another traditional ciphertext-based data sharing method (i.e., hybrid encryption) realizes the sharing of ciphertext-based data by managing visitor rights of the symmetric key by key distribution schemes. Hybrid encryption uses symmetric encryption to encrypt data and public-key encryption to encrypt the symmetric key. The key distribution scheme is used to control the access authority of data by controlling the distribution of the symmetric key. Recently, the proposed key distribution systems include group key distribution [65], lightweight key management [66], and quantum key distribution schemes [67]. To facilitate key management, researchers often use identity-based encryption rather than public-key encryption to construct sharing schemes [68, 69]. However, the method based on hybrid encryption or identity-based hybrid encryption shares data by sharing the symmetric encryption key of the data owner. Therefore, the symmetric key and original ciphertext must be updated each time to ensure confidentiality. This causes an increase in the number of symmetric keys and encryption operations as the number of visitors grows, thus increasing storage and computing costs to data owners and CSPs.

PRE [70] is an encryption scheme in which a semi-honest proxy server can convert the cipher of a data owner into a cipher that can be decrypted by a target visitor without obtaining any plaintext information. Thus, the proxy server is entrusted by the delegator to convert the ciphertext into the authorized party without decryption, in which the converted ciphertext can be decrypted by the authorized party's private key. This single-hop PRE realizes one-to-one data sharing based on ciphertext. Currently, most PREs use single-hop re-encryptions; however, the multi-hop PRE scheme is more practical. There have been multiple studies on PRE scheme designs and applications: certain studies were based on quantum-resistant learning with errors (LWE); some were designed for the pursuit of forward security, collusion

attack resistance, or chosen ciphertext attack (CCA) security; and some were applied in multi-hop or multiuser scenarios. In particular, David et al. [71] studied and formalized the forward-secrecy property of PRE. They proposed a forward secure PRE structure with provable security and instantiated a forward secure PRE scheme. In addition to examining the forward security property for auditing the behavior of malicious proxies participating in collusion attacks, Guo et al. [72] proposed the concept of accountable proxy re-encryption (APRE) with a judgment algorithm that determines whether the proxy is participating in a collusion attack. Finally, a noninteractive APRE scheme was instantiated with proof of CPA security under the standard model, and a CCA security extension was provided. Moreover, IBE and ABE have been added to realize decryption authority conversion based on the given identity or attribute structure, which can be used to flexibly select re-encryption agents. Thus, the access authority of visitors can be changed without decryption. To realize the ciphertext transformation from one identity to another, Green et al. [73] first proposed identity-based PRE, which is noninteractive and allows multiple re-encryptions. IB-BPRE [74] was proposed to solve the limitation of a large number of re-encryption keys in a mass message scenario. This converts the ciphertext of the delegator into the ciphertext of a group of delegates. In addition to broadcast PRE schemes, attribute-based PRE (ABPRE) [75] was proposed to share ciphertext-based data in a mass-message scenario. The agent converts the ciphertext under one access policy to ciphertext under another access policy. The flexibility of the proxy authorizer was enhanced to adapt to additional application scenarios when performing the re-encryption process. For example, Liu et al. [76] proposed a multi-conditional proxy broadcast re-encryption (MC-PBRE) scheme for file sharing systems to control the conversion conditions of proxy re-encryption flexibly. Fang et al. [77] presented a conditional proxy broadcast re-encryption approach with a fine-grained policy (CPBRE-FG), the re-encryption key of which is generated by an access tree and the ciphertext by a condition set. The proxy implements the ciphertext conversion, if and only if, the ciphertext condition set satisfies the access tree. The important revocation of dynamic users may cause heavy computing tasks for the data owner. Therefore, Ge et al. [78] proposed a revocable identity-based broadcast proxy re-encryption (RIB-BPRE) scheme, with a proxy that can revoke a set of delegates designated by the delegator by invalidating their re-encryption keys. PRE successfully solves the limitation of ciphertext-based data being shared via semi-trusted third parties, and it has been extensively used in social networks [79], media subscriptions [80], and medical information systems [81]. However, the establishment, storage, and management of re-encryption keys on the re-encryption proxy server may incur huge storage and computational costs, thus creating efficiency considerations in the big data environment for massive data and users.

3.2 One-to-many ciphertext-based data sharing

One-to-many ciphertext-based data sharing can be realized using a group key distribution scheme in which multiple visitors share the same encryption key, or via ABE [82] or FE [83], as shown in Figure 4.

The former primarily includes GKA and BE. The GKA protocol provides that multiple users establish the same group key in a public network, and group members can use the shared key for secure communications. The existing Burmester-Desmedt protocol [84] requires only two rounds of interaction to achieve group key establishment. However, it is increasingly difficult to realize the flexible joining and withdrawal of group users, and the change of group members must call the protocol again to establish a new group key. Although the dynamic GKA scheme [85, 86] solves the problem of dynamic group membership, the restriction that the data owner must be in the same group with the data visitor cannot be avoided. Thus, multiple GKAs are required for data sharing with visitors in different groups, which results in plenty of communication costs. The asymmetric GKA (AGKA) [87, 88] protocol enables multiple users to obtain a shared group encryption key through negotiation, and each user has a decryption key to use in establishing a process requiring only one round of interaction. The advantages of offline key establishment, forward security, and white-box tracking of malicious users can be realized. Attribute-based AGKA protocols [89] and identity-based AGKA [90, 91] have been examined to improve the flexibility and reduce key management overhead. BE enables data owners to safely send data to multiple visitors on public channels, which requires a trusted third party to generate public parameters and a private key for each user. The sender can encrypt and generate a ciphertext that is only decrypted by a prespecified combination of visitors. After BE is proposed, research hotspots may include improving the scheme efficiency, adaptive security, and provable secure, and there were rich research results [92–94]. Unfortunately, researchers have discovered that in BE schemes, particularly in identity-based ones, the

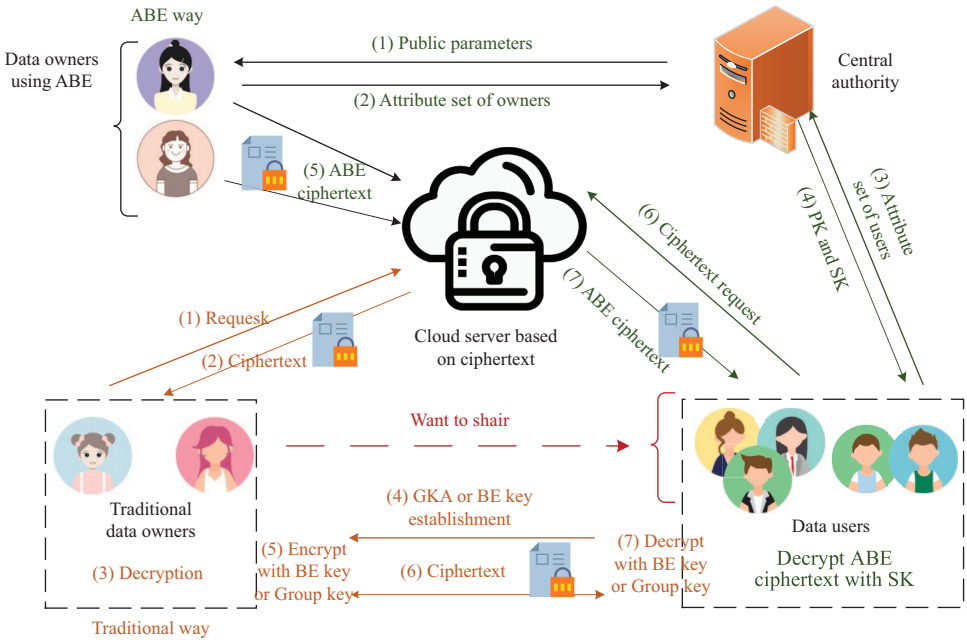

Figure 4 (Color online) One-to-many ciphertext-based data sharing.

identity information of any authorized person can often be learned by any other authorized person in the ciphertext. Hence, the privacy of data visitors is at risk; therefore, anonymous BE [95] was proposed to solve this limitation to protect the privacy of data receivers. CCA secure and complete anonymity efficient BE schemes were then proposed using the random-oracle model [96]. To explore new anonymous BE schemes, Boneh et al. [97] reported the possibility of solving the anonymity problem of the BE scheme using multilinear mapping and indistinguishability obfuscation. Subsequent research has focused on anonymous and IND-CCA-secure BEs under the adaptive security model such as BEs with weak robustness [98], privacy-preserving fully anonymous attribute-based BEs (ABBEs) with a constant-size secret key [99], adaptively secure BEs in standard model [100], and identity-based BEs (IBBEs) with shorter decryption keys [101]. Although GKA and BE schemes can meet the requirements of data owners who require to safely share data with multiple data visitors, the existence of massive users in the big data scenario increasingly demands flexibility and autonomy of the data owner's sharing authorization, security, and efficiency while supporting the rapid management and revocation of visitor permissions. Generally, GKA and BE must be called for each sharing opportunity, and the joining and revoking of group users and the establishment and maintenance of broadcast keys mostly require online computations of users without using cloud computing resources. Consequently, the expense of online communication is relatively high, and algorithm flexibility is low. Furthermore, these are essentially plaintext-based data sharing solutions, which differ from the ciphertext-based data sharing scenario in the big data cloud storage environment.

As a typical FE scheme [83], ABE [82], which essentially binds the decryption authority in the encryption key or ciphertext, provides another feasible way to realize one-to-many ciphertext-based data sharing. In ABE schemes, the data owner's ciphertext or encryption key depends on the corresponding attribute set; thus, the ciphertext can be correctly decrypted only when the user's attributes meet the attribute structure of the ciphertext or encryption key, which corresponds to ciphertext-policy (CP) ABE [102] and the key-policy (KP) ABE [103]. Recently, Cao [104] proposed the "channel security + X" model, where X includes security attributes (e.g., traceable, revocable, and multi-institutional). This indeed realizes fine-grained ciphertext access control.

In terms of traceable ABE, Liu et al. [105] provided the first CP-ABE that supported both high expressiveness and white-box traceability. This type of traceability informs us who the malicious users are and who leaked the keys. This scheme achieves adaptive security under the standard model, thus allowing an arbitrary monotonic access strategy, and the size of the ciphertext has a linear relationship

with the size of the ciphertext access strategy. However, the solution must maintain a list of recorded users to achieve white-box traceability. When the number of users gradually increases, the maintenance of the user list will become a bottleneck in the actual application. Liu et al. [106] proposed the first ciphertext-policy ABE that supported both high expressiveness and anti-collusion black-box traceability. As a black-box traceable ABE resistant to collusion attacks, the ciphertext size of the scheme reached the best level, which has only a sublinear relationship with the total number of users. Subsequently, Ning et al. [107] provided an efficient black-box traceable ciphertext-policy ABE with shorter ciphertext, anti-collusion, anti-adaptability key, and a fixed-strategy decryption black box. There were two limitations in the existing traceable multi-authority CP-ABE schemes, namely, a small universe and less expressiveness. The former restricts the attribute fixed time at system setup and attribute space to a polynomial size. The latter presents a contradiction between the expressiveness of access policy and the efficiency of the scheme. In response to the abovementioned limitations, Zhang et al. [108] proposed an efficient traceable large universe multi-authority CP-ABE scheme, in which policies can be expressed as any monotone access structures, and the tracing process does not require a central authority (CA) or an identity table.

In terms of revocable ABE, Liang et al. [109] proposed the first multipurpose one-way attribute-based PRE scheme in 2009. Based on the authorization, the complete key revocation from one access control strategy to another was effectively realized. Subsequently, Qian et al. [110] proposed a revocable ABE scheme without authorization, which aroused the interest of Sahai et al. [111] who then proposed another revocable ABE scheme based on a binary tree. Their scheme set each user to be related to the leaf node of a binary tree, thus making the number of key updates logarithmically related to the number of users and adding the nature of "ciphertext proxy" to achieve efficient key revocation. To solve the key escrow problem, Yang et al. [112] proposed two efficient multi-authority access control schemes that support attribute revocation for cloud storage and provided a security proof under the random oracle model. Li et al. [113] solved the user revocation problem by updating the user key and used outsourcing calculation to reduce the local calculation complexity. To address the primary efficiency drawbacks that ABE lacks an efficient and practical user revocation mechanisms, the binary tree method was deprecated because of its periodical inefficient decryption key update, and the first cloud server-aided revocable ABE (SR-ABE) scheme was presented [114] in which almost all workloads of users incurred by the user revocation were outsourced to an untrusted server; moreover, each user only required to store a private key of the constant size. However, it suffered from local decryption key exposure (DKE) attacks, and the CSP in its security model could not be fully compromised by an adversary. Thus, the security model was enhanced, and a dual framework for server-aided revocable ABE was proposed [115] without impacting the efficiency in which the update keys were distributed to local users. Furthermore, a generic construction of SR-ABE [116] that can transform a revocable ABE (RABE) scheme to an SR-ABE scheme was obtained, and the operational overheads of users could be outsourced to an untrusted server, thus greatly reducing the users' storage and computation cost.

In terms of multi-institution ABE, Chase [117] proposed a scheme for multi-authority organizations (MA-ABE), which allows any number of independent authorities to manage attributes and distribute keys. However, the trusted CA in their scheme still decrypted all ciphertexts. To avoid relying on a fully trusted CA, many MA-ABEs [118–120] were studied and designed in which multiple authorities are introduced, and each authority is responsible for issuing a piece of a user's secret key associated with a category or domain of attributes. To address the expressiveness and CA problems with the existing MA-ABE schemes, Okamoto et al. [121] proposed the first decentralized multi-authority ABE (DMA-ABE) scheme with fully decentralized processes for general relations, which supported non-monotone access structures combined with inner-product relations. Apart from the setting of a parameter for a prime order bilinear group and a hash function, no CA exists and no global coordination is required. Moreover, they presented the first decentralized multi-authority attribute-based signature (DMA-ABS) scheme for the abovementioned general relations, and its fully secure, adaptive-predicate unforgeable, and perfectly private method was proven in a decentralized multi-authority (DMA) security model.

In terms of practicability and application, researchers proposed a fine-grained anonymous CP-ABE scheme [122], a searchable CP-ABE scheme [123], an attribute-based PRE [124], an ABE for circuits [125], and others. ABE can be used for efficient and secure data sharing and access control in different types of cloud scenes, such as multilevel hierarchical ABE for file sharing [126], attribute-based framework in vehicular ad hoc networks (VANETs) [127, 128], and privacy-preserving white-box traceable MAABEs with revocation for personal health records (PHRs) in e-healthcare cloud [129, 130].

FE is a generalized extension of (anonymous) identity-based encryption, ABE, hidden-vector encryp-

tion [131], inner product encryption [132, 133], and predicate encryption (PE) [134, 135]. In terms of the FE scheme of function $F(\cdot,\cdot)$, the CA generates a private key for the user as per a master private key. After receiving the encrypted ciphertext of data x, the user having the private key, sk_k, can only obtain $F(k,x)$, but they cannot calculate any information about data x. Regarding the FE applied to access control, decryption keys are associated with functions, and the FE contains three entities: a key generation center, an encryptor, and a decryptor. $F(X,Y)\rightarrow\{0,1\}$ is a binary Boolean function defined on (X,Y), where X is the ciphertext index space and Y is the key index space. A pair of public and private keys, MPK and MSK, is generated when the system is established, and the encryptor encrypts the message M, based on MPK and index X. The important generation center generates the decryptor's private key as per MSK and index Y of the data visitor. Only when $F(X,Y)=1$ will the decryptor successfully operate. Identity-based encryption is a special case of FE in which the ciphertext index X is the user identity and the key index Y is the user identity. When $X=Y$, $F(X,Y)=1$, and thus decryption is successful. Similarly, ABE is another special case of FE, in which the ciphertext index X is an access structure (i.e., a collection of n-variable Boolean functions) and the key index Y is a user attribute (i.e., a collection of n-bit strings). When the user's attribute meets the access structure required by the encryptor, $F(X,Y)=1$, and the decryption is successful. To reduce the computational overhead of verifiability testing for CCA-security predicate encryption, Nandi et al. [136] proposed a delegation-based conversion from the ABE algorithm to PE algorithm, which is suitable for subclasses such as (hierarchical) inner-product PE. To resolve both privacy and usability requirements in multiple application scenarios, Naveed et al. [137] proposed controlled functional encryption (C-FE), which inherits the function of FE and requires the user to send a fresh key request to the authority every time the ciphertext function value is requested. Efficient instantiation is provided by combining the CCA2 secure public-key encryption and garbled circuit. Subsequently, Ambrona et al. [138] reported that Naveed's work supports only one instantiation for linear functions over data supplied by a single data owner. Therefore, they extended the C-FE scheme to a multi-authority C-FE (mCFE) that assigns the trust, or role of authority, to multiple parties and can calculate the quadratic function of multiuser data. In addition to the indistinguishability obfuscation (IO)-based and LWE-based FE schemes under the standard model, Bitansky et al. [139] confirmed that, in the presence of subexponentially secure public-key encryption, subexponentially secure secret-key functional encryption can be used to develop IO schemes. That is, secret-key functional encryption can become a bridge for developing IO schemes from encryption schemes. Compared with the work of Lin [140], the dependence on the difficult problem is weakened from the LWE assumption to any plain public-key encryption. Also interested in Lin's work, Cho et al. [141] conducted a security analysis of Lin's FE based on noisy multilinear maps that calculate polynomials of any degree. They reported an FE polynomial-time attack on each noisy multilinear map.

Summary and prospect. In view of the demand for privacy protection and data utilization of massive numbers of users, data owners must have sufficient autonomy and flexibility for ciphertext-based data in the cloud. Indeed, there are multiple cryptographic solutions for the fine-grained sharing of ciphertext-based data in different application scenarios. Therefore, mastering the functions, characteristics, and application scopes of various solutions is important to realizing big data sharing using cryptography technology. The following can be concluded from the overview of the research on big data sharing. (1) In scenarios where the frequency of data sharing is not high and the scope is not large, the security requirements are high, and cryptographic protocols and PREs provide safe and effective solutions. Unfortunately, the interaction cost of key agreement and the management cost of re-encryption keys have become unbearable as the scale of data sharing increased such that it is unsuitable for big data flexible sharing of massive users. (2) GKA and BE schemes can meet the requirements of data owners who require to safely share data with multiple data visitors. Note that both GKA and BE must be called for each sharing opportunity, and the joining and revocation of group users and the establishment and maintenance of broadcast keys mostly require online computations of users without using cloud computing resources. Furthermore, they are essentially plaintext-based data sharing solutions. Hence, each time data is shared, the ciphertext-based data require to be downloaded from the cloud and decrypted, and the plaintext is encrypted again by a GKA session key or a BE key before sharing and transmission. Consequently, the expense of online communications is relatively high and algorithm flexibility is low. (3) ABE is a one-to-many secure and efficient data sharing cryptography solution without interaction. Regardless of efficiency and deployment, the diverse variants of ABE and combination of ABE and PRE may be more consistent with the practical requirements of various applications. As a general extension of ABE, FE retains more flexibility and applicability compared with ABE in big data scenarios. In

particular, FE uses predicates to control the decryption authority of the ciphertext to break through the limitation of ciphertext only being decrypted by fixed predefined users. At present, many efficient and flexible ABE and FE schemes to achieve access control have been proposed for different scenarios and security models; there are many practical studies on application scenarios (e.g., medical and vehicular). The future development of data sharing primarily includes two directions. (1) However, there remain open problems such as attribute update and management, key escrow, attribute hiding, flexible expressions of attribute strategy, and reductions of communication costs between multiple authorities. (2) FE can use predicates to control the decryption result, aiming to break through the limitation under which ciphertext can only be decrypted to plaintext. Thus, when the predicates are applied to access control, only data visitors meeting specific hidden access control conditions can decrypt messages. If the predicate of the FE is applied to the decrypted content, the visitor can only yield the function value $f(m)$ when decrypting ciphertext $\mathrm{Enc}\{m\}$ using a secret key associated with a function f and get nothing more about m. This may bring additional flexibility and versatility to FE schemes. With research going on and open problems being solved, FE will have a wide range of application prospects for fine-grained ciphertext-based data sharing in the future. (3) As per the functional and security requirements of big data applications, customized solutions based on existing theories and technologies for ciphertext sharing are becoming a critical direction for further research.

4 Ciphertext-based data computing

In the future, most of the data will be stored in ciphertext on the cloud. To achieve a better balance between privacy protection and data mining, research on ciphertext-based data manipulation, including searching, querying, statistics, computing, and training, is an important direction for cryptography in the big data security domain. Encrypted data searches and query technologies can be divided into two types: attribute-preserving encryption and SEs. Attribute-preserving encryption enables ciphertext-based data querying by preserving certain attributes of plaintext in ciphertext, and SE realizes ciphertext-based data querying by establishing a search trapdoor. Ciphertext-based data computing, which is based on the homomorphic encryption algorithm, completes the calculation, analysis, and training of ciphertext in various application scenarios. Based on the number of participants, it can be divided into a single- and multiuser ciphertext-based data computing scenario. Corresponding cryptographic technology includes (fully) homomorphic encryption and secure MPC protocol. Ciphertext-based data computing between multiple users performs calculations between ciphertexts encrypted with different keys, which is mainly solved by secure MPC protocols. There are various secure MPC protocols based on threshold homomorphic encryption, multi-key homomorphic encryption, and combinations of garbled-circuit (GC) and oblivious-transfer (OT) methods. Additionally, code- and interaction-based schemes can be used to solve dedicated secure MPC problems (e.g., scientific, geometric, set intersection, and ciphertext machine learning). With the cross-combination of access control algorithms, such as identity-based encryption, ABE, or threshold encryption, ciphertext-based data computing can also flexibly manage the sharing permissions of calculation results. That is, the ciphertext-based problems of "what to compute" and "to whom the results can be shared" are solved concurrently. The continuous maturity of (fully) homomorphic encryption algorithms and secure MPC technologies has promoted innovation in real-life scenarios, such as those of medical data privacy computing, node computing for the internet of vehicles, and image-privacy processing. This section provides an overview of the technologies that can be used for ciphertext-based data searching and computing, including attribute-preserving encryption, SE, (fully) homomorphic encryption, and secure MPC protocols.

4.1 Ciphertext-based data searching

The data owner encrypts the data prior to uploading them to the cloud, making them unreadable while in the cloud. This creates challenges to cloud data retrieval, which begs the question of how ciphertext-based data searching can be achieved in the cloud. Instinctively, taking file retrieval as an example, users must download an encrypted file from the cloud server, decrypt it into plaintext, and then retrieve the data. However, data files in a big data environment are often relatively large, and the downloading and decryption incur great communication and computational costs. Ciphertext-based data searching aims to borrow cloud storage and computing resources to directly query and search the stored encrypted data while mitigating calculation and communication costs. Users rely on cryptographic trapdoors to

search for keywords or partial documents, in which the whole process must not expose any information about the target documents or trapdoors. Obviously, ciphertext-based data searching has a wide range of application prospects, such as the search for personal private data, confidential commercial documents, or sensitive medical data.

The main techniques used for ciphertext-based data searching include attribute-preserving encryption and SE. Attribute-preserving encryption provides that the ciphertext retains some attributes of plaintext, such as equivalence, sequence, and data format. This typically contains deterministic encryption (DE) and order-preserving encryption (OPE). On the one hand, DE ensures that the ciphertexts are the same when the same plaintexts are encrypted and that the plaintext search can be realized through the ciphertext equality search. OPE, on the other hand, ensures that the ciphertext retains the value order of the plaintext after encryption and the user can directly search the sorted ciphertext according to the order of the plaintext. Searchable encryption supports keyword searches on ciphertext, including public-key SE and symmetric SE. Users can directly search ciphertext data of SE under the condition of knowing the search trapdoor of keywords.

In 2004, Agrawal et al. [142] first proposed the idea of OPE but failed to provide a specific algorithm. In 2009, Boldyreva et al. [143] provided a formal definition of an IND-order-chosen plaintext attack (IND-OCPA) for the ideal security of OPE, but the scheme they provided did not satisfy ideal security. To satisfy the ideal security of IND-OCPA, Popa et al. [144] proposed a mutable OPE (mOPE) in 2013, but the encryption process required online interactions between the user and the cloud. Kerschbaum et al. [145] optimized the communication costs of Popa's scheme and proposed frequency-hiding OPE via randomization that achieved better security than IND-OCPA. Boneh et al. [146] proposed a noninteractive, IND-OCPA-secure, orderly visible OPE scheme based on multilinear mapping. Because of its computational efficiency, OPE has been put into practical applications, such as in encrypted database systems CryptDB and Cipherbase. To further improve the efficiency of the algorithm to better serve big data searching, based on computational hardness primitives, two novel but simple randomized OPE schemes [147] are proposed for the first time. Computational hardness primitives were general approximate common divisor problems (GACDPs) and decisional polynomial approximate common divisor problems (DPolyACDPs), respectively, and schemes have near optimal information leakage. Because of the reservation of the plaintext value order, which is an inherent problem, OPE will inevitably suffer from inference attacks [148], resulting in the adversary revealing some relevant information of the plaintext from the reserved value sequences of the ciphertext.

The first SE scheme [149] was proposed in 2000, and it spread relatively rapidly. According to the number of data owners and visitors in application scenarios, SE can be divided into four types: single-write single-read (S/S), multiple-write single-read (M/S), single-write multiple-read (S/M), and multiple-write multiple-read (M/M). The S/S SE scheme provides that the data owner is also the data visitor and searches for encrypted data stored in the cloud. The first SE scheme proposed by Song et al. [149] was an S/S type. The solution was based on the DE of keywords blinded by XOR pseudorandom numbers. The M/S-type SE provides that multiple data owners use the public key of the unique data visitor to encrypt data and keywords before uploading data. Only the data visitor uses a private key to generate search trapdoors to query ciphertext-based data. The first solution was public-key encryption with keyword search (PEKS), proposed by Boneh et al. [150] in 2004. It soon became a pronoun of the M/S-type SE because of its versatility. Abdalla et al. [151] subsequently used identity-based encryption instead of public-key encryption and proposed an identity-based PEKS scheme. Subsequent relevant research of single-read SE focused on targeted functionality extensions to satisfy the demand of practice. Xia et al. [152] proposed a multi-keyword sorting search scheme for the dynamic ciphertext on the cloud, which applies a special tree-based structure and a greedy depth-first search algorithm for the linear complexity searches and data deletions or insertions on the cloud. In response to similar requirements, Mohd et al. [153] proposed a direct search method over sentences using the conjunctive search function without any index. Based on a disjunctive search function, an SE scheme with multiple search queries that supports disjunctive search is also provided. The above multi-keyword exact matching or single-keyword fuzzy search algorithms are far less practical than multi-keyword fuzzy search on ciphertext-based data. For this reason, based on the first multi-keyword fuzzy search encryption of Wang et al. [154], Fu et al. [155] designed a new method of keyword transformation based on the uni-gram model, which simultaneously improves and enables the handling of other spelling mistakes. In addition to the multi-keyword fuzzy search, the substring of the secret data must be searched for and located in, for example, a DNA bank scenario. Based on the position heap tree-data structure, Strizhov et al. [156] proposed a tree-based

substring position searchable symmetric encryption (SSP-SSE) with ideal encryption and search efficiency. They also provided a multiuser extended setting, which supports arbitrary groups of users searching the encrypted data on the cloud. Although SE provides privacy protection for searchers, Gajek [157] proposed a constrained functional encryption (CFE)-based dynamic searchable symmetric encryption without any keyword information leakage. Targeting how to check the accuracy of search results, Jiang et al. [158] constructed a special data structure, QSet, based on an inverted index structure. Based on the QSet, a verifiable multi-keyword ranked search scheme is proposed. Unlike Jiang's method, Liu et al. [159] realized the verifiability of search results by designing aggregate key-based verifiable SE.

For multi-read scenarios, the M/M-type SE is the most suitable for real-life applications, in which any data owner can upload data and open search authorization for all users, and any user can obtain authorization from all data owners to search ciphertext-based data on the cloud. Therefore, research on the M/M-type SE (MMSE) is often combined with access control technologies such as ABE to jointly realize multiuser fine-grained searchable ciphertext-based data sharing, and research results are relatively rich. Zhao et al. [160] proposed an MMSE scheme based on ABE and ABS, optimized the search range of the scheme, and reduced the risk of information leakage. Sun et al. [161] combined proxy and lazy re-encryption to design an attribute-based MMSE scheme, which outsourced the user-withdrawal process to a semi-trusted cloud server. Liang et al. [123] provided flexible keyword update services for attribute-based MMSE based on attribute-based PRE. However, due to doubts about the credibility of the third party, some researchers tried to design MMSE solutions without one. One solution used a unique key [162] for each document, and the data owner set the search permission ahead of uploading and added the permission information at the end of the document. This solution was required to determine and solidify the search permissions before uploading, which affected the flexibility of searching and sharing. Another scheme [163] was based on the keyword authorization binary tree (KAB tree) with a fixed number of keywords, which limited the scalability of the scheme. Subsequently, to enhance the ability to resist an offline keyword guessing attack caused by the polynomial-size keyword space, a hidden policy ciphertext-policy attribute-based encryption with keyword search (HP-CPABKS) [164] was proposed. They also provided strict complementary proof of the indistinguishability of keywords and access structures under a rigorous selective security analysis. Conversely, Mamta et al. [165] designed a KP-ABSE based on key-policy ABE that efficiently supports dynamic users and specifies different access keywords for different data users for the same data. Based on the above work, Hayata et al. [166] discussed the relationship between the ABE and the PEKS constructions and developed a generic anonymous key-policy ABE construction from PEKS, the search condition of which is specified by logical disjunctions and logical conjunctions. Concerning dynamic ciphertext-based data retrieval, Bost [167] found a privacy leakage problem caused by information on update keywords of dynamic data being leaked. Thus, forward private searchable symmetric encryption (fs-SSE) based on trapdoor permutations was proposed in response to this problem. However, Bost's fs-SSE does not support data deletion, and Kim et al. [168] proposed a forward-secure dynamic data searchable symmetric encryption based on their new data structure dual dictionary. Presently, no solution includes all capabilities, such as sublinear search time, security of data and trapdoor hiding, concise indexes, and efficient authorization. For this purpose, Deng et al. [169] proposed a multiuser searchable encryption (MSE) scheme based on asymmetric bilinear Type-3 map groups and keyword authorization binary tree (KAB tree), which are asserted to satisfy the above properties simultaneously.

4.2 Single-user (single-key) ciphertext-based data computing: (fully) homomorphic encryption

Homomorphic encryption originated from the privacy homomorphism, which allowed certain operations to be performed on ciphertexts to increase the flexibility of encryption algorithms. Early research on homomorphic encryption mainly focused on partial homomorphic encryption, which only supports a single homomorphic operation, such as addition or multiplication. For example, Paillier only supports homomorphic addition operations, and ElGamal and RSA only support homomorphic multiplication operations. Fully homomorphic encryption (FHE) supports unlimited addition and multiplication calculations, including integer-based FHE schemes and lattice-based FHE schemes. Although FHE can support an infinite number of multi-operator homomorphic calculations, low efficiency and ciphertext noise expansion are still major obstacles to its application in large-scale data computing scenarios. This has received significant attention from researchers in recent years. The RSA, ElGamal, and Paillier encryption schemes

cannot resist the threats of quantum computing, while lattice-based FHE resists quantum attacks and supports homomorphic operations; therefore, it is very popular in this research field.

In 2009, Gentry [170] constructed the first FHE scheme based on an ideal lattice at the Annual ACM Symposium on Theory of Computing. In 2010, the US Defense Advanced Research Projects Agency (DARPA) launched the "Programming Computing on Encrypted Data" project, which examined the mathematical foundation of FHE, algorithm optimization, and programming languages of ciphertext homomorphic calculations, aiming to develop practical ciphertext-based computing methods. From the various difficult assumptions of fully homomorphic construction, there remain difficult problems in the lattice and the approximate greatest-common-divisor problem on the integer. The lattice-based FHE can be divided into the Gentry scheme FHE construction based on the ideal lattice, the FHE based on LWE assumption, and the NTRU-based FHE structure with key-switching.

FHE research based on difficult problems on the lattice can be roughly divided into three generations. The first generation of lattice-based FHE is represented by Gentry's construction, which is based on the difficult assumptions of the bounded distance problem (BDDP) and sparse-subset sun problem (SSSP) on the ideal lattice. The scheme first constructed a somewhat homomorphic encryption (SWHE) scheme that satisfied a limited number of addition and multiplication calculations using the bootstrapping program to achieve noise reduction to avoid noise expansion to the threshold and to decryption errors. Thus, it realized the unlimited time of ciphertext-based homomorphic calculation operations. Gentry's scheme could only satisfy CPA security and could not resist CCA. The researchers followed up on the efficiency, key size, and bootstrapping improvements. In 2010, Smart and Vercauteren [171] used simple instruction multiple data (SIMD) technology to expand the single-bit FHE to a multi-bit FHE scheme on public-key cryptography, realizing the parallel processing of multiple bits. However, the security of the SSSP assumption still requires further study, and the efficiency of bootstrapping programs is low. In 2011, Brakerski et al. [172] proposed the Brakerski-Vaikuntanathan (BV) scheme based on the LWE assumption. Hence, research on a second-generation FHE based on the (ring) LWE assumption began. The BV scheme uses multiple linearizations to construct the SWHE scheme based on LWE and proposes a dimension-modules reduction to replace Gentry's squashing technology of bootstrapping. In 2012, Brakerski et al. [173] constructed the Brakerski-Gentry-Vaikuntanathan (BGV) scheme under both ring-LWE and LWE assumptions and obtained leveled homomorphic encryption (LHE). Research on a second-generation FHE has mainly focused on noise control and efficiency improvement [174]. In 2013, Gentry et al. [175] used the approximate characteristic vector method to construct the Gentry-Sahai-Waters (GSW) scheme and realized simple and efficient homomorphic calculations through matrix addition and multiplication. Later, Alperin-Sheriff and Perkert [176] proposed an improved efficient bootstrapping program for GSW based on the gadget matrix. Subsequent studies were mostly based on the LWE assumption or its variant, aiming to optimize the efficiency, getting rid of the Gaussian noise sampling process, and handling false data injection or leakage attacks [177–179]. Generally, lattice-based FHE research has endured three generations to become resistant to quantum attacks. The first-generation FHE used a re-encryption algorithm, and the second-generation FHE used key- and module-switching to reduce the size and noise of the ciphertext. Third-generation FHE constructed LHE based on approximate feature vectors. However, it has not been able to eliminate the dependence on the bootstrapping program to realize unlimited homomorphic calculations.

In 2010, Dijk et al. [180] constructed the homomorphic encryption scheme Dijk-Gentry-Halevi-Vaikuntanathan (DGHV) based on the approximate greatest common divisor problem on integers. It was then converted into a fully homomorphic scheme using the bootstrapping program. In 2013, Cheon et al. [181] proposed a multi-bit DGHV scheme based on SIMD technology and the Chinese remainder theorem, which was slightly better than the original DGHV in terms of plaintext space size, ciphertext size, and efficiency. In 2015, Cheon et al. [182] constructed a fully homomorphic scheme based on the improved approximate greatest common divisor problem to further reduce the size of the ciphertext. In 2017, Benarroch et al. [183] proposed an integer FHE based on approximate characteristic vectors with approximate greatest common divisors and circular security, which could be resistant to quantum-computing risks and could be expanded from a single bit to multiple bits without requiring the assumption of noise free. Subsequent integer-based schemes [184, 185] mainly focused on public-key size reduction, ciphertext noise control, and ciphertext size reduction in single-bit encryption schemes.

Low computational efficiency is the biggest obstacle to the practical application of FHE in big data scenarios. However, most current schemes are single-bit FHE schemes, which require multiple bit extensions via iteration or splicing. Whether the SIMD technology is used in the first generation of FHE,

or ciphertext packaging and optimized bootstrapping programs are used in the second and third generations of FHE [186], efficiency problems arise, including excessively large ciphertexts and key sizes, fast noise growth, long running times, and small plain-ciphertext ratios. On the other hand, although the design of FHE schemes has undergone three generations, it has never eliminated its dependence on the bootstrapping program. Because the major approach to converting SWHE into FHE supports an unlimited number of calculations, the bootstrapping program greatly affects FHE computational efficiency. The main way to solve this problem is to build a new noise reduction technology to replace the bootstrapping technology, propose a more efficient bootstrap technology, or design a noiseless FHE scheme. Additionally, with ciphertext-based computing, especially multiplicative homomorphic calculations, both ciphertext and noise will grow at a certain large scale, and the control and reduction of noise will remain a limitation of FHE efficiency. Apart from efficiency, there are still open problems to be resolved in terms of security assumptions, security analysis, and practical applications. With regard to security assumptions, Doröz et al. [187] identified new difficult assumptions based on finite field isomorphisms (FFIs) on public-key cryptography in 2018 and constructed a new SWHE scheme based on the decision-FFI problem, in which the noise performance was analyzed, and the FHE scheme was further constructed through the bootstrapping program. Regarding security proofing and analysis, most FHE schemes were cleared of security under the CPA model, and it was impossible to achieve adaptive CCA (CCA2) security because of the homomorphic nature of FHE. Therefore, the FHE scheme that satisfied the non-adaptive chosen-ciphertext attack (CCA1) security [188] became the major research direction, which included schemes resistant to side-channel and key-recovery attacks [189]. Regarding practical applications, in 2018, Halevi and Shoup [190] improved the efficiency of the FHE software library, HElib[3)], increasing speeds 30–75 times via fast linear transformation. To further solve the problem of huge FHE computational and communication overhead, Zhou et al. [191] first proposed an efficient, fully homomorphic data encapsulation technology based on an arbitrary one-way trapdoor permutation.

As a basic encryption algorithm for ciphertext-based computing, many variants of FHE with special properties have been proposed, which are used in the construction of protocols (e.g., secure MPC). The threshold FHE [192, 193] combines threshold cryptography and homomorphic encryption to control the sharing of homomorphic calculation results. Multi-key fully homomorphic encryption (MFHE) [194] can realize the homomorphic operation of the ciphertext encrypted by different keys. However, the underlying MFHE schemes in previous studies still involve the common value, CRS, which seems to weaken the power of using MFHE to allow users to independently generate their own keys. MFHE schemes without CRS [195] and secure MPC protocol against semi-malicious security were proposed under the multi-key-CPA security model. In response to the subfield attacks and rapid growth of error in key-switching techniques of [194], modified NTRU-type MFHEs without key-switching [196] were provided, which decreased the magnitude of the error exponentially and minimized the dimension of ciphertexts. Additionally, FHE can be combined with other cryptographic primitives to extend its functionality, such as identity-based FHE [197, 198] and attribute-based FHE [199]. It is noteworthy that the recent bilinear-map-based iO schemes [200, 201] are conjectured to be secure; their security also relies on certain pseudorandom objects with novel security properties; other iO schemes must be redesigned for new computational problems [202]. To address such problems, Brakerski et al. [203] proposed a new cryptographic primitive, split FHE, which is a universal and concise heuristic-construction iO scheme.

4.3 Multiuser ciphertext-based data computing: secure MPC

Secure MPC provides that the participants use their own private input to complete the calculation of a certain function via cooperation or alternatively with the help of semi-trusted third parties, and no private information other than the result can be disclosed during the calculation process. In the ciphertext-based cloud storage and computing environment, secure MPC is an important tool for ensuring that multiple parties share collaborative computing results without revealing sensitive data. For example, Yao's millionaires' problem is used to only disclose the comparison result of two wealth values without revealing them.

The classical millionaires' problem was first raised by Yao [204] in 1982. Goldreich [205] provided the security definition of the secure MPC and proposed a protocol that could compute arbitrary functions, preliminarily establishing a theoretical framework for secure MPC. Subsequently, there were many

3) HElib: an implementation of homomorphic encryption. 2018. https://github.com/noelniles/HElib.

theoretical results (e.g., security models, general and specific schemes, basic tools, and computing systems) for secure MPC. At present, open problems to be solved mainly focus on security model definition, security proofing, fairness of the secure MPC protocol, efficiency improvement, and computing-system development. Application problems have also expanded from the millionaires' problem to privacy-set calculations, ranking and sorting calculations, max- and min-value calculations, statistical calculations, geometric calculations, etc. The application area has extended to electronic voting, auctions, data statistics, and confidential payment inquiries. Obviously, secure MPC has important theoretical significance and application value.

This subsection first reviews research on the basic tools of secure MPC, including the oblivious transfer and the garbled circuit. Second, summarized research on the general construction of secure MPC based on Yao's protocol and FHE is presented, which supports all the calculation problems. Finally, from the perspective of practical applications, the development status of solutions to problems of dedicated secure MPC supporting using one type of calculation are elaborated, including the millionaire problem, privacy-set computing, comparative ranking, and dedicated secure MPC systems.

4.3.1 *Basic tools for secure MPC*

The basic tools of secure MPC include OT, (fully) homomorphic encryption, GC, bit commitment. The most classic and commonly used are OT and GC.

The OT was first proposed by Rabin [206]. During OT, a sender S has only one secret message m, and the receiver R is to receive the message with a probability of $1/2$. S does not know whether R has obtained the message. Subsequently, a one-out-of-two OT protocol, OT_2^1, was proposed, in which S has two secret messages, m_1 and m_2, and S wants R to choose one of them randomly. However, S does not know which message R has been chosen. Further, more efficient and concise fully simulatable one-out-of-two OT schemes have been designed [207], and they have been widely applied to the construction of blind signatures, fair and secure electronic auction schemes, electronic voting schemes, and secure MPC schemes. Naturally, by calling the OT_2^1 protocol n times, the one-out-of-n OT protocol OT_n^1 was proposed. Afterward, a UC-secure OT_n^1 protocol based on dual-mode [208] was proposed. After the k-out-of-n transfer protocol OT_n^k was proposed, through repeated calls of OT_2^1 and OT_n^1, Guo et al. [209] constructed an OT_n^k protocol based on subset-membership encryption and a smooth projection hash function under the semi-honest and malicious adversary models. Initial OT protocols were based on the decisional Diffie-Hellman (DDH) problem, homomorphic encryptions, or smooth projection hash functions, and they were constructed under weak security models, such as privacy-only or one-sided simulations. Then, based on cut-and-choose technologies or smooth projection hash functions, OT protocols under a completely simulated malicious adversary model [210,211] were proposed. Efficiency research was mainly concentrated on round-number reduction, computational-cost reduction, OT expansion [212,213], and lightweight construction of the OT protocols [214] based on q-power DDH (q-PDDH) and decisional bilinear Diffie-Hellman (DBDH) assumptions. In terms of application, as a basic tool for secure MPC, the OT protocol can independently protect the privacy of computing input data and directly play an important role in the construction of auction and voting schemes. On the other hand, it can be used as a basic tool to construct secure MPC protocols to realize ciphertext-based cloud computing services.

The GC is a circuit protection method first proposed by Yao [215] in 1986 to solve the problem of secure two-party calculation. The calculation was converted into a combination of Boolean circuits, encrypting each gate and disrupting the circuit order. The constructor sends the GC and its computing input to another participant. The receiver selects his input to complete the calculation using OT, and the constructor decrypts the calculated GC to obtain the calculation result. Later, GC was formalized, and its foundation and security definitions of privacy, forgetfulness, reliability were provided [216]. In 2016, Hemenway et al. [217] proposed an adaptively secure GC scheme that was not reusable. Based on this scheme, Jafargholi et al. [218] proposed an indistinguishable adaptively secure GC in 2017. In terms of efficiency, Zahur et al. [219] proposed the half gate, which could reduce the number of ciphertext transmissions to two using an AND-gate calculation. Free-XOR technology was proposed to simplify the calculation of XOR gates, and it was later used by Ball et al. [220] to simplify the calculation of addition and multiplication gates. To further improve the efficiency of GC so that it can meet real-world applications, there were many efficiency optimization methods, including chaotic Gaussian elimination, fleXOR, weakening assumptions, pipeline execution, PartialGC, and size or depth optimizations. A better method was circuit reuse, and reusable GC schemes were constructed and studied based on attribute-

based FHE and random linear codes [221, 222]. Furthermore, Innocent et al. [223] proposed garbled circuit construction with the universal gates, which reduced the number of rows in the garbled table to two rows per gate with two or zero encryption and decryption calls during garbled circuit construction and evaluation. In terms of application studies, there have been constructions of efficient secure MPC schemes under various kinds of security models for different applications [224–228]. They have been widely used for delegating computation, noninteractive verifiable computing, key-dependent message security, private DNA matching, and deriving genomic diagnoses.

4.3.2 *General secure MPC schemes*

The first general secure MPC scheme was the Yao protocol, which was constructed by integrating GC and OT. Because the calculation of any function can be completed in the form of a Boolean circuit, the Yao protocol remains an effective basic method for constructing a general secure MPC protocol. More specifically, using the Yao protocol, the GC constructor generates an obfuscated version of the Boolean circuit and sends it to the calculator. After receiving the GC, the calculator selects its own input and calculates the output result of the circuit through the OT. However, the Yao protocol is insecure under the malicious security model, in which the adversary may not execute according to the protocol and can construct wrong GCs on purpose. To solve this problem, zero-knowledge proof [229] and committed input technologies [230] can trivially constrain the behavior of calculation participants to construct circuits honestly according to the objective function, but they greatly affect the efficiency of the protocol. To efficiently construct a general secure MPC protocol under the malicious adversary model, there are many solutions (e.g., Lego technology [231], preprocessing models [232], and cut-and-choose technologies [233]), whose purposes were to ensure that the GC is honestly constructed. However, the commitment input method uses a zero-knowledge proof to ensure the correctness of the circuit door-by-door, and the Lego technology essentially uses a cut-and-choose technique at the gate level. Both are unsuitable for larger calculation circuits. The preprocessing model uses a single online calculation as the presumed credible preprocessing stage, and it can be used to construct a secure MPC scheme under the UC model. However, the preprocessing model cannot be reused and is difficult to ensure that each calculation has a credible preprocessing stage for real-life scenarios. Compared with the above methods, the cut-and-choose technology that can achieve the honest construction of the calculation circuit is currently a more efficient and practical method. It constructs multiple GCs at the expense of minimal storage and calculation costs and verifies the correctness of the sampled verification circuits. The calculation is completed by the calculation circuit. Subsequently, cut-and-choose oblivious transfer (CCOT) [234] in a semi-honest model was proposed, whose efficiency approximates that of the state-of-the-art scheme. However, there are still problems, such as the input consistency of the GC constructor and the selection failure attack of the OT. To solve the problem of input consistency, public-key encryption is used to ensure the consistency of the calculation input instead of the commitment-based scheme, which requires a higher communication cost. To resist failure attacks of OT, optimizing the OT protocol and constructing OT variants with special attributes have been proposed, such as OT extensions [212, 213]. The research of general secure MPC schemes, especially the design of MPC protocol, mainly focused on the improvement of the security model, security assumptions and efficiency of OT and GC. Based on the OT or GC variants with new properties, new MPC protocols are constructed, such as noninteractive secure two-party computations [224], efficient authenticated garbling secure two-party computations [225, 226], and exact round complexity three-party computations [227].

Another construction method for a general secure MPC scheme is based on FHE. First, the general secure MPC scheme using homomorphic encryption [235, 236] requires multiple rounds of interaction to complete the calculation of any function, during which the computation and communication cost is high when the computing circuit depth is complex. Subsequently, MPC protocols based on threshold-based FHE and multi-key FHE have been proposed. Asharov et al. [237] used a threshold FHE to construct a three-round MPC protocol against semi-malicious adversaries based on the LWE assumption under the common random string (CRS) model. They used noninteractive zero-knowledge proof to propose a secure four-round MPC protocol for any number of malicious adversaries. Aliasgari et al. [238] presented secure solutions for both two-party and multi-party floating-point operation computation models and both semi-honest and malicious settings based on threshold homomorphic encryption, which achieved high accuracy and provable security guarantees. To improve efficiency, the correlation between the communication complexity and that of the objective function was decoupled. However, secure MPC based on threshold

FHE requires the computing participants to jointly generate a short-time public and private key for each calculation, and in real-life scenarios, users are more inclined to use long-term public and private keys to implement secure MPC. Consequently, a dynamic MPC [239] was proposed to realize the conversion from the NTRU-based FHE to a multi-key FHE scheme. They also used the scheme of Brakerski et al. [172, 173] to construct a three-round MPC protocol against semi-malicious adversaries under the CRS model. Therefore, the multi-key FHE scheme is another method that can realize the calculation of ciphertexts encrypted with different keys and construct MPC protocols. Since NTRU-based [240], GSW-based [192], and BGV-based [241, 242] multi-key FHE schemes were proposed, researchers have consecutively proposed corresponding secure MPC schemes, such as CRS-based single-hop dynamic MPC, in which each participant must be determined before the agreement starts. Dynamic MPC without CRS [243] and dynamic MPC based on distributed settings [244] were also developed. Additionally, a dynamic MPC scheme that supports multi-hop homomorphic operations [192] was proposed to replace the single-hop dynamic MPC, and secure MPC schemes under various security models were proposed to be resistant to semi-malicious, malicious, and mixed adversaries. Goyal [245] also proposed the concept of quantum multi-key FHE with a general method to transform a single-user-leveled FHE to a quantum multi-key FHE. Chen et al. [242] proposed a multi-key version of the fast FHE over the Torus (TFHE) library, which became the first code implementation of the multi-key FHE scheme. It provided a practical promotion for the universal structure of secure MPC based on multi-key FHE. Zhou et al. [246] proposed a lightweight multiuser (multi-key) fully homomorphic data encapsulation mechanism based on arbitrary one-way trapdoor replacement. This scheme re-encrypted the ciphertexts encrypted by different keys into the ciphertext under a unified encryption key, and the calculation and communication costs were further reduced.

4.3.3 *Dedicated secure MPC schemes and systems*

General secure MPC schemes are created to achieve the calculation of arbitrary functions; however, sometimes, the system only requires repeating the calculation of a single or uncomplicated function for multiple practical applications. Therefore, secure MPC schemes or systems for single specific problems have become an important research area, which does not require comprehensive support of calculation functions. The primary aim of the dedicated schemes is to achieve high efficiency realization for specific function calculation, and they can eliminate inefficient components such as GCs and OTs.

The computing problems targeted by dedicated secure MPC primarily include privacy-preserving scientific computing, computational geometry issues, private set intersection issues, and ciphertext-based machine learning issues, and many dedicated computing systems have been proposed based on their solutions.

In terms of privacy-preserving scientific computing, Yao's millionaires' problem is essentially a ciphertext-based comparison problem; it is a basic problem for secure MPC. The initial solution [215] is primarily based on general constructions, such as GCs and OTs, demanding high computational and communication complexity. Lin et al. [247] used a zero-to-one coding method to solve Yao's millionaires' problem and transformed the ciphertext-based data comparison into the number of common elements in two sets. The solution was efficient and concise; however, it only solved two problems: that of A being greater than B or A not being greater than B without considering the equality situation. Subsequent solutions, including FHE combined with hidden assumptions, arithmetic coding, and 1-r coding, were proposed to efficiently solve Yao's millionaires' problem [248, 249]. The extended problems included the blind millionaires' problem, socialist millionaires' problem, and rational number calculation [250].

The ciphertext sorting problem is primarily divided into ciphertext sorting without equal data and ciphertext sorting under normal circumstances (with equal data). Consecutively, researchers [251, 252] have proposed multiple secure and efficient solutions under the malicious model based on sorting networks, oblivious keyword sorting, quick sorting, and parallel fast sorting, which could both protect data privacy and avoid additional information leakage, ranking loss, and increase data flexibility.

The computational geometry problem is an important research direction for secure MPC, and it has a wide range of important applications in the calculation of sensitive geographic location data such as the internet of vehicles, oceans, and the military. After the geometry problem [253] was proposed based on secure MPC, the point inclusion problem, convex polygon intersection problem, and nearest-point judgment were presented. Inspired by their work, researchers presented a number of computational geometry problems and provided solutions, primarily including two types of problems, i.e., inclusion and

intersection. Point inclusion problems involve the relations of points and lines, points and segments, points and planes, points and curves, points and polygons, points and circles, and points and ellipses. The intersection problem focuses on the relations of lines and lines, segments and segments, curves and curves, lines and planes, planes and planes, polygons and polygons, circles and circles, and lines and circles. In response to the abovementioned problems, based on schemes of Yao's millionaires' problem, researchers established mathematical models of geometric problems, vector-advantage calculation, OT, homomorphic encryption, and proposed multiple general or dedicated solutions [254, 255].

The private set intersection (PSI) problem aims to find the intersection set without revealing the element information in the set, and it is one of the best-studied applications of secure computation and many PSI protocols that have been proposed. Abadi et al. [256] converted the privacy-set intersection problem into a polynomial greatest common-factor problem and extended the two-party set intersection to multiple sets. Pinkas et al. [257] suggested a new PSI protocol based on OT extension, whose runtime was superior to that of existing protocols. Research in this direction [258, 259] has been mainly focused on anti-collusion attacks under the malicious adversary model and the design of future anti-quantum attacks in terms of security. With regard to efficiency, it mainly reduces the number of overloaded operations, such as modular multiplication operations, and reduces the communication overhead of the solution.

The ciphertext-based machine learning problem aims to perform privacy-preserving data mining, which realizes the analysis, summary, and prediction of sensitive data, including ciphertext-based statistical and machine learning. Currently, there is a strong demand in fields involving sensitive data calculations, such as government data mining, health-care and medical information, and vehicular and geographical location data. Ciphertext-based machine learning includes machine training and reasoning. Because the latter problem often involves relatively small amounts of data and calculations and the realization efficiency has basically satisfied the realistic needs in real-life scenarios, current research is focused primarily on machine reasoning for ciphertext-based data classification [260]. Additionally, there are solutions to specific problems, such as the incremental support vector learning [261], delegating computation [262], and ciphertext-based image processing [263]. In particular, in order to learn a shared model by aggregating locally computed updates on the premise that training data is distributed on devices, McMahan et al. [264] advocated a scheme and named it decentralized approach federated learning. Beyond this, Yang et al. [265] introduced definitions, architectures, and applications for comprehensive secure federated learning framework, including horizontal federated learning, vertical federated learning, and federated transfer learning, and provided building data networks among organizations based on federated mechanisms. Expensive communication, systems heterogeneity, statistical heterogeneity, and privacy concerns are four of the core challenges that make federated learning different from distributed learning in data center settings or traditional private data analyses, and the main recent work [266] has begun to address these challenges as well as their productionizing and benchmarking in federated settings[4)].

Based on theoretical research results, the program development of dedicated secure MPC systems is gradually transforming theory into practice to meet the requirements of real-life scenarios. The first secure MPC system program was Fairplay [267], which was proposed in 2004. Subsequent work continued to improve the optimal algorithms for each component of the Yao protocol to achieve efficient computing of massive ciphertext-based data. Based on the Yao protocol, the first-generation secure MPC system represented by Fairplay used garbled circuits to generate target function codes, including FastGC [268], PICCO [269], Wysteria [270], and SoK [228], which required a relatively time-consuming compilation and recompilation process. The new generation of secure MPC systems that used programmable object codes includes EMP-toolkit [271], TinyGarble based on JustGarble [272], Obliv-C [273], ObliVM [274] based on ObliVM-GC, and Frigate [275]. Programmable target coding is a more concise intermediate representation of a circuit. The circuit does not require to be expanded under the intermediate representation using loop instructions, which greatly improves the computational efficiency. The research and development of secure MPC systems based on the Yao protocol have been slowly improving the efficiency of GCs and reducing computing bandwidth. In addition to general secure MPC systems, multiple dedicated secure MPC tools for specific application scenarios to solve specific problems have been proposed. For example, Google developed Private Join and Compute [276] for PSIs based on homomorphic encryption, as well as Password Checkup[5)] for weak-login password detection. Dedicated secure MPC tools do not require building a general calculation framework that can achieve the calculation of any function. It

4) Tensorflow federated: machine learning on decentralized data. https://www.tensorflow.org/federated.

5) Google Password Checkup. https://support.google.com/accounts?p=password-checkup. 2019.

Table 2 Comparison of MPC systems

Scheme	Languages	Protocol	Participants	Security model	Data types	Operators
PICCO [269]	C/C++	Hybrid Model	3+	Semi-honest/mixed	6	7
Wysteria [270]	Ocaml	Multi-party Circuit	2+	Semi-honest/mixed	3	3
EMP-toolkit [271]	C++	Garbled Circuits	2	Semi-honest/mixed/malicious	7	7
TinyGarble [272]	C/C++	Garbled Circuits	2	Semi-honest	0	Optimizer
Obliv-C [273]	C/Ocaml	Garbled Circuits	2	Semi-honest/mixed	6	7
ObliVM [274]	Java	Garbled Circuits	2	Semi-honest/mixed	4	7
Frigate [275]	C++	Garbled Circuits	2+	Mixed	4	6
PJ-C [276]	C++	Partial Homomorphic	2	Semi-honest	2	2

can efficiently process a certain type of function in real-life scenarios. Its high efficiency will provide efficient services and broad application prospects for real-life scenarios of big data. Table 2 shows the comparison of various MPC systems, including security models such as semi-honest adversaries, malicious adversaries, and hybrid models. A semi-honest adversary indicates that participants are performing as per the protocol but try to learn additional information. A malicious adversary indicates that the adversary breaks the protocol arbitrarily to learn information or to cause an incorrect result. The hybrid model indicates that the participants of the protocol include honest, semi-honest, and malicious users. There are seven types of data: booleans, fixed-length integers, arbitrary-length integers, floats, static arrays, dynamic arrays, and structs. Moreover, there are seven types of operators: logical, comparison, addition, multiplication, division, bit shift, and bitwise.

Summary and prospect. In this subsection, we focused on the cryptographic techniques used for ciphertext operation and calculation in big data scenarios, including attribute-preserving encryption and SE for ciphertext searching, FHE and secure MPC for ciphertext-based calculation. (1) In terms of ciphertext-based data searching, studies have primarily focused on the M/M-type SE scheme, which is the most complex and suitable for big data applications. There are rich research results for designing various schemes, efficiency improvements, semantic expression improvements, and various security models and proofs. Presently, they can theoretically meet the basic functional and security requirements of various big data applications. (2) For ciphertext-based data computing, in terms of single-user ciphertext computing for real big data applications, fully homomorphic solutions that are truly suitable for massive data encryption and ciphertext-based calculation remain immature, because of efficiency limitations. Certain partial homomorphic encryptions, such as Paillier, ElGamal, and RSA, have been gradually adopted to solve simple ciphertext-based computing problems in big data scenarios. In terms of multiuser ciphertext computing, this subsection outlines the development status of the secure MPC schemes from four aspects: basic tools, general constructions, dedicated schemes, and systems. Generally, theoretical research involves the design of basic tools and schemes as well as the study of security models, computational complexity, mathematical tools, and improvements to scheme efficiency. Currently, the general MPC scheme construction based on GCs is booming, and it evolves from theoretical research to practical application. There are many efficient computing systems, but some cannot directly complete calculations based on the ciphertext stored in the cloud. Because MFHE-based MPC can be realized in an offline manner, the general scheme based on MFHE is more suitable for these requirements. (3) Finally, in solving a specific computing problem, dedicated secure MPC schemes and systems have been customized and developed. The key scientific problem in this direction is figuring out how to decompose the specific computing function into lower-order polynomial problems that can be solved by partial or fully homomorphic encryption. In addition to the loss of flexibility and universality, its efficiency and customization are more likely to satisfy real-world applications in the field of big data. The future development of ciphertext-based data computing primarily includes three directions. (1) However, additional research on the security and efficiency of SE is still required under the conditions of massive data and users. (2) The efficiency of the MFHE currently restricts the development of this research direction. Therefore, research on efficient MFHE algorithms or the study of multi-key partial homomorphic and somewhat/fully homomorphic encryption algorithms requires breakthroughs. (3) In addition to the abovementioned security and efficiency issues, the fairness of the secure MPC scheme indicates that the participation of the GC constructor and circuit calculation party is unequal, and their contributions are not the same. This is another issue worthy of study. It is possible that the development transformation from key transfer protocol to key agreement protocol will be used as an important reference to solve the fairness problem.

5 Z-CABDS architecture and development prospects

The original purpose of cryptography was to protect data from being readable by illegal users. From the information theory's perspective, the plaintext is the transmission of all data and the deeper information that can be obtained by data mining. To protect privacy in future big data cloud computing environments, all data must be encrypted before uploading them to the cloud. Intuitively, this is an extreme zero-or-one processing scenario for security and usability. Any information of the ciphertext as well as additional private information from big data mining, including statistics, analysis, and training, cannot be leaked. This can be guaranteed by the indistinguishable security of cryptographic algorithms. Alternatively, users who meet all requirements for access authorization can decrypt the information, disclosing everything in plaintext. However, in real-life scenarios, the following situations often occur. Originally, a user only required the statistical summation of the privacy data of multiple users. However, the plaintext-based calculation still reveals other information, such as specific input values, the number of users or inputs, medians, averages, variances, and other statistical and distribution information of inputs. This runs counter to users' increasing demand for privacy protection. Therefore, the fine-grained sharing and multilevel controllable disclosure of data information have become important issues that big data security cryptography is trying to resolve.

Complex applications give rise to technological convergence and innovation. From the research overview, it can be seen that different cryptographic technologies aim to solve different security issues. The type, security requirement, and form of data are completely different according to different application scenarios, and it becomes necessary to adaptively adopt cryptographic schemes that can meet the requirements in terms of functionality, security, and efficiency. Big data security systems or platforms in complex scenarios must solve combined security issues, such as data storage, analysis, mining, management, sharing, and training. Discretely invoking multiple cryptographic techniques one by one to protect the security of the big data life cycle may cause unexpected security threats, and it will likely increase the communication and computing costs of the system. The deep integration of cryptographic technology can produce and customize an efficient and secure composite cryptosystem that will become an important method of solving the security problems of complex applications in big data environments. Therefore, based on surveys and integration of cryptographic techniques and from a holistic perspective of the big data life cycle security, Z-CABDS architecture, an extensible, compatible, and comprehensive reference cryptographic architecture for big data security, is given, as shown in Figure 5.

5.1 Z-CABDS architecture

The Z-CABDS architecture is extensible and Figure 5 shows only a few representative business flows, which can be intuitively adjusted as required as per application requirements. All business flows have compatible and unified key management and user management infrastructures, which demonstrates a high degree of syncretism and integration of the architecture. Storage cloud and computing cloud have basic login authentication, situational awareness, vulnerability scan, cloud log, and other security services; furthermore, there is an audit cloud for data owners to implement third-party integrity audits. In terms of the storage business, we select searchable source encryption such that the encrypted data can be flexibly retrieved at any time after it is stored in the personal data center of the cloud. In terms of the sharing business, we consider that the sharing demands include regular sharing, sudden sharing, and carbon copy. In response to regular sharing requirements, we choose searchable ABE or FE to store encrypted documents in the cloud for decryption by users who meet the access policy. When the cloud receives a carbon copy request, it directly retrieves the target ciphertext and sends it to the proxy server. The proxy re-encryption server manages the re-encryption keys between users; moreover, it can realize the conversion process from ciphertext of owners to that of users via re-encryption. If there is a temporary or sudden sharing requirement, the data owner needs to retrieve the target ciphertext from the cloud; after downloading and decrypting it, he then can share it by calling the AKA, GKA protocol, or BE encryption. In terms of computing services, it is divided into regular computing and sudden computing. Therefore, the data to be calculated needs to be protected by multi-key fully homomorphic encryption before uploading to the calculation server; furthermore, the server implements homomorphic calculations of circuits on the ciphertext encrypted with different user keys as per the calculation requirements. For sudden computing requires, the data owner needs to retrieve the target data to be calculated from the storage cloud or the calculation server with storage capabilities, download and decrypt it, and implement

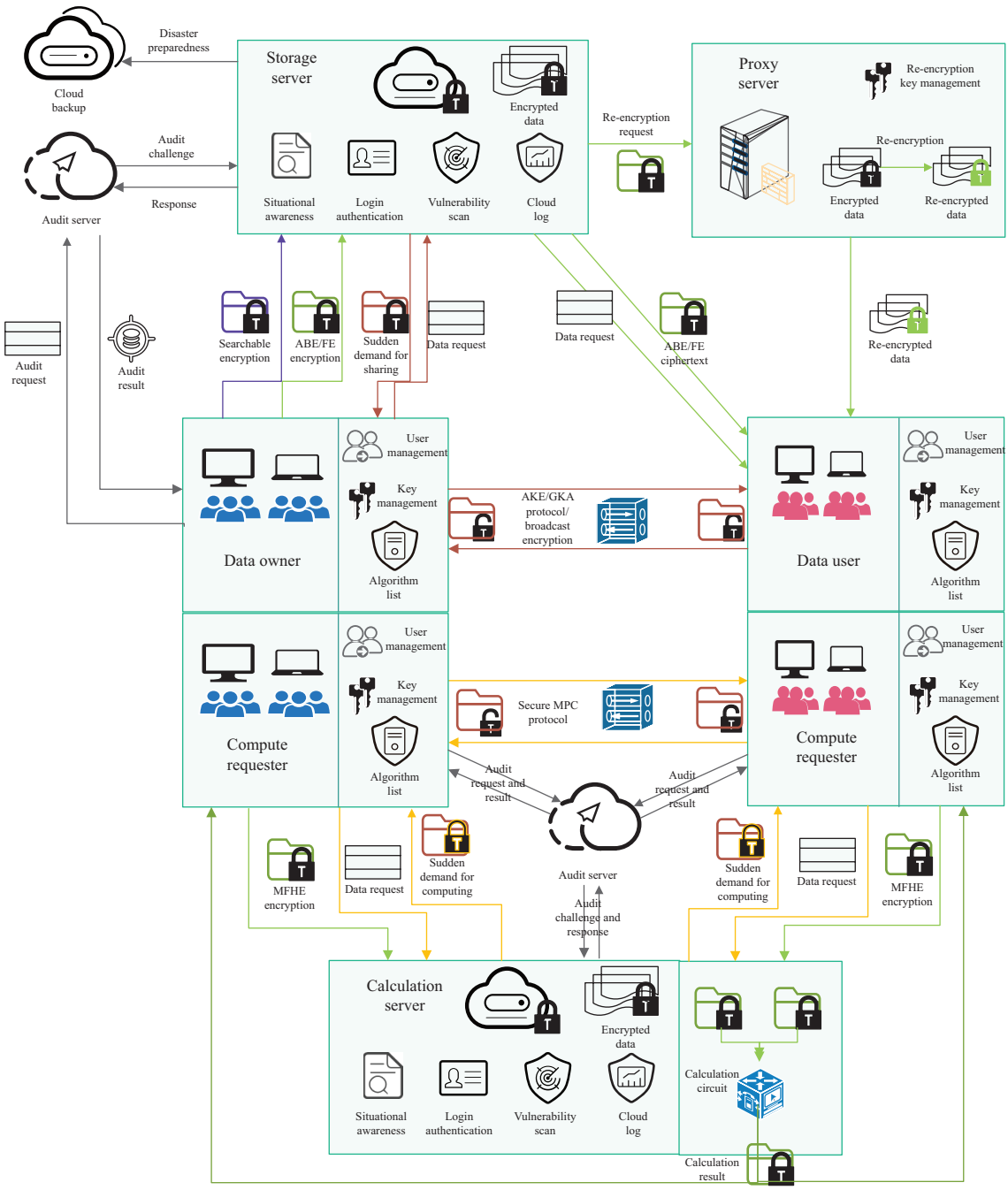

Figure 5 (Color online) Z-CABDS architecture.

it via a secure multi-party computing protocol.

The Z-CABDS architecture realizes the infrastructure resource sharing and business integration of primary big data application scenarios. Supplementarily, we still require achieving deep technical integration for security or efficiency requirements. For example, combining SE and ABE, attribute-based SE, which is used in the sharing business above, can not only realize the authority control of the data visitor but it can also determine the secret search of the access content in which the visitor can query the ciphertext-based data containing specific keywords. The hybrid encryption algorithm, combining symmetric encryption and ABE, uses efficient authenticated encryption to protect the confidentiality and integrity of data; moreover, it uses ABE to protect the symmetric key. It realizes the access control of the plaintext by controlling the access of the symmetric key. Identity-based BE [101] is based on the integration of an identity-based encryption scheme and a BE scheme that realizes secure and concise broadcast

communication in a certificateless manner. Considering identity-based FHE and attribute-based FHE as examples, data sharing technologies, such as identity-based encryption and ABE combined with FHE-based secure MPC, can flexibly secure and share fine-grained ciphertext-based data calculation results. Combined PRE technology with data sharing techniques, identity-based PREs, or attribute-based PREs can solve the limitation of secret data sharing between different keys or encryption algorithms. The combination of SE and (fully) homomorphic encryption can realize searches and calculations based on encrypted data [277]. Personally, designing efficient dedicated solutions and schemes for massive structured or unstructured data in various scenarios under the Z-CABDS architecture will be a key point of research for big data security promotion.

5.2 Development prospects

Assuming that massive data in the future will be encrypted before uploading to the cloud and stored in the form of ciphertext, study provides a comprehensive introduction of the research status of cryptography from the three aspects of big data secure storage, flexible and fine-grained sharing of ciphertext, and ciphertext-based data calculation. We focus on the essential problem to be solved by each technology, thus overviewing the current development statuses and gaps for satisfying the demands in real-life scenarios; moreover, we consider future development trends too. We believe that research on cryptography for big data security may focus on the following aspects.

(1) The complexity and diversity of practical big data applications promulgate additional detailed functional, security, and efficiency requirements, and security and efficiency are still the two primary development routes of various cryptographic technologies. Researchers analyzed and designed algorithms and schemes in terms of functional expansion, security, and efficiency improvement, as well as solutions to existing open problems. Moreover, big data algorithms are converted to sublinear time or space complexity algorithms to adapt to the scale of massive data that are continuously and rapidly generated. In a constantly updated big data environment, these algorithms suffer efficiency and implementation problems under plaintext conditions, let alone the ciphertext-based processing algorithms for massive data, such as the problem of calculating the median of massive ciphertext-based data constantly being generated. Consequently, the fusion of cryptographic and processing algorithms for massive data is an important limitation that must be considered and examined.

(2) Big data and cloud computing technologies render data information in a hierarchical manner. The entropy of information theory is possibly used to describe the amount of information in data transmission and mining. Therefore, a method for determining the amount or hierarchy of information is proposed for the security of encryption schemes used for ciphertext-based data sharing and calculation. The essence of big data privacy protection is to solve the fine-grained and precise transmission of data information. In addition to the original cryptographic provable security theory, the entropy value may be used to quantify the information released by the ciphertext-based data and describe to whom the data information will be transmitted and how much information will be released. It can estimate the accurateness of the encryption algorithm protecting and transmitting the information. This may become another security criterion for information security in a ciphertext-based big data environment. For example, the amount of information required by Yao's millionaires' problem is only one bit. In other words, it is the result of comparing two parties' data. Consequently, the ultimate result of the ideal solution to Yao's millionaires' problem is to leak only one bit of information without any additional data. However, multiple current solutions based on encoding or garbled circuits fall flat, and the information leaked during the calculation process comprises more than one bit; therefore, it can lead to inference attacks and additional information leakage problems. Furthermore, collusion attacks against ABE and secure MPC can be characterized by the amount of released ciphertext information. An attack indicates that the amount of information transmitted in a scheme or protocol surpasses the owner's expectations. This may become another information-based security consideration model to be applied to big data security alongside the provable security theory of cryptography.

(3) The main problem of the dynamic, secure MPC depends on the calculation of the distributed ciphertext encrypted by different keys. Although secure MPC schemes have solved this limitation to some extent, they often require users to obtain ciphertext-based data from cloud storage, decrypting the ciphertext to plaintext and calling the plaintext-based secure MPC protocol whose cost for online interactive communication is extremely high. Therefore, distributed ciphertext-based data calculations on clouds are more suitable for actual application scenarios. The current multi-key FHE scheme aims

to solve this limitation, but its efficiency is far from practical and is troubled by the multi-hop problem of key conversion. Aiming to solve the limitation of distributed ciphertext-based data calculation, it is necessary to further improve and optimize the multi-key and threshold-based FHE scheme in terms of efficiency. It should be determined whether the PRE scheme and key-switching technology should become alternatives for solving the key conversion problem in distributed ciphertext-based data calculation.

(4) The development of new technology has come up with the technological innovation of cryptography for big data security. The basic idea of indistinguishability obfuscation technology [278] is to transform the program into a multilinear jigsaw puzzle, and it reduces the security to the mathematical puzzles on the grid. Its successful construction [279] and combinations with other cryptographic technologies may create new solutions to the cryptographic technology for big data security. Furthermore, based on processing hardware, security dynamic monitoring, and control technologies, dynamic security checks [280] integrated with encryption schemes might provide confidentiality and integrity protection at the hardware level, thus preventing an attack caused by the loose coupling of encryption and data security. The encryption algorithm used in the hardware layer will provide a description of a strong binding security model for system security, and it can protect the original logical structure of the program, resisting tampering, reversing, and malicious code injection. Furthermore, it is possible to produce more underlying and central protection for big data security at the hardware level.

Acknowledgements This work was supported by National Key Research and Development Project (Grant No. 2020YFA0712300), National Natural Science Foundation of China (Grants Nos. 61772548, 61632012), Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-17-001), and Peng Cheng Laboratory Project of Guangdong Province (Grant No. PCL2018KP004).

References

1 Jiao L, Hao Y L, Feng D G. Stream cipher designs: a review. Sci China Inf Sci, 2020, 63: 131101
2 Yang J, Johansson T. An overview of cryptographic primitives for possible use in 5G and beyond. Sci China Inf Sci, 2020, 63: 220301
3 Dobraunig C, Eichlseder M, Mendel F, et al. 2016. Ascon-submission to the CAESAR competition. http://ascon.iaik.tugraz.at
4 Wu H, Preneel B. AEGIS: a fast authenticated encryption algorithm (v1.1). http://competitions.cr.yp.to/round3/aegisv11.pdf. 2016
5 Jean J, Nikolic I, Peyrin T, et al. Deoxys v1.41. http://competitions.cr.yp.to/round3/deoxysv141.pdf. 2016
6 Wu H. ACORN: A lightweight authenticated cipher (v3). http://competitions.cr.yp.to/round3/acornv3.pdf. 2016
7 Ted K, Rogaway P. OCB(v1.1). https://competitions.cr.yp.to/round3/ocbv11.pdf. 2016
8 Elena A, Andrey B, Nilanjan D, et al. COLM v1. http://competitions.cr.yp.to/round3/colmv1.pdf. 2016
9 Datta N, Luykx A, Mennink B, et al. Understanding RUP integrity of COLM. IACR Trans Symmetric Cryptol, 2017, 2017: 143–161
10 Jutla C S. Encryption modes with almost free message integrity. J Cryptol, 2008, 21: 547–578
11 Abed F, Forler C, List E, et al. RIV for robust authenticated encryption. In: Fast Software Encryption. Berlin: Springer, 2016. 23–42
12 Rogaway P, Shrimpton T. A provable-security treatment of the key-wrap problem. In: Advances in Cryptology—EUROCRYPT 2006. Berlin: Springer, 2006. 373–390
13 Neethu R, Sindhu M, Srinivasan C. XUBA: an authenticated encryption scheme. In: Data Engineering and Intelligent Computing. Singapore: Springer, 2016. 647–655
14 Ashur T, Dunkelman O, Luykx A. Boosting authenticated encryption robustness with minimal modifications. In: Advances in Cryptology—CRYPTO 2017. Berlin: Springer, 2017. 3–33
15 Naito Y. Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. IACR Trans Symmetric Cryptol, 2017, 2017: 1–26
16 Chakraborti A, Chattopadhyay A, Hassan M, et al. TriviA: a fast and secure authenticated encryption scheme. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015. 330–353
17 Reyhanitabar R, Vaudenay S, Vizár D. Boosting OMD for almost free authentication of associated data. In: Proceedings of International Workshop on Fast Software Encryption. Berlin: Springer, 2015. 411–427
18 Cogliani S, Maimut D, Naccache D, et al. Offset Merkle-Damgård (OMD) version 1.0. 2016. http://competitions.cr.yp.to/round1/omdv10.pdf
19 Thomas P, Yannick S. Counter-in-tweak: authenticated encryption modes for tweakable block ciphers. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2016. 33–63
20 Bellare M, Tackmann B. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2016. 247–276
21 Reyhanitabar R, Vaudenay S, Vizar D. Authenticated encryption with variable stretch. In: Advances in Cryptology—ASIACRYPT 2016. Berlin: Springer, 2016. 396–425
22 Hoang V, Krovetz T, Rogaway P. Robust authenticated-encryption AEZ and the problem that it solves. In: Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015. 15–44
23 Barwell G, Martin D P, Oswald E, et al. Authenticated encryption in the face of protocol and side channel leakage. In: Advances in Cryptology—ASIACRYPT 2017. Berlin: Springer, 2017. 693–732
24 Barbosa M, Farshim P. Indifferentiable authenticated encryption. In: Advances in Cryptology—CRYPTO 2018. Cham: Springer, 2018. 187–220
25 Simon T, Batina L, Daemen J, et al. Friet: an authenticated encryption scheme with built-in fault detection. In: Advances in Cryptology—EUROCRYPT 2020. Berlin: Springer, 2020. 581–611

26 Todo Y, Morii M. Bit-based division property and application to simon family. In: Fast Software Encryption. Berlin: Springer, 2016. 357–377
27 Todo Y, Isobe T, Hao Y, et al. Cube attacks on non-blackbox polynomials based on division property. In: Advances in Cryptology—CRYPTO 2017. Berlin: Springer, 2017. 250–279
28 Zhang P, Guan J, Li J, et al. Research on the confusion and diffusion properties of the initialization of MORUS. J Cryptol Res, 2015, 45: 155–187
29 Dwiedi A D, Morawiecki P, Wójtowicz S. Differential and rotational cryptanalysis of round-reduced MORUS. In: Proceedings of International Conference on Security and Cryptography, 2017. 23–56
30 Dobraunig C, Eichlseder M, Mendel F, et al. Cryptanalysis of ascon. In: Topics in Cryptology—CT-RSA 2015. Berlin: Springer, 2015. 371–387
31 Morawiecki P, Pieprzyk J, Straus M, et al. Applications of key recovery cube-attack-like. IACR Cryptology ePrint Archive, 2015. https://eprint.iacr.org/2015/1009
32 Ashur T, Dunkelman O, Luykx A. Boosting authenticated encryption robustness with minimal modifications. In: Advances in Cryptology—CRYPTO 2017. Berlin: Springer, 2017. 3–33
33 Bost R, Sanders O. Trick or tweak, on the (In)security of OTR's tweaks. In: Advances in Cryptology—ASIACRYPT 2016. Berlin: Springer, 2016. 333–353
34 Bay A, Ersoy O, Karakoc F. Universal forgery and key recovery attacks on ELmD authenticated encryption algorithm. In: Advances in Cryptology—ASIACRYPT 2016. Berlin: Springer, 2016. 354–368
35 Dodis Y, Grubbs P, Ristenpart T, et al. Fast message franking: from invisible salamanders to encryptment. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2018. 155–186
36 Grubbs P, Lu J, Ristenpart T. Message franking via committing authenticated encryption. In: Advances in Cryptology—CRYPTO 2017. Berlin: Springer, 2017. 66–97
37 Ateniese G, Burns R C, Curtmola A R, et al. Provable data possession at untrusted stores. In: Proceedings of the ACM Conference on Computer and Communications Security, 2007. 598–609
38 Juels A, Kaliski J B S. PORs: proofs of retrievability for large files. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2007. 584–597
39 Shacham H, Waters B. Compact proofs of retrievability. In: Advances in Cryptology—CRYPTO 2008. Berlin: Springer, 2008. 90–107
40 Wang C, Ren K, Lou W, et al. Toward publicly auditable secure cloud data storage services. IEEE Network, 2010, 24: 19–24
41 Xu C X, He X H, Abraha D. Cryptanalysis of Wang's auditing protocol for data storage security in cloud computing. In: Information Computing and Applications. Berlin: Springer, 2012. 422–428
42 Worku S G, Xu C X, Zhao J, et al. Secure and efficient privacy-preserving public auditing scheme for cloud storage. Comput Electrical Eng, 2014, 40: 1703–1713
43 Cui H, Mu Y, Au M H. Proof of retrievability with public verifiability resilient against related-key attacks. IET Inf Security, 2015, 9: 43–49
44 Liu H, Chen L, Davar Z, et al. Insecurity of an efficient privacy-preserving public auditing scheme for cloud data storage. J Univers Comput Sci, 2015, 21: 473–482
45 Yu J, Ren K, Wang C, et al. Enabling cloud storage auditing with key-exposure resistance. IEEE Trans Inform Forensic Secur, 2015, 10: 1167–1179
46 Yu J, Ren K, Wang C. Enabling cloud storage auditing with verifiable outsourcing of key updates. IEEE Trans Inform Forensic Secur, 2016, 11: 1362–1375
47 Wang B Y, Li B C, Li H. Oruta: privacy-preserving public auditing for shared data in the cloud. IEEE Trans Cloud Comput, 2014, 2: 43–56
48 Yu Y, Au M H, Mu Y, et al. Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. Int J Inf Secur, 2015, 14: 307–318
49 Liu J, Huang K, Rong H, et al. Privacy-preserving public auditing for regenerating-code-based cloud storage. IEEE Trans Inform Forensic Secur, 2015, 10: 1513–1528
50 Wang B, Li B, Li H. Panda: public auditing for shared data with efficient user revocation in the cloud. IEEE Trans Serv Comput, 2015, 8: 92–106
51 Yang G, Yu J, Shen W, et al. Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. J Syst Software, 2016, 113: 130–139
52 Chris E C, Alptekin K, Charalampos P, et al. Dynamic provable data possession. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2009. 213–222
53 Liu C, Ranjan R, Yang C, et al. MuR-DPA: top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud. IEEE Trans Comput, 2015, 64: 2609–2622
54 Chen X, Shang T, Kim I, et al. A remote data integrity checking scheme for big data storage. In: Proceedings of IEEE 2nd International Conference on Data Science in Cyberspace (DSC), 2017. 53–59
55 Sookhak M, Yu F R, Zomaya A Y. Auditing big data storage in cloud computing using divide and conquer tables. IEEE Trans Parallel Distrib Syst, 2018, 29: 999–1012
56 Cash D, Küpçü A, Wichs D. Dynamic proofs of retrievability via oblivious RAM. J Cryptol, 2017, 30: 22–57
57 Wang B, Li B, Li H, et al. Certificateless public auditing for data integrity in the cloud. In: Proceedings of IEEE Conference on Communications and Network Security (CNS), 2013. 233–239
58 He D, Zeadally S, Wu L. Certificateless public auditing scheme for cloud-assisted wireless body area networks. IEEE Syst J, 2018, 12: 64–73
59 Li J, Squicciarini A C, Lin D, et al. MMBcloud-tree: authenticated index for verifiable cloud service selection. IEEE Trans Dependable Secure Comput, 2017, 14: 185–198
60 Shen W, Qin J, Yu J, et al. Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. IEEE Trans Inform Forensic Secur, 2019, 14: 331–346
61 Yang L, Xia L. An efficient and secure public batch auditing protocol for dynamic cloud storage data. In: Proceedings of International Computer Symposium (ICS), 2017. 671–675
62 Bao H, Chen L. A lightweight privacy-preserving scheme with data integrity for smart grid communications. Concurr Computat-Pract Exper, 2016, 28: 1094–1110
63 Xu J, Wei L, Wu W, et al. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system. Future Gener Comput Syst, 2020, 108: 1287–1296

64 Liu X Y, Liu S L, Gu D W, et al. Two-pass authenticated key exchange with explicit authentication and tight security. In: Advances in Cryptology—ACIACRYPT 2020. Berlin: Springer, 2020. 785–814
65 Mitchell C J. Yet another insecure group key distribution scheme using secret sharing. J Inf Secur Appl, 2021, 57: 102713
66 Kong L, Zhai F, Zhao Y J, et al. Lightweight key management scheme for wireless communication system of distribution network. J Phys Conf Ser, 2021, 1754: 01216–012134
67 Fan-Yuan G J, Wang Z H, Wang S, et al. Optimizing decoy-state protocols for practical quantum key distribution systems. Adv Quantum Tech, 2021, 4: 2000131
68 Emura K, Seo J H, Watanabe Y. Efficient revocable identity-based encryption with short public parameters. Theor Comput Sci, 2021, 863: 127–155
69 Katsumata S, Matsuda T, Takayasu A. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. In: Public-Key Cryptography—PKC 2019. Berlin: Springer, 2019. 41–71
70 Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In: Advances in Cryptology—EUROCRYPT 1998. Berlin: Springer, 1998. 127–144
71 David D, Stephan K, Thomas L, et al. Revisiting proxy re-encryption: forward secrecy, improved security, and applications. In: Public-Key Cryptography—PKC 2018. Berlin: Springer, 2018. 219–250
72 Guo H, Zhang Z F, Xu J, et al. Accountable proxy re-encryption for secure data sharing. IEEE Trans Dependable Secure Comput, 2021, 18: 145–159
73 Green M, Ateniese G. Identity-based proxy re-encryption. In: Applied Cryptography and Network Security. Berlin: Springer, 2007. 288–306
74 Xu P, Jiao T, Wu Q, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. IEEE Trans Comput, 2016, 65: 66–79
75 Ge C, Susilo W, Fang L, et al. A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. Des Codes Cryptogr, 2018, 86: 2587–2603
76 Liu Y P, Ren Y J, Ge C P, et al. A CCA-secure multi-conditional proxy broadcast re-encryption scheme for cloud storage system. J Inf Secur Appl, 2019, 47: 125–131
77 Fang L M, Wang J D, Ge C P, et al. Conditional proxy broadcast re-encryption with fine grain policy for cloud data sharing. Int J Embedded Syst, 2019, 11: 115–124
78 Ge C, Liu Z, Xia J, et al. Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. IEEE Trans Dependable Secure Comput, 2021, 18: 1214–1226
79 Huang Q, Yang Y, Fu J. PRECISE: identity-based private data sharing with conditional proxy re-encryption in online social networks. Future Gener Comput Syst, 2018, 86: 1523–1533
80 Borcea C, Gupta A B D, Polyakov Y, et al. PICADOR: end-to-end encrypted publish-subscribe information distribution with proxy re-encryption. Future Gener Comput Syst, 2017, 71: 177–191
81 Vijayakumar V, Priyan M K, Ushadevi G, et al. E-health cloud security using timing enabled proxy re-encryption. Mobile Netw Appl, 2019, 24: 1034–1045
82 Sahai A, Waters B. Fuzzy identity-based encryption. In: Advances in Cryptology—EUROCRYPT 2005. Berlin: Springer, 2005. 457–473
83 Boneh D, Sahai A, Waters B. Functional encryption: definitions and challenges. In: Theory of Cryptography. Berlin: Springer, 2011. 253–273
84 Mike B, Yvo D. A secure and efficient conference key distribution system. In: Advances in Cryptology—EUROCRYPT 1994. Berlin: Springer, 1994. 275–286
85 Zhang Q K, Wang B L, Zhang X S, et al. Blockchain-based dynamic group key agreement protocol for ad hoc network. Chin J Electron, 2020, 29: 447–454
86 Xu Z S, Li F, Deng H, et al. A blockchain-based authentication and dynamic group key agreement protocol. Sensors, 2020, 20: 4835–4845
87 Teng J K, Ma H Y. Dynamic asymmetric group key agreement protocol with traitor traceability. IET Inf Secur, 2019, 13: 703–710
88 Gan Y, Wang B, Zhuang Y, et al. An asymmetric group key agreement protocol based on attribute threshold for Internet of Things. Trans Emerging Tel Tech, 2021, 32: e4179
89 Zhang Q K, Wang X M, Yuan J L, et al. A hierarchical group key agreement protocol using orientable attributes for cloud computing. Inf Sci, 2019, 480: 55–69
90 Zhang L, Wu Q H, Qin B, et al. Certificateless and identity-based authenticated asymmetric group key agreement. Int J Inf Secur, 2017, 16: 559–576
91 Chen Q N, Wu T, Hu C N, et al. An identity-based cross-domain authenticated asymmetric group key agreement. Information, 2021, 12: 112–121
92 Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts). In: Advances in Cryptology—EUROCRYPT 2009. Berlin: Springer, 2009. 171–188
93 Wee H. Déjà Q: encore! Un petit IBE. In: Theory of Cryptography. Berlin: Springer, 2016. 237–258
94 Acharya K, Dutta R. Constructing provable secure broadcast encryption scheme with dealership. J Inf Secur Appl, 2021, 58: 102736
95 Libert B, Paterson K G, Quaglia E A. Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model. In: Public Key Cryptography—PKC 2012. Berlin: Springer, 2012. 206–224
96 He K, Weng J, Liu J, et al. Anonymous identity-based broadcast encryption with chosen-ciphertext security. In: Proceedings of ACM on Asia Conference on Computer and Communications Security, 2016. 247–255
97 Boneh D, Zhandry M. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. Algorithmica, 2017, 79: 1233–1285
98 Abdalla M, Bellare M, Neven G. Robust encryption. J Cryptol, 2018, 31: 307–350
99 Mandal M. Privacy-preserving fully anonymous ciphertext policy attribute-based broadcast encryption with constant-size secret keys and fast decryption. J Inf Secur Appl, 2020, 55: 102666
100 Chen L Q, Li J G, Lu Y, et al. Adaptively secure certificate-based broadcast encryption and its application to cloud storage service. Inf Sci, 2020, 538: 273–289
101 Mishra P, Renuka P, Verma V. Identity based broadcast encryption scheme with shorter decryption keys for open networks. Wireless Pers Commun, 2020, 115: 961–969
102 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE Symposium on

Security and Privacy, 2007. 321–334
103 Vipul G, Omkant P, Amit S, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2006. 89–98
104 Cao Z F. New trends of information security—how to change people's life style? Sci China Inf Sci, 2016, 59: 050106
105 Liu Z, Cao Z F, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Trans Inform Forensic Secur, 2013, 8: 76–88
106 Liu Z, Cao Z, Wong D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on an ebay. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2013. 475–486
107 Ning J, Cao Z, Dong X, et al. Traceable CP-ABE with short ciphertexts: how to catch people selling decryption devices on eBay efficiently. In: Computer Security—ESORICS 2016. Berlin: Springer, 2016. 276–288
108 Zhang K, Li H, Ma J F, et al. Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability. Sci China Inf Sci, 2018, 61: 032102
109 Liang X, Cao Z, Lin H, et al. Attribute based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009. 276-286
110 Qian J, Dong X. Fully secure revocable attribute-based encryption. J Shanghai Jiaotong Univ (Sci), 2011, 16: 490–496
111 Sahai A, Seyalioglu H, Waters H. Dynamic credentials and ciphertext delegation for attribute-based encryption. In: Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012. 199–217
112 Yang K, Jia X. Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE Trans Parallel Distrib Syst, 2014, 25: 1735–1744
113 Li J, Yao W, Zhang Y, et al. Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Trans Serv Comput, 2017, 10: 785–796
114 Cui H, Deng R H, Li Y J, et al. Server-aided revocable attribute-based encryption. In: Computer Security—ESORICS 2016. Berlin: Springer, 2016. 570–587
115 Qin B D, Zhao Q L, Zheng D, et al. (Dual) server-aided revocable attribute-based encryption with decryption key exposure resistance. Inf Sci, 2019, 490: 74–92
116 Cui H, Yuen T H, Deng R H, et al. Server-aided revocable attribute-based encryption for cloud computing services. Concurr Computat Pract Exper, 2020, 32: e5680
117 Chase M. Multi-authority attribute based encryption. In: Theory of Cryptography. Berlin: Springer, 2007. 515–534
118 Zhou S L, Chen G X, Huang G J, et al. Research on multi-authority CP-ABE access control model in multicloud. China Commun, 2020, 17: 220–233
119 Banerjee S, Roy S, Odelu V, et al. Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment. J Inf Secur Appl, 2020, 53: 102503
120 Zhao Q Q, Wu G F, Ma H, et al. Black-box and public traceability in multi-authority attribute based encryption. Chin J Electron, 2020, 29: 106–113
121 Okamoto T, Takashima K. Decentralized attribute-based encryption and signatures. IEICE Trans Fundamentals, 2020, E103.A: 41–73
122 Liang K T, Susilo W, Liu J K. Privacy-preserving ciphertext multi-sharing control for big data storage. IEEE Trans Inform Forensic Secur, 2015, 10: 1578–1589
123 Liang K T, Susilo W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans Inform Forensic Secur, 2015, 10: 1981–1992
124 Xu X, Zhou J, Wang X. Multi-authority proxy re-encryption based on CPABE for cloud storage systems. J Syst Eng Electron, 2016, 27: 211–223
125 Gorbunov S, Vaikuntanathan V, Wee H. Attribute-based encryption for circuits. In: Proceedings of the 45th Annual ACM Symposium on Theory of Computing, 2015. 545–554
126 Wang S, Zhou J, Liu J K, et al. An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Trans Inform Forensic Secur, 2016, 11: 1265–1277
127 Xia Y, Chen W, Liu X, et al. Adaptive multimedia data forwarding for privacy preservation in vehicular Ad-Hoc networks. IEEE Trans Intell Transp Syst, 2017, 18: 2629–2641
128 Cui H, Deng R H, Wang G. An attribute-based framework for secure communications in vehicular ad hoc networks. IEEE/ACM Trans Networking, 2019, 27: 721–733
129 Liu X H, Liu Q, Peng T, et al. Dynamic access policy in cloud-based personal health record (PHR) systems. Inf Sci, 2017, 379: 62–81
130 Athena J, Sumathy V. TBAC: tree-based access control approach for secure access of PHR in cloud. Int J Biomed Eng Technol, 2019, 29: 246–272
131 Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Theory of Cryptography. Berlin: Springer, 2007. 535–554
132 Okamoto T, Takashima K. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. Des Codes Cryptogr, 2015, 77: 725–771
133 Gaybullaev T, Kwon H Y, Kim T, et al. Efficient and privacy-preserving energy trading on blockchain using dual binary encoding for inner product encryption. Sensors, 2021, 21: 2024
134 Jie C, Gay R, Wee H. Improved dual system ABE in prime-order groups via predicate encodings. In: Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015. 595–624
135 Ling S, Nguyen K, Wang H, et al. Server-aided revocable predicate encryption: formalization and lattice-based instantiation. Comput J, 2019, 62: 49–62
136 Nandi M, Pandit T. Delegation-based conversion from CPA to CCA-secure predicate encryption. Int J Appl Cryptogr, 2020, 4: 16
137 Naveed M, Agrawal S, Prabhakaran M, et al. Controlled functional encryption. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2014. 1280–1291
138 Ambrona M, Fiore D, Soriente C. Controlled functional encryption revisited: multi-authority extensions and efficient schemes for quadratic functions. Proc Privacy Enhancing Technol, 2021, 2021: 21–42
139 Bitansky N, Nishimaki R, Passelégue A, et al. From cryptomania to obfustopia through secret-key functional encryption. J Cryptol, 2020, 33: 357–405
140 Lin H. Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs. In: Advances in Cryptology—CRYPTO 2017. Berlin: Springer, 2017. 599–629

141 Cho W, Kim J, Lee C. (In)security of concrete instantiation of Lin17's functional encryption scheme from noisy multilinear maps. Des Codes Cryptogr, 2021, 89: 973–1016
142 Agrawal R, Kiernan J, Srikant R, et al. Order-preserving encryption for numeric data. In: Proceedings of the ACM SIGMOD International Conference on Management of Data, 2004. 563–574
143 Boldyreva A, Chenette N, Lee Y, et al. Order-preserving symmetric encryption. In: Advances in Cryptology—EUROCRYPT 2009. Berlin: Springer, 2009. 224–241
144 Popa R A, Li F H, Zeldovich N. An ideal-security protocol for order-preserving encoding. In: Proceedings of IEEE Symposium on Security and Privacy, 2013. 463–477
145 Kerschbaum F. Frequency-hiding order-preserving encryption. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2015. 656–667
146 Boneh D, Lewi K, Raykova M, et al. Semantically secure order-revealing encryption: multi-input functional encryption without obfuscation. In: Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015. 563–594
147 Dyer J, Dyer M, Djemame K. Order-preserving encryption using approximate common divisors. J Inf Secur Appl, 2019, 49: 102391
148 Naveed M, Kamara S, Wright C V. Inference attacks on property-preserving encrypted databases. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2015. 644–655
149 Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of IEEE Symposium on Security and Privacy, 2000. 44–55
150 Boneh D, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search. In: Advances in Cryptology—EUROCRYPT 2004. Berlin: Springer, 2004. 506–522
151 Abdalla M, Bellare M, Catalano D, et al. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. In: Advances in Cryptology—CRYPTO 2005. Berlin: Springer, 2005. 205–222
152 Xia Z, Wang X, Sun X, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst, 2016, 27: 340–352
153 Kamal A A A M, Iwamura K. Searchable encryption using secret sharing scheme that realizes direct search of encrypted documents and disjunctive search of multiple keywords. J Inf Secur Appl, 2021, 59: 102824
154 Wang B, Yu S, Lou W, et al. Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud. In: Proceedings of IEEE Conference on Computer Communications, 2014. 2112–2120
155 Fu Z, Wu X, Guan C, et al. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inform Forensic Secur, 2016, 11: 2706–2716
156 Strizhov M, Osman Z, Ray I. Substring position search over encrypted cloud data supporting efficient multi-user setup. Future Internet, 2016, 8: 28–35
157 Gajek S. Dynamic symmetric searchable encryption from constrained functional encryption. In: Topics in Cryptology—CT-RSA 2016. Berlin: Springer, 2016. 75–89
158 Jiang X, Yu J, Yan J, et al. Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data. Inf Sci, 2017, 403-404: 22–41
159 Liu Z, Li T, Li P, et al. Verifiable searchable encryption with aggregate keys for data sharing system. Future Gener Comput Syst, 2018, 78: 778–788
160 Zhao F, Nishide T, Sakurai K. Fine-grained access control aware multi-user data sharing with secure keyword search. IEICE Trans Inf Syst, 2014, 97: 1790–1803
161 Sun W, Yu S, Lou W, et al. Protecting your right: attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In: Proceedings of IEEE Conference on Computer Communications, 2014. 226–234
162 Tang Q. Nothing is for free: security in searching shared and encrypted data. IEEE Trans Inform Forensic Secur, 2014, 9: 1943–1952
163 Popa R, Zeldovich N. Multi-key searchable encryption. IACR Cryptology ePrint Archive, 2013. https://eprint.iacr.org/2013/508/20130817:204810
164 Qiu S, Liu J Q, Shi Y F, et al. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. Sci China Inf Sci, 2017, 60: 052105
165 Mamta, Gupta B B. An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud. Concurr Computat Pract Exper, 2020, 32: e5291
166 Hayata J, Ishizaka M, Sakai Y, et al. Generic construction of adaptively secure anonymous key-policy attribute-based encryption from public-key searchable encryption. IEICE Trans Fundamentals, 2020, 103: 107–113
167 Bost R. $\Sigma o\Phi o\zeta$: forward secure searchable encryption. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2016. 1143–1154
168 Kim K S, Kim M, Lee D, et al. Forward secure dynamic searchable symmetric encryption with efficient updates. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2017. 1449–1463
169 Deng Z, Li K L, Li K Q, et al. A multi-user searchable encryption scheme with keyword authorization in a cloud storage. Future Gener Comput Syst, 2017, 72: 208–218
170 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing, 2009. 169–178
171 Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Public Key Cryptography—PKC 2010. Berlin: Springer, 2010. 420–443
172 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. In: Proceedings of IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011. 97–106
173 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping. ACM Trans Comput Theor, 2014, 6: 1–36
174 Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In: Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012. 868–886
175 Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Proceedings of Annual Cryptology Conference. Berlin: Springer, 2013. 75–92
176 Alperin-Sheriff J, Peikert C. Faster bootstrapping with polynomial error. In: Advances in Cryptology—CRYPTO 2014. Berlin: Springer, 2014. 297–314
177 Li Z, Ma C, Wang D. Leakage resilient leveled FHE on multiple bit message. IEEE Trans Big Data, 2021, 7: 845–858
178 Luo F C, Wang F Q, Wang K P, et al. Fully homomorphic encryption based on the ring learning with rounding problem.

IET Inf Secur, 2019, 13: 639–648
179 Amuthan A, Sendhil R. Hybrid GSW and DM based fully homomorphic encryption scheme for handling false data injection attacks under privacy preserving data aggregation in fog computing. J Ambient Intell Human Comput, 2020, 11: 5217–5231
180 van Dijk M, Gentry C, Halevi S. Fully homomorphic encryption over the integers. In: Advances in Cryptology—EUROCRYPT 2010. Berlin: Springer, 2010. 24–43
181 Cheon J H, Coron J S, Kim J, et al. Batch fully homomorphic encryption over the integers. In: Advances in Cryptology—EUROCRYPT 2013. Berlin: Springer, 2013. 315–335
182 Cheon J H, Stehlé D. Fully homomophic encryption over the integers revisited. In: Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015. 513–536
183 Benarroch D, Brakerski Z, Lepoint T. FHE over the integers: decomposed and batched in the post-quantum regime. In: Public-Key Cryptography—PKC 2017. Berlin: Springer, 2017. 271–301
184 Aung K M M, Lee H T, Tan B H M, et al. Fully homomorphic encryption over the integers for non-binary plaintexts without the sparse subset sum problem. Theor Comput Sci, 2019, 771: 49–70
185 Dyer J, Dyer M, Xu J. Practical homomorphic encryption over the integers for secure computation in the cloud. Int J Inf Secur, 2019, 18: 549–579
186 Chillotti I, Gama N, Georgieva M, et al. Faster packed homomorphic operations and efficient circuit bootstrapping for TFHE. In: Advances in Cryptology—ASIACRYPT 2017. Berlin: Springer, 2017. 377–408
187 Doröz Y, Hoffstein J, Pipher J, et al. Fully homomorphic encryption from the finite field isomorphism problem. In: Public-Key Cryptography—PKC 2018. Berlin: Springer, 2018. 125–155
188 Ran C, Raghuraman S, Richelson S, et al. Chosen-ciphertext secure fully homomorphic encryption. In: Public-Key Cryptography—PKC 2017. Berlin: Springer, 2017. 213–240
189 Li Z, Galbraith S D, Ma C. Preventing adaptive key recovery attacks on the GSW levelled homomorphic encryption scheme. In: Provable Security. Berlin: Springer, 2016. 373–383
190 Halevi S, Shoup V. Faster homomorphic linear transformations in HElib. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2018. 93–120
191 Zhou J, Choo K K R, Cao Z, et al. PVOPM: verifiable privacy-preserving pattern matching with efficient outsourcing in the malicious setting. IEEE Trans Dependable Secure Comput, 2019. doi: 10.1109/TDSC.2019.2947436
192 Boneh D, Gennaro R, Goldfeder S, et al. Threshold cryptosystems from threshold fully homomorphic encryption. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2018. 565–596
193 Lu Y, Zhou T, Tian Y, et al. Web-based privacy-preserving multicenter medical data analysis tools via threshold homomorphic encryption: design and development study. J Med Internet Res, 2020, 22: e22555
194 Adriana L A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing, 2012. 1219–1234
195 Kim E, Lee H S, Park J. Towards round-optimal secure multiparty computations: multikey FHE without a CRS. Int J Found Comput Sci, 2020, 31: 157–174
196 Che X L, Zhou T P, Li N B, et al. Modified multi-key fully homomorphic encryption based on NTRU cryptosystem without key-switching. Tinshhua Sci Technol, 2020, 25: 564–578
197 Yamada S. Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques. In: Advances in Cryptology—CRYPTO 2017. Berlin: Springer, 2017. 161–193
198 Clear M, Mcgoldrick C. Additively homomorphic IBE from higher residuosity. In: Public-Key Cryptography—PKC 2019. Berlin: Springer, 2019. 496–515
199 Brakerski Z, Cash D, Tsabary R, et al. Targeted homomorphic attribute-based encryption. In: Theory of Cryptography. Berlin: Springer, 2016. 330–360
200 Agrawal S. Indistinguishability obfuscation without multilinear maps: new methods for bootstrapping and instantiation. In: Advances in Cryptology—EUROCRYPT 2019. Berlin: Springer, 2019. 191–225
201 Jain A, Lin H, Christian M, et al. How to leverage hardness of constant-degree expanding polynomials overaRto build iO. In: Advances in Cryptology—EUROCRYPT 2019. Berlin: Springer, 2019. 251–281
202 Boneh D, Lewi K, Wu D J. Constraining pseudorandom functions privately. In: Public-Key Cryptography—PKC 2017. Berlin: Springer, 2017. 494–524
203 Brakerski Z, Döttling N, Garg S, et al. Candidate iO from homomorphic encryption schemes. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2020. 79–109
204 Yao A C. Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, 1982. 160–164
205 Goldreich O. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge: Cambridge University Press, 2009
206 Rabin M O. How to exchange secrets with oblivious transfer. IACR Cryptology ePrint Archive, 2005. http://eprint.iacr.org/2005/187
207 Kumar M, Praveen I. A fully simulatable oblivious transfer scheme using vector decomposition. In: Advances in Intelligent Systems & Computing. New Delhi: Springer, 2015. 309: 131–137
208 Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer. In: Advances in Cryptology—CRYPTO 2008. Berlin: Springer, 2008. 554–571
209 Guo F, Mu Y, Susilo W. Subset membership encryption and its applications to oblivious transfer. IEEE Trans Inform Forensic Secur, 2014, 9: 1098–1107
210 Dttling N, Garg S, Hajiabadi M, et al. Two-round oblivious transfer from CDH or LPN. In: Advances in Cryptology—EUROCRYPT 2020. Berlin: Springer, 2020. 119–135
211 Goyal V, Jain A, Jin Z, et al. Statistical zaps and new oblivious transfer protocols. In: Advances in Cryptology—EUROCRYPT 2020. Berlin: Springer, 2020. 235–270
212 Orrú M, Orsini E, Scholl P. Actively secure 1-out-of-N OT extension with application to private set intersection. In: Topics in Cryptology—CT-RSA 2017. Berlin: Springer, 2017. 381–396
213 Patra A, Sarkar P, Suresh A. Fast actively secure OT extension for short secrets. In: Proceedings of Network and Distributed System Symposium, 2017. 131–154
214 Mi B, Huang D, Wan S, et al. A post-quantum light weight 1-out-n oblivious transfer protocol. Comput Electrical Eng, 2019, 75: 90–100
215 Yao C C. How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science, 1986. 162–167

216 Bellare M, Hoang V T, Rogaway P. Foundations of garbled circuits. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2012. 784–796
217 Hemenway B, Jafargholi Z, Ostrovsky R, et al. Adaptively secure garbled circuits from one-way functions. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2016. 149–178
218 Jafargholi Z, Scafuro A, Wichs D. Adaptively indistinguishable garbled circuits. In: Theory of Cryptography. Berlin: Springer, 2017. 40–71
219 Zahur S, Rosulek M, Evans D. Two halves make a whole. In: Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015. 220–250
220 Ball M, Malkin T, Rosulek M. Garbling gadgets for Boolean and arithmetic circuits share on. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2016. 565–577
221 Wang X A, Xhafa F, Ma J, et al. Reusable garbled gates for new fully homomorphic encryption service. Int J Web Grid Serv, 2017, 13: 25–38
222 Alam M, Emmanuel N, Khan T, et al. Secure policy execution using reusable garbled circuit in the cloud. Future Gener Comput Syst, 2018, 87: 488–501
223 Innocent A A T, Sangeeta K, Prakash G. Universal gates on garbled circuit construction. Concurr Computat Pract Exper, 2019, 22: e5236
224 Mohassel P, Rosulek M. Non-interactive secure 2PC in the offline/online and batch settings. In: Advances in Cryptology—EUROCRYPT 2017. Berlin: Springer, 2017. 425–455
225 Xiao W, Ranellucci S, Katz J. Authenticated garbling and efficient maliciously secure two-party computation. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2017. 21–37
226 Katz J, Ranellucci S, Rosulek M, et al. Optimizing authenticated garbling for faster secure two-party computation. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2018. 365–391
227 Patra A, Ravi D. On the exact round complexity of secure three-party computation. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2018. 425–458
228 Hastings M, Hemenway B, Noble D, et al. SoK: general purpose compilers for secure multi-party computation. In: Proceedings of IEEE Symposium on Security and Privacy, 2019. 1220–1237
229 Katz J, Ostrovsky R. Round-optimal secure two-party computation. In: Advances in Cryptology—CRYPTO 2004. Berlin: Springer, 2004. 335–354
230 Jarecki S, Shmatikov V. Efficient two-party secure computation on committed inputs. In: Advances in Cryptology—EUROCRYPT 2007. Berlin: Springer, 2007. 97–114
231 Nielsen J B. MiniLEGO: efficient secure two-party computation from general assumptions. In: Advances in Cryptology—EUROCRYPT 2013. Berlin: Springer, 2013. 537–556
232 Nielsen J B, Nordholt P S, Orlandi C, et al. A new approach to practical active-secure two-party computation. In: Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012. 681–700
233 Lindell Y. Fast cut-and-choose based protocols for malicious and covert adversaries. In: Advances in Cryptology—CRYPTO 2013. Berlin: Springer, 2013. 1–17
234 Wei X C, Xu L, Zhao M H, et al. Secure extended wildcard pattern matching protocol from cut-and-choose oblivious transfer. Inf Sci, 2020, 529: 132–140
235 Bendlin R, Damgård I, Orlandi C, et al. Semi-homomorphic encryption and multiparty computation. In: Advances in Cryptology—EUROCRYPT 2011. Berlin: Springer, 2011. 169–188
236 Damgrd I, Pastro V, Smart N P, et al. Multiparty computation from somewhat homomorphic encryption. In: Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012. 643–662
237 Asharov G, Jain A, Adriana L A, et al. Multiparty computation with low communication, computation and interaction via threshold FHE. In: Advances in Cryptology—EUROCRYPT 2012. Berlin: Springer, 2012. 483–501
238 Aliasgari M, Blanton M, Bayatbabolghani F. Secure computation of hidden Markov models and secure floating-point arithmetic in the malicious model. Int J Inf Secur, 2017, 16: 577–601
239 Gordon S D, Liu F H, Shi E. Constant-round MPC with fairness and guarantee of output delivery. In: Proceedings of Annual International Cryptology Conference. Berlin: Springer, 2015. 371–400
240 Chongchitmate W, Ostrovsky R. Circuit-private multi-key FHE. In: Public-Key Cryptography—PKC 2017. Berlin: Springer, 2017. 241–270
241 Chen H, Dai W, Kim M. Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2019. 395–412
242 Chen H, Chillotti I, Song Y. Multi-key homomophic encryption from TFHE. In: Advances in Cryptology —ASIACRYPT 2019. Berlin: Springer, 2019. 446–472
243 Kim E, Lee H S, Park J. Towards round-optimal secure multiparty computations: multikey FHE without a CRS. In: Proceedings of Australasian Conference on Information Security and Privacy. Berlin: Springer, 2018. 101–113
244 Brakerski Z, Halevi S, Polychroniadou A. Four round secure computation without setup. In: Theory of Cryptography. Berlin: Springer, 2017. 678–710
245 Goyal R. Quantum multi-key homomorphic encryption for polynomial-sized circuits. IACR Cryptology ePrint Archive, 2018. https://eprint.iacr.org/2018/443
246 Zhou J, Cao Z, Qin Z, et al. LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs. IEEE Trans Inform Forensic Secur, 2020, 15: 420–434
247 Lin H Y, Tzeng W G. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Applied Cryptography and Network Security. Berlin: Springer, 2005. 456–466
248 Li S D, Guo Y M, Zhou S F, et al. Efficient protocols for the general millionaires' problem. Chin J Electron, 2017, 26: 696–702
249 Liu M, Nanda P, Zhang X. Asymmetric commutative encryption scheme based efficient solution to the millionaires' problem. In: Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and the 12th IEEE International Conference on Big Data Science and Engineering Combined Conference, 2018. 990–995
250 Liu X, Choo K K R, Deng R H, et al. Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE Trans Dependable Secure Comput, 2018, 15: 27–39
251 Hamada K, Kikuchi R, Dai I, et al. Practically efficient multi-party sorting protocols from comparison sort algorithms. In: Information Security and Cryptology—ICISC 2012. Berlin: Springer, 2012. 202–216

252 Marszaek Z. Parallel fast sort algorithm for secure multiparty computation. J Universal Comput Sci, 2018, 24: 488–514
253 Atallah M J, Du W. Secure multi-party computational geometry. In: Proceedings of the 7th International Workshop on Algorithms and Data Structures (WADS 2001). Berlin: Springer, 2001. 165–179
254 Qin J, Duan H, Zhao H, et al. A new Lagrange solution to the privacy-preserving general geometric intersection problem. J Network Comput Appl, 2014, 46: 94–99
255 Liu W J, Xu Y, Yang J C N, et al. Privacy-preserving quantum two-party geometric intersection. Comput Mater Continua, 2019, 60: 1237–1250
256 Abadi A, Terzis S, Dong C. O-PSI: delegated private set intersection on outsourced datasets. In: ICT Systems Security and Privacy Protection. Berlin: Springer, 2005. 3–17
257 Pinkas B, Schneider T, Zohner M. Faster private set intersection based on OT extension. In: Proceedings of the 23rd USENIX Security Symposium, 2014. 797–812
258 Freedman M J, Hazay C, Nissim K, et al. Efficient set intersection with simulation-based security. J Cryptol, 2016, 29: 115–155
259 Hirofumi M, Noritaka S, Hiromi M. A proposal of profit sharing method for secure multiparty computation. Int J Innovative Comput Inform Control, 2018, 14: 727–735
260 Juvekar C, Vaikuntanathan V, Chandrakasan A. Gazelle: a low latency framework for secure neural network inference. In: Proceedings of the 27th USENIX Conference on Security Symposium, 2018. 1651–1668
261 Gu B, Sheng V S, Tay K Y, et al. Incremental support vector learning for ordinal regression. IEEE Trans Neural Netw Learning Syst, 2015, 26: 1403–1416
262 Goldwasser S, Kalai Y T, Rothblum G N. Delegating computation: interactive proofs for muggles. J ACM, 2015, 62: 1–64
263 Zheng Y, Cui H, Wang C, et al. Privacy-preserving image denoising from external cloud databases. IEEE Trans Inform Forensic Secur, 2017, 12: 1285–1298
264 McMahan H B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 2017. 1273–1282
265 Yang Q, Liu Y, Chen T, et al. Federated machine learning: concept and applications. ACM Trans Intell Syst Technol, 2019, 10: 1–19
266 Li T, Sahu A K, Talwalkar A, et al. Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag, 2020, 37: 50–60
267 Malkhi D, Nisan N, Pinkas B, et al. Fairplay: a secure two-party computation system. In: Proceedings of the 13th Conference on USENIX Security Symposium, 2004. 20–59
268 Gueron S, Lindell Y, Nof A, et al. Fast garbling of circuits under standard assumptions. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2015. 5670-578
269 Zhang Y, Steele A, Blanton M. PICCO: a general-purpose compiler for private distributed computation. In: Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2013. 813–826
270 Rastogi A, Hammer M A, Hicks M. Wysteria: a programming language for generic, mixed-mode multiparty computations. In: Proceedings of IEEE Symposium on Security and Privacy, 2014. 655–670
271 Wang X, Malozemoff A J, Katz J, et al. EMP-toolkit: efficient multiparty computation toolkit. 2016. https://github.com/emp-toolkit
272 Songhori E M, Hussain S U, Sadeghi A R, et al. TinyGarble: highly compressed and scalable sequential garbled circuits. In: Proceedings of IEEE Symposium on Security and Privacy, 2015. 411–428
273 Zahur S, Evans D. Obliv-C: a language for extensible data-oblivious computation. IACR Cryptology ePrint Archive 2015/1153, 2015
274 Liu C, Xiao S W, Nayak K, et al. ObliVM: a programming framework for secure computation. In: Proceedings of IEEE Symposium on Security and Privacy, 2015. 359–376
275 Mood B, Gupta D, Carter H, et al. Frigate: a validated, extensible, and efficient compiler and interpreter for secure computation. In: Proceedings of IEEE European Symposium on Security and Privacy, 2016. 112–127
276 Mihaela I, Kreuter B. On deploying secure computing commercially: private intersection-sum protocols and their business applications. IACR Cryptology ePrint Archive, 2019. https://eprint.iacr.org/2019/723.pdf
277 Cheon J H, Kim M, Kim M. Optimized search-and-compute circuits and their application to query evaluation on encrypted data. IEEE Trans Inform Forensic Secur, 2016, 11: 188–199
278 Garg S, Gentry C, Halevi S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits. sIn: Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, 2013. 40–49
279 Jain A, Lin H, Sahai A. Indistinguishability obfuscation from well-founded assumptions. In: Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, 2021. 60–73
280 Liu L B, Luo A, Li G H, et al. Jintide®: a hardware security enhanced server CPU with Xeon®Cores under runtime surveillance by an In-Package dynamically reconfigurable processor. In: Proceedings of IEEE Hot Chips 31 Symposium (HCS), 2019. 1–25