SCIENCE CHINA
Information Sciences

• REVIEW •
Special Focus on Security of Cyberspace

November 2015, Vol. 58 110101:1–110101:43
doi: 10.1007/s11432-015-5433-4

Survey on cyberspace security†

ZHANG HuanGuo[1*], HAN WenBao[2], LAI XueJia[3], LIN DongDai[4], MA JianFeng[5] & LI JianHua[6]

[1]*Computer School of Wuhan University, Wuhan* 430072*, China;*
[2]*State Key Laboratory of Mathematics Engineering and Advanced Computing, Wuxi* 214122*, China;*
[3]*Department of Computer, Shanghai Jiaotong University, Shanghai* 200240*, China;*
[4]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[5]*School of Cyber Engineering, Xidian University, Xi'an* 710071*, China;*
[6]*School of Information Security Engineering, Shanghai Jiaotong University, Shanghai* 200240*, China*

Received August 6, 2015; accepted September 29, 2015

Abstract Along with the rapid development and wide application of information technology, human society has entered the information era. In this era, people live and work in cyberspace. Cyberspace is the collection of all information systems; it is the information environment for human survival. Therefore, it is necessary to ensure the security of cyberspace. This paper gives a comprehensive introduction to research and development in this field, with a description of existing problems and some currently active research topics in the areas of cyberspace itself, cyberspace security, cryptography, network security, information system security and information content security.

Keywords cyberspace security, information security, cryptography, network security, information system security, information content security

Citation Zhang H G, Han W B, Lai X J, et al. Survey on cyberspace security. Sci China Inf Sci, 2015, 58: 110101(43), doi: 10.1007/s11432-015-5433-4

1 Cyberspace

1.1 Concept of cyberspace

After the mechanical and electronic eras, human society has entered a new era of information technology. In this information era, the information industry has become the largest in the world. Information is now a fundamental resource, akin to water, electricity and oil. Information and information technology are changing the ways in which people live and work. Electronic information equipment, such as computers, the Internet, television and mobile phones, has become essential for much of the world's population. Thus, in the information age, people live in a three-dimensional world composed of the physical world, human society and the information space [1–4].

In order to describe the information environment or information space where humans live, the term **cyberspace** was coined in English. However, there is no single equivalent term in Chinese. There are

* Corresponding author (email: liss@whu.edu.cn).
† Sections 1, 2 and 5 of this paper are written by ZHANG HuanGuo, Section 3 by HAN WenBao, LAI XueJia and LIN DongDai, Section 4 by MA JianFeng, Section 6 by LI JianHua.

a number of descriptions, which can be translated into English as "information space", "cyberspace", "electronic and magnetic space", "digital world", and there is an expression in Pinyin, "Sai Bo Kong Jian".

In his 1982 science fiction short story "Burning Chrome", Canadian writer William Gibson used the word "cyberspace" to means a virtual information space created by computers. The use of "cyber" expressed computer enthusiasts' hallucinations experienced during gaming, embodying the concept that cyberspace comprises not only the information itself, but also its impact on human thought and cognition. Since then, with the rapid development of information technology and the ubiquity of the Internet, the concept of cyberspace has continued to evolve.

The National Security Presidential Directive (NSPD) 54, published on January 9, 2008, defined cyberspace as "the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries".

At present, however, there is no unified definition of cyberspace. We can think of cyberspace as the information environment in which people live in the information era and as a collection of the totality of information systems. Therefore, it is better to consider cyberspace both as an information space and as a network space. The former conception highlights the core aspect of information, while the latter highlights the important feature of network-based interconnection. In this paper, we shall mainly adopt the conception of cyberspace as a network space.

1.2 Cyberspace security

Information security is the shadow of information—where there is information, there will be information security issues.

From the perspective of information theory, the system is the carrier and the information is the content. Cyberspace is a collection of all information systems, and it is the information environment in which humans live. People and information are influenced by each other. Therefore, cyberspace has more significant information security issues than other spaces. However, the core concept here is still information security.

At present, on the one hand, information technology and its industrial applications are flourishing like never before. On the other hand, information security issues are becoming ever more prominent. Hostile actions such as hacker attacks, malicious software intrusions, computer crimes and privacy breaches constitute great threats to information security. In addition, developments in both science and technology have posed new challenges to information security. Because of the parallelism achievable with quantum and DNA computers, many existing public key cryptographic systems (ELGamal, RSA, ECC, etc.) are no longer secure. As a result, the situation with regard to cyberspace security can be considered to be very grim [5,6].

For China, the serious security situation in cyberspace is a result not only of the above threats, but also of the fact that essential hardware components (e.g., CPUs) and fundamental software (e.g., operating systems) come mainly from foreign suppliers. Consequently, China has lost the basis on which it can control its own cyberspace.

President Xi Jinping has pointed out "If there is no cyberspace security, there will be no national security. If there is no informatization, there will be no modernization."

It is essential that China ensures its cyberspace security.

2 Cyberspace security as a new discipline

2.1 The concept of cyberspace security

Traditional information security emphasizes the security of the information (data) itself, with the following principal considerations:

- Confidentiality of information: Information is accessible only to those authorized to have access.

• Integrity of information: Information cannot be modified in an unauthorized or undetectable manner.

• Availability of information: Information must be available when it is needed.

It is basic to information theory that information cannot be separated from its carrier, so we cannot talk about information security without an information system. This means that we should consider information security from the perspective of the information system. Therefore, we divide information system security into four levels: equipment safety, data security, content security, and behavioral security, with data security being the traditional way in which information security is conceived [1–4].

1. Equipment safety. Safety of the information system is the primary problem of information system security.

• Stability of equipment: The probability that equipment can work without failure in a certain period of time.

• Reliability of equipment: The probability that equipment can perform tasks within a certain period of time.

• Availability of equipment: The probability that equipment can be used at any time.

Equipment safety is the material basis of information system security. Without equipment safety, information system security becomes a castle in the air. Any damage to the equipment will endanger the security of the information system. However, equipment safety alone is insufficient to guarantee information system security. In addition, we must further ensure data security.

2. Data security. Measures should be taken to ensure that data is protected from unauthorized disclosure, tampering and destruction.

• Confidentiality: Data is accessible only to those authorized to have access.

• Integrity: Data cannot be modified in an unauthorized or undetectable manner.

• Availability: Data must be available when it is needed.

3. Content security. Content security is essential for information security at the political, legal and moral levels.

• Information content is politically acceptable.

• Information content complies with national laws and regulations.

• Information content conforms to the moral norms of the Chinese nation.

In addition, in its broad sense, content security also includes, among other things, confidentiality of information content, protection of intellectual property, information concealment and privacy protection.

4. Behavioral security. Data security is a form of static security, whereas behavioral security is a form of dynamic security.

• Confidentiality of behavior: The behavioral pattern and its results cannot harm data confidentiality. When necessary, the behavioral process and its results should be secret.

• Integrity of behavior: The behavioral pattern and its results cannot harm data integrity, and should be predictable.

• Controllability of behavior: When behavior deviates from its expected pattern, this can be determined, controlled or corrected.

The concept of behavioral security is in accordance with the philosophical principle that practice is the sole criterion for testing truth, and it is also in accordance with the Chinese government's information security strategy according to which information should be secure and controllable.

To ensure information security a systematic approach is necessary, in which a number of measures must be taken in concert. In particular, it is important to emphasize that law, education and management should not be ignored, and indeed in many cases they play even more important roles than technical measures.

Hardware safety and operating system security are the basis of information system security, and, in this context, cryptography and network security technology play key roles. Moreover, it is necessary to enhance security at the low levels of hardware and software, and take measures in a systematic way, in order to effectively ensure the security of an information system [1–4,7–9].

In summary, we propose a definition of cyberspace security as a new discipline that focuses on the study of information security assurance problems with regard to the acquisition, storage, transmission

and processing of information [7–9].

Cyberspace security has a cross-disciplinary nature in that involves the disciplines of computer science, electronics, communications, mathematics, physics, biology, management, law and education. It has close connections with these disciplines, but is essentially an independent discipline with its own nomenclature, theory, technology and applications. It is key to the information society, and, indeed, in June 2015, the Education Ministry of China formally designated cyberspace security as a top-level discipline.

2.2 Main directions of research in cyberspace security

Currently, the main research directions in cyberspace security are cryptography, network security, information system security, information content security and information confrontation [7–9].

1. Cryptography. Cryptography comprises cryptography and cryptanalysis. Cryptography is the coding of information to achieve hidden information, and cryptanalysis is mainly concerned with studying ciphertext to obtain corresponding plaintext. The main research directions in cryptography are as follows:

(a) symmetric-key cryptography;
(b) public-key cryptography;
(c) hash functions;
(d) cryptographic protocols;
(e) new approaches to cryptography: biological cryptography, quantum cryptography, etc.;
(f) key management;
(g) applications of cryptography.

2. Network security. The basic idea of network security is to take protective measures at different levels and with different scopes, in order to discover a variety of network security threats, and then to take appropriate response measures to ensure information security in the network environment. Protection, detection and response are required to be based on certain security policies and security mechanisms. The main research directions in network security are as follows:

(a) network security threats;
(b) communication security;
(c) protocol security;
(d) network protection;
(e) intrusion detection;
(f) intrusion response;
(g) trusted networks.

3. Information system security. The information system is the carrier of information, which has a direct interface with users. Users obtain information services from information systems. The central feature of information system security is that information security threats and protection against them are considered systematically. The main research directions in information system security are as follows:

(a) information system security threats;
(b) hardware safety;
(c) software security;
(d) access control;
(e) trusted computing;
(f) level of protection of information system security;
(g) information system security evaluation and certification;
(h) application security.

4. Information content security. Information content security is the requirement for information security at the political, legal and moral levels. We request that information content be secure, that is, that information content be politically acceptable, conform to laws and regulations, and be in accordance with the moral norms of Chinese society. The main research directions in information content security are as follows:

(a) information content acquisition;
(b) analysis and recognition of information content;

(c) management and control of information content;

(d) legal guarantee of information security.

At present, there is no agreement among the academic community regarding security of information content. Generalized information content security also includes information content confidentiality, intellectual property protection, information hiding, and privacy protection, among other things.

5. Information confrontation. Information confrontation concerns the application of comprehensive technical countermeasures against attempts to interfere with or gain control over information and information systems, primarily using electronic methods. It is essentially based on the fact that different regions of the electromagnetic spectrum can be used to process and transmit information. The main research directions in information confrontation are as follows:

(a) communication confrontation;

(b) radar confrontation;

(c) photoelectric confrontation;

(d) computer network warfare.

2.3 Theoretical foundations of cyberspace security

During its foundation and development as a new discipline, cyberspace security has acquired its own unique theoretical foundation and methodology [7–9].

2.3.1 *Mathematics*

Mathematics is the theoretical basis of the physical sciences, and therefore it is also the theoretical basis for information security. Modern cryptography can be divided into two categories: mathematically based cryptography and non-mathematically cryptography. However, non-mathematically based cryptography (such as quantum cryptography and DNA cryptography) is still in its initial stage of development and is not widely used. At present, the most widely used cryptographic methods are still based on mathematics. It is generally accepted that the design of a cryptographic method is essentially the design of a mathematical function and that deciphering is the solution of a mathematical problem. Algebra, number theory, probability and statistics, and combinatorics are all branches of mathematics that play foundational roles in cryptography.

Protocol forms the core of a network, so protocol security is essential for network security. Another branch of mathematics, logic, is one of the theoretical foundations of protocol security.

Game theory, yet another branch of modern mathematics, is the study of confrontational or competitive behavior. In general, confrontational or competitive behavior is game behavior. In game behavior, different parties who participate in the competition or confrontation have different goals or interests, and try to select the best or the most reasonable scheme. Game theory studies whether there exists a most reasonable behavior for different parties and how this reasonable solution can be found. Game theory considers both the expected behavior and the actual behavior of the different sides and studies the optimization strategy. The idea of game theory has existed since ancient times: China's "Military Science of Sun Tzu" is not only a military bible but also the first game theory monograph. Game theory has been widely used in economics, military planning, sport and business. Competitive behavior is ubiquitous in the field of information security. For instance, network attack and defense, cryptographic encryption and decryption, computer viruses and protection against them, information hiding and analysis, information warfare, and so on are all good examples. Because the information security essentially involves an offensive and defensive struggle between humans, game theory becomes a basis for cyberspace security.

2.3.2 *Information theory, control theory and system theory*

Information theory was founded by Shannon to solve problems in modern communication systems, control theory is founded by Wiener to deal with the technology of automatic control and system theory originating as a way to solve organizational and management problems. These are all independent scientific

theories, but they are closely related to each other and their development has tended toward integration and unification. These theories are also basic to information security.

Information theory is at the foundation of cryptography and information hiding. Information theory provides a mathematical analysis of the information source, keys, encryption and cryptanalysis, leverages uncertainty and the closeness to an exclusive solution to measure the security of the cryptosystem, clarifies important concepts such as that of a cryptosystem itself, perfect secrecy, pure cryptography, theoretical secrecy and practical secrecy, and lays a solid mathematical foundation for cryptography. Indeed the use of information theory marked the debut of cryptography as an independent discipline.

From the perspective of information theory, information hiding (embedding) can be understood as the transmission of a narrowband signal (hidden information) in a wideband channel (the original host signal) by spread spectrum communication technology. Although the hidden signal has certain energy, it is difficult to detect the energy distributed to any of the characteristics of the channel. Detection of hidden information is a weak signal detection problem in a noisy channel. Therefore, information theory provides a theoretical basis for information hiding.

System theory investigates the general patterns, structures and laws governing systems. The core idea of system theory is that any system is an organic unity and not just a mechanical combination or addition of individual components. The function of the system is not available when the components are isolated from one another.

Control theory (or cybernetics) investigates the general laws of control and communication in machines, living organisms and society. It studies how equilibrium states or stable states can be maintained in a changing environment. Control improves the function or the state of a controlled object by obtaining and using particular pieces of information. Thus, the basis of control theory is information and information transmission, and control is dependent on information feedback.

For information security compliance, the "wooden barrel principle" (Cannikin law) is the embodiment of system theory in the field of information security.

Protection, detection and response (PDR) is the basic strategy used to ensure the security of an information system and network. In an information system and network, the system's secure state is its equilibrium state or stable state. The intrusion of malicious software breaks balance and stability. Once such an intrusion has been detected, control information can be obtained and it is then possible to kill the malicious software, so that the system can be recovered into its secure state.

Information system security assurance is a systematic project. In order to ensure information system security, it is necessary to start from the underlying hardware and software of the system and to take overall comprehensive measures.

The above approach to information security has been proved in practice to be correct and effective. It conforms to the basic principles of system theory and control theory. This shows that system theory and control theory are fundamental to information system and cyberspace security.

2.3.3 *Theory of computation*

Many problems of cyberspace security are computing security issues, so the theory of computation is also part of the theoretical foundation of cyberspace security, including computability theory and computational complexity theory.

Computability theory is an area of mathematics focusing on the general nature of computation. It distinguishes between what is computable and what is not computable by establishing a mathematical model. For decision problems, computability theory focuses on what is decidable and what is undecidable.

Computational complexity theory leverages mathematical methods to quantitatively analyze the resources required for a computation, and studies the basic properties of various problems of computational complexity and the relations among them. Computability theory studies what is computable and what is not computable, but the computational task can be a theoretical computation or it can be carried out in principle. Computational complexity theory, on the other hand, investigates the more practical aspects of computation, such as how much time and how much storage space is needed to compute a problem class. Computational complexity theory also attempts to determine which problems are realistically computable

and which are theoretical computable but cannot realistically be computed because their complexity is too great.

Authorization is at the core of information system access control mechanisms. For an information system to be secure, its authorization system must be secure. According to computability theory, in general, the problem of whether a given authorization system is secure is undecidable, but some restricted authorization system security issues are decidable. Thus, general operating system security problems are undecidable, but a specific operation system security problem is decidable. For example, the famous "halting problem" is undecidable in general, but the halting problem for a specific problem is decidable. General computer virus detection is an undecidable problem, but detection of a specific computer virus is a decidable problem. This is why computability theory is one of the theoretical foundations of information system security.

In essence, cryptanalysis involves the solution of a mathematical problem. If this problem is theoretically uncomputable, then the cryptosystem is theoretically secure. If the problem is theoretically computable but its computational complexity is too great for realistic computation, then the cryptosystem is secure in practice, or computationally secure. A one-time cryptosystem has a password that is theoretically secure, but other cryptosystems can only be computationally secure. According to computational complexity theory, NPC problems are among the most difficult of NP-difficult problems. The construction of public key cryptosystems is often based on NPC problems in order to provide a sufficient degree of security. For example, the McEliece, Knapsack and MQ cryptosystems are based respectively on the facts that the general decoding of error-correcting codes, the solution of the general knapsack problem and the solution of multivariable nonlinear quadratic equations are all NPC problems. This shows that computational complexity theory is another component of the theoretical foundations of cryptography.

2.3.4 *Access control theory*

Access control is a central problem in information system security. The essence of access control is to allow authorized persons to perform operations to obtain particular resources, while preventing unauthorized persons from doing so. Many information security techniques can be regarded as access control. For example, identity authentication in network and other information systems is the most basic access control. Cryptographic techniques can also be seen as access control. The key in cryptographic techniques provides privileged access: If a person is in possession of the key, they can perform the operations necessary to obtain to get information with the key; without the key, they cannot do so. Similarly, information hiding techniques can also be regarded as access control. In this case, the hiding technique provides the privileged access: The hidden information can be obtained by a person who knows the hiding technique; otherwise, the hidden information cannot be obtained.

Access control theory consists of various access control models and authorization theories, for example, the matrix model, BLP model, BIBA model, the Chinese wall model, the role-based model (RBAC) and attribute encryption. Attribute-based encryption is a new type of access control, combining cryptography and access control.

Access control is an important technique and is widely applied in different fields of information security. Access control theory is therefore another essential component of the theoretical basis of cyberspace security.

2.3.5 *Cryptology theory*

Although cryptology was developed on the basis of information theory, during its development, cryptology has already gone beyond the boundaries of traditional information theory, and has led to the construction of some new theories, for instance, one-way trapdoor function theory, public key cryptography theory, zero-knowledge proof theory, and multiparty security computing theory, as well as aspects of cryptosystem design and analysis. From the point of view of applications, cryptology techniques are part of the common technology of information security and are widely used in many information security fields. Cryptology theory thus forms another component of the theoretical basis of cyberspace security.

In conclusion, the mathematics, information theory (including system theory and control theory) and the theory of computation (including computational complexity theory) form the theoretical foundations of the discipline of cyberspace security, with particularly important roles being played by game theory, access control theory and cryptography theory.

2.4 Methodology of cyberspace security

In 1637, Descartes published "Discourse on the Method". This work on problem-solving had a great influence on ways of thinking and on scientific research in the Western world. Descartes divided the research method into four steps:

1. Never accept a truth that one does not know oneself. For what one does not know, no matter what the authority behind the conclusion, can be suspected.

2. Decompose a complex problem into simpler and smaller problems as far as possible, and solve these problems one by one.

3. Rank these smaller problems from simple to complex, and solve the easiest problem first.

4. After solving all problems, combine their results and verify if the problem is completely solved.

Descartes' methodology highlights the decomposition of complex problems into smaller, more easily solved, problems; it is a strategy of divide and conquer. But this methodology ignores the particular relevance of each part and the influence of each on the others. In modern science, especially with the development of systems theory, it has been found that many complex problems cannot be solved by decomposition, since the original overall properties are lost after decomposition. So we must leverage systems theory and methodology, which leads to the emergence of systems engineering. Methodology has developed from traditional methodology to systems methodology.

Cyberspace security uses both a traditional methodology (divide and conquer) and a comprehensive system engineering methodology, and integrates them into an organic whole. It includes theoretical analysis, reverse analysis, experimental verification and technological implementation [7–9], which can be used independently or combined with one another. These methodologies can provide guidance in solving the problems of information security, and help promote the development of the discipline of cyberspace security. When applying these methodologies to analyze and solve problems of information security, emphasis should be given to systematic characteristics. That is, the problems of information security should be analyzed and solved through the use of low-level software and hardware of the information system.

Reverse analysis is essential to cyberspace security. This is because cyberspace security essentially involves a battle between offense and defense. As the "Military Science of Sun Tzu" pointed out: "you should know both the enemy and yourself". Knowing your enemy is to apply reverse analysis. Each branch of information security has two aspects of offense and defense. For example, cryptography is composed of cryptography and cryptanalysis, network security is composed of network defense and network attacks, and so on. Therefore, we must carry out research from the point of view of both the offensive and defensive sides. For example, in cryptography, it is necessary to study not only cryptography design but also cryptanalysis. In network security, it is necessary to study not only network defense but also network attacks. When designing network protection mechanisms, we must first carry out security threat analysis and risk assessment. These are concrete applications of the methodology of reverse analysis, and have been proved to be both correct and effective approaches.

When designing and analyzing information system security, not only technology is involved, but also organizational management, legal protection, and many other aspects. In addition, because humans are both managers and users of the system, human factors constitute the most important determinant of information system security. As the nature of information security is a confrontation between intelligent humans, it is not possible to effectively solve the problem of information security without considering human factors.

Therefore, regarding human factors as crucial, we should combine qualitative and quantitative analysis, being aware all the time that quantitative change will lead to qualitative change.

3 Cryptography

Cryptography is concerned with how to protect communication and information security in the presence of an adversary. Public research on cryptography has only a short history. The iconic events are the publication of Shannon's "Communication theory of secrecy systems" in 1949 and the development of the DES algorithm and public key cryptography in the 1970s. Later, many government-supported cryptography research projects were established, such as AES, NESSIE, eSTREAM, SHA3 and CAESAR. These projects give rise to many new ideas and methods and greatly promoted the development of cryptography. In addition, new application environments, such as cloud computing and big data, and new attack methods, such as side-channel attacks, led to new security requirements. As a result, many new research directions have emerged, such as homomorphic encryption, attribute-based encryption, functional encryption, program obfuscation encryption and leakage resilient encryption. In this section, we describe recent progress in cryptography from the aspects of cryptographic algorithms, cryptographic protocols, cryptographic implementation and key management security, and we briefly recommend some areas on which research should focus.

3.1 Cryptographic algorithms

The principal cryptographic algorithms are block ciphers, stream ciphers, MACs and hash functions, public key cryptography, and the authenticated encryption algorithm. In the 1970s, the US National Standards Institute (ANSI) published the famous DES national standards. With the development of networks and improvements in computing capacity, the disadvantage that the DES key is too short was gradually exposed. In the RSA race of 1999, the organization Distributed.net obtained the DES key by exhaustive search with 100000 ordinary computers in one day. In order to replace DES, the US National Institute of Standards and Technology (NIST) launched a competition for an advanced encryption standard (AES). After three rounds of screening, from the initial 15 candidate algorithms, NIST selected Rijndael as AES. AES is able to resist all known attacks, including differential attack and linear attack. Furthermore, it has very good properties in terms of memory requirement and speed of hardware and software implementation. After AES was released, the focus of theoretical research turned to analyzing the security of existing cryptographic structures, and a series of important advances were published [10–12]. A notable research direction in the area of block ciphers is the rapid development of lightweight cryptographic algorithms, which have broad requirements in real applications. Examples include PRESENT [13], LBlock [14], PRINCE [15], PRIDE [16] and Simplified AES [17], and security analyses on these new lightweight algorithms have been proposed.

At the beginning of the twenty-first century, algebraic attacks posed a great threat to LFSR-based stream cipher algorithms. Typically, the NESSIE plan, which ended in 2003, even rejected all candidate stream cipher algorithms. Since stream ciphers can be generated by adjusting the operational modes of block ciphers, many investigators, such as Shamir, queried whether there remained a need for a stream cipher of dedicated design. However, there was a counter-argument that stream ciphers for software applications with high throughput or hardware applications with highly restricted resources were valuable in practical applications. So the European research project ECRYPT launched the eSTREAM stream cipher design competition in 2004. After careful evaluation, four stream cipher algorithms (HC-128, Rabbit, Salsa20 and SOSEMANUK) that can be implemented with high throughput on software and three (Grain v1, MICKEY v2, and Trivium) that need low hardware resources were selected. The eSTREAM competition has greatly promoted the development of stream cipher design and analysis. In terms of algorithm design, two new research trends arose. One concerned the appearance of a nonlinear chaotic source in stream ciphers. The other involved the gradual integration of the design ideas of block ciphers into stream ciphers. In terms of algorithm analysis, some new methods of attack were proposed [18,19], such as fast correlation attack for LFSR [20], distinguish attack [21], high-order difference attack [22] and cube attack [23]. Chinese researchers obtained excellent theoretical results on stream ciphers [24,25]. Specifically, the ZUC algorithm [26] was selected as an international standard for LTE in 2011, which has greatly amplified China's voice in the field of next-generation wireless communication.

A hash function maps an arbitrary-length message into a fixed-length message. A hash function controlled by a secret key is called a message authentication code (MAC). Both hash functions and MACs can be used for authentication and digital signature and have very important practical applications. For example, it was found in 2012 that a new computer virus "Flame" is able to circumvent antivirus software. This is because Flame obtains a collision of the hash function that used in the Windows update process. It is then able to generate a digital signature for itself such that the antivirus software believes that Flame owns a legitimate digital certificate. After the breakthrough in attacking methods [27–30] achieved by Professor WANG XiaoYun on the famous hash functions MD5 and SHA-1, NIST launched the SHA-3 project in 2007. SHA-3 collected new hash functions all over the world. Eventually, Keccak was chosen as the final SHA-3 algorithm. The SHA-3 competition promotes the rapid development of hash functions and MACs. Many new kinds of structures and design methods have emerged, such as HAIFA, SPONG, wide pipe and double pipe. At the same time, there have been developments in associated security analysis methods [31–34]. The recent development of a practical homomorphism MAC represents a notable direction in terms of hash function and MAC design [35].

Authenticated encryption has emerged as an important research direction in recent years. The goal of authenticated encryption is to simultaneously provide confidentiality, integrity and authentication with a single cryptographic scheme. An authentication encryption scheme can be constructed through the OCB or CCM mode of a block cipher, but there is an efficiency. In 2013, NIST launched the CAESAR competition[1)] to construct an authentication encryption scheme. Since then, many authentication encryption schemes have been proposed, such as ALE, FIDES, and AEZ [36–42]. However, no one has yet completely mastered all the security issues in this emerging field, and a number of security problems [43–46] have emerged. Research on authentication encryption is likely to become one of the most popular research directions in the coming years.

Since Diffie and Hellman created the concept of public key cryptography (PKC) in 1976, many public key cryptosystems have been proposed, including RSA, ELGamal and elliptic curve cryptosystems. However, the key certificate management of PKC is very complex in practical applications. In order to simplify the key management, Shamir [47] proposed the concept of identity-based cryptography, and Boneh and Franklin [48] constructed the first practical scheme, based on a bilinear pairing technique. Subsequently, many excellent identity-based schemes [49–52] have been proposed. Many new types of public key cryptosystems have also been proposed and used in practical applications; these include certificateless encryption [53], broadcast encryption [54,55], attribute-based encryption [56–59], predicate encryption [60,61] and functional encryption [62,63]. In particular, attribute-based encryption, predicate encryption and functional encryption have become important techniques for solving data security and privacy protection problems in cloud environments.

Since the proposal of the Shor quantum algorithm, traditional public key algorithms, which are based on large-integer factorization or discrete logarithms, have faced a huge security threat. There is now an urgent need for public key cryptosystems that are able to resist quantum attack. The study of cryptosystems that are able to resist quantum computer attacks is called anti-cryptography quantum computing. Currently, anti-cryptography quantum computing algorithms include three kinds: physics-based quantum cryptography, biology-based quantum cryptography and mathematics-based quantum cryptography. The main areas of mathematics-based quantum cryptography are multivariable cryptosystems, ECC, lattice-based cryptosystems and Hash cryptosystems [5].

3.2 Cryptographic protocols

Cryptographic protocols implement a series of regulation steps to accomplish certain security functions for an information system. Usually, cryptographic protocols need two or more participators. For concrete applications, the scope of cryptographic protocols is very large. It includes not only identity authentication, key exchange, secret sharing, digital signature, zero-knowledge proof, multiparty secure computation and many other basic cryptographic tools, but also complex functions such as electronic voting.

1) Cryptographic competitions. http://competitions.cr.yp.to/index.html.

The concept of secret sharing was proposed by Shamir and Blakley. Its purpose is to split a secret into multiple pieces and hand these over to the care of different people. Only when the number of secret holders reaches a threshold can the original secret be recovered. Shamir realized a secret sharing scheme through Lagrange interpolation. Blakley constructed a secret sharing scheme with points in a multidimensional space. Secret sharing protocols are under continuous development [64], with linear secret sharing first to appear, followed recently by function secret sharing [65]. At present, secret sharing has become a basic tool to construct more complicated cryptographic protocols [66,67].

Zero-knowledge proof refers to a prover and a verifier. The prover lets the verifier believe that he knows a secret but does not reveal any information about the secret. This concept was proposed by Goldwasser, Micali and Rackoff [68] in 1985 and achieved by a series of interactions between the prover and the verifier. Subsequently, Santis et al. [69,70] proposed non-interactive zero-knowledge proof. Deng et al. [71,72] solved the simultaneous resettable conjecture problem in zero-knowledge proof. Zhao and Andrew [73] designed concurrent knowledge extraction for public key models. Zero-knowledge proof is the foundation of many kinds of security protocol, and has been widely used to achieve identity authentication, electronic voting protocols and many other application protocols. Some new models and methods [74,75] have recently appeared in particular applications [76] of zero-knowledge proof.

Secure multiparty computation is a distributed computing protocol executed by multiple participants. Each participant provides input parameters and gains calculation results. However, at the end of the calculation, no participant can obtain the inputs provided by the other participants. Secure multiparty computation came from the Yao millionaire question [77]. Initially, this question involved just two parties, but later a multiparty question [78] was proposed. Secure multiparty computation uses secret sharing, zero-knowledge proof, bit commitment [79] and casual transmission [80] as its basic tools. It can be used to construct electronic voting protocols and electronic auction protocols. In addition, it plays an important role in threshold signature, database query, data mining and privacy protection. In 1997, Goldwasser [81] gave a comprehensive summary of secure multiparty computation. In recent years, secure multiparty computation theory has continued to develop. Some new results, such as black box secure multiparty computation [82], suspendable secure multiparty computation [83] and non-interactive secure multiparty computation [84] are worthy of attention.

With the development of various new types of networks and applications, outsourcing computing [85,86], verifiable storage [87,88] and many new application protocols have been designed. With the new demands produced by cloud computing, the Internet of Things, vehicle network, the Internet+ and wisdom city, the design and analysis of cryptographic protocols are sure to undergo new developments.

3.3 Cryptographic implementation

Cryptographic algorithms include three forms of expression: mathematical, software and hardware. Usually, we say that a cryptographic algorithm is secure if it is secure mathematically. However, if we want to put a cryptographic algorithm to practical use, it has to be implemented in software or hardware form. A cryptographic algorithm that is secure mathematically is not necessarily secure in terms of software or hardware.

Side-channel attack uses the physical properties related to the implementation of the cryptographic algorithm to obtain exposed secret parameters in cryptographic operations. The calculational effort then needed in theoretical analysis can be reduced greatly. In 1996, Kocher [89–91] first proposed the side-channel attack and successfully analyzed RSA and DES by measuring the algorithm's execution time. Later, error [92,93], energy [94], radiation [95,96], noise, voltage and many other physical properties [97,98] were used in the side channel attack technique. It is worth to point out that Chinese investigators, GU DaWu , ZHOU YongBin and TANG Ming, have also made excellent contributions in this field. To resist side-channel attacks, many methods have been adopted, such as the use of a random instruction sequence or the addition of noise, masks or random delays. However, none of these methods can completely resist the more and more complex side-channel attacks that have been developed.

In 2008, Petite et al. [99] suggested that channel information leakage should be considered at the beginning of algorithm design and proposed a compact stream cipher algorithm. Dziembowski and

Pietrzak [100] further proposed the concept of leakage-resilient cryptography. The information that may be leaked from a channel is abstracted as a mathematical function. As a result, potential problems existing in the physical implementation are turned into mathematical problems again. Algorithms designed using this model are able to avoid possible security issues regarding physical devices. Recently, many leakage-resilient algorithms [101–104] using this approach, with different application targets, have been proposed. Leakage-resilient cryptography has become an important new research direction. Chinese investigators, such as YU Yu, have also done excellent work [105,106] in this field.

On the other hand, in many applications, attackers are able to invade the system and extract key information of the cryptographic system. Such an attack is called a white box attack. A method that is able to resist white box attack is called white box implementation [107,108]. It makes the key into a query table and distributes the table to the entire network such that each block appears to be independent of the key and an attacker cannot obtain the key directly. Several white box implementations have been proposed. At the same time, there have been several attacks [109] on these implementations. Thus, we have to say there are no white box cryptographic implementations that are widely accepted with regard to both security and efficiency. Since the significant progress that was achieved with obfuscation techniques [110] in 2013, an obfuscation-based white box cryptographic algorithm has been proposed. However, its efficiency still represents a bottleneck. Obfuscation techniques will probably become a method to guarantee the safety of cryptographic algorithms and keys.

3.4 Key management security

The secret key is the most important resource in any cryptographic system. The most effective way to attack a cryptographic system is by obtaining the secret key. The goal of key management is to ensure the safety of the whole life cycle of the secret key, including key generation, distribution, storage, usage, backup/restore, update, revocation and destruction.

Generally, secret keys should be generated randomly. A weak random number generator will directly decrease the security of a cryptographic system. For example, in 2013, Snowden revealed that the NSA had designed a pseudorandom number generation algorithm Dual_EC_DRBG, which hides a trapdoor, and established it as a standard through the NIST. Then, the NSA set Dual_EC_DRBG as the default random number generation algorithm in Bsafe security software by bribing the RSA company. As another example, researchers were able to obtain secret keys of the RSA algorithm by large-scale scanning of the RSA modules and then calculating the common factor of each pair of modules. This is possible primarily because when using a random number generator to generate an RSA private key, collision happens between private keys of different RSA systems.

As mentioned before, the secret key is usually generated by a random number generator, which includes a true random number generator (TRNG) and a pseudorandom number generator (PRNG). The TRNG generates random numbers by random factors in a physical environment. Recent research on TRNG has mainly focused on high-speed implementation [111], security analysis and entropy estimation theory [112, 113]. The randomness of the PRNG is obtained by a deterministic algorithm with the input parameter of a random seed. For both TRNG and PRNG, security analysis and detection are necessary before they are used.

With the wide application of embedded devices and wearable devices, the problem has arisen of how to protect the secret key in these devices. Physical unclonable functions (PUFs) [114] provide integration of key generation and storage protection. This technology uses the fingerprint of a physical chip combined with a temporary key generation algorithm to extract a user's secret key each time the key is needed. After the power has been turned off, no one can read the key through direct physical intrusion. Many low-cost and highly reliable PUF designs have been proposed, but they still require further study with regard to their security analysis and applications [115].

Currently, key management technology in communication network models is relatively mature. The key management system includes a hierarchical key structure and a standardized key agreement protocol. The key is stored in hardware or in ciphertext form, with secret sharing or key escrow being used to store/recover it. Key management with public key technology (PKI) has also matured. However,

key management technology is closely related to specific applications. A reasonable key management scheme must aim at a specific application. Cloud computing, the Internet of Things, big data and new application environments impose more requirements and challenges to key management. Thus, research on key management technology for these emerging applications is becoming an important direction.

3.5 Research focus

This section introduces several currently important research topics in cryptography. They are expected to develop into new research directions or to solve significant cryptographic problems. These topics include anti-cryptography quantum computing, lattice-based encryption, fully homomorphic encryption, procedure-confusing encryption, attribute-based encryption, functional encryption, and automatic cryptography design and analysis.

Currently, there are three types of anti-cryptography quantum computing: physics based quantum cryptography, biology-based quantum cryptography and mathematics-based quantum cryptography. The most mature scheme in quantum cryptography is quantum key distribution. Quantum key distribution is based on the basic principles of quantum mechanics and achieves unconditional security. China is at the forefront of studies and applications in this field. It should be pointed out that quantum cryptography is not only quantum key distribution. Quantum block ciphers and quantum public key cryptography are important aspects. However, the latter algorithms are not yet mature, being restricted by the need for further development of quantum computing complexity theory. More investment is needed. Since biology-based quantum cryptography is not based on calculation, it has the ability to resist quantum computing attacks. Chinese investigators have proposed DNA-based block cipher and public key cryptography schemes [116,117]. However, current DNA cryptography is mainly based on experimental technology. Without a theoretical basis, its design and application are not easy to accomplish. All of these shortfalls need to be studied in greater depth. Mathematics-based quantum cryptography at present basically includes multivariate cryptography, ECC cryptography, lattice-based cryptography and hash-based cryptography. Lattice-based cryptography and multivariate cryptography have attracted the most attention. Research has shown that many multivariate schemes are not secure, and indeed it is very difficult to design a secure and effective multivariate cryptosystem. Lattice-based cryptography has the advantages of security and efficiency and is considered to be the most promising form of anti-cryptography quantum computing.

The most mature protocol in quantum cryptography is quantum key distribution. So far, there have been a variety of quantum key distribution protocols based on different physical principles, transmission media and encoding methods, including the BB84 protocol [118], the B92 protocol [119], the EPR protocol [120], the differential phase protocol [121], the coherent one-way protocol [122], the continuous-variable protocol [123] and the counterintuitive protocol [124]. The security of the BB84 protocol is widely acknowledged. Although, in theory, the quantum key distribution protocols are absolutely secure, practical devices are not ideal. The research focus of quantum key distribution protocols has gradually turned to the issue of security combined with the development of practical systems, including measurement device-independent quantum key distribution protocols [125], half device-independent quantum key distribution protocols [126], completely device-independent quantum key distribution protocols [127] and others. It must be pointed out that quantum cryptography concerns not only quantum key distribution, but quantum encryption, signature, authentication and other cryptogrammic algorithms need further study.

Hard problems on lattices have not vary from worst case to average case and are widely considered to resist quantum computing attack. They play an important role in fully homomorphic encryption [123,128] as well. At present, hard problems on lattices have been used to construct standard CPA, CCA-secure public key encryption schemes [129,130], identity-based encryption schemes [131–133], digital signature schemes [134–137], key agreement protocols [138], blind transfer protocols [139] and hash functions [140]. In addition, the ideal lattice [141] makes lattice-based cryptosystem a practical proposition. However, since the difficulty level of hard problems on lattices is not entirely clear, compared with RSA, ECC and

other public key cryptosystems, assessing the security of lattice-based cryptography and choosing more precise parameters are subjects for further research.

Fully homomorphic encryption permits the use of ciphertext without knowledge of a secret key. The result after these operations is equivalent to that of the same operations after decryption because of the homomorphic nature. Fully homomorphic encryption has very important applications in cloud computing. The idea of fully homomorphic encryption was proposed by Rivest in 1978, but the first scheme [142] was proposed by Gentry in 2009. After this, a large number of fully homomorphic encryption schemes emerged. Currently, efficient fully homomorphic encryption schemes are mainly constructed based on the LWE problem [123,143] on an ideal lattice. Supported by the "ciphertext programmable" project of the US DARPA , fully homomorphic encryption has achieved important breakthrough in fast implementation [144–147]. Computational efficiency has been improved by five to six orders of magnitude compared with the Gentry scheme. Key numbers have also been reduced from GB magnitude to MB. Despite all this, the efficiency is still a long way from suitability for large-scale practical application. Improving the security of homomorphic encryption is another area that merits further study.

Program-confusion cryptography makes a program unrecognizable while preserving its original functionality. Initially, this function mainly used heuristic methods. In 2001, Barak et al. [120] gave the strict definition of program-confusion cryptography for the first time and made a systematic study. Since Grag et al. [110] achieved a breakthrough in the general undistinguishable confusion scheme in 2013, investigators in this field have developed deniable encryption [148] and a provable security global hash scheme under the standard model [149] in succession based on program confusion. Many difficult problems in cryptography have been solved and a new design method for general confusion [150,151] has been developed. However, its construction and safety reduction are very complex and of low efficiency. Recently, among the basic tools, multilinear mapping, which is need to construct the program-confusion scheme, has been attacked [152,153], and so program-confusion cryptography may need to be reviewed.

Both the ciphertext and key of attribute-based encryption are associated with a set of attributes. The encryptor is able to specify the attributes of receivers, such that only receivers that satisfy the encryption policy are able to decrypt the ciphertext. We can see that attribute-based encryption has the one-to-many property. Functional encryption can be regarded as extended attribute-based encryption. The encryptor not only determines the attributes that a decryptor should possess, but also determines the data (function) form that users can decrypt. For the function of flexible fine-grained access control, attribute-based encryption and functional encryption have become important tools in big data and cloud storage, and of course have become a major research focus of cryptography.

It is well known that high security intensity is a basic requirement for any cryptosystem. However, designing a cryptosystem with high security intensity is a very complex task. Secure cryptosystem design and automatic cryptosystem design are long-term goals. In [154,155], the design of cryptogrammic functions was studied with intelligent computing. These were important steps in the automatic design of cryptogrammic functions. In [156,157], cryptography and intelligent computing were combined, inspired by biological evolution, and the concept of evolution cryptography was proposed and then used to achieve automation of cryptosystem design and analysis. A summary of the relevant research results is given in [3]. In recent years, quantum intelligent algorithms have emerged. Chinese investigators have designed cryptogrammic functions with a quantum intelligent algorithm and have obtained good grades in the context of multi-index optimization. It should be pointed out that cryptosystems are complex systems. Their automatic design and analysis are not easy. However, in today's information society, it is clear that computers should play a more important role in cryptosystem design and analysis.

4 Network security

4.1 Security requirements

With the rapid development of wireless communication, mobile terminals, cloud computing and other emerging technologies, hierarchicalization, virtualization, aggregation and XaaS (X as a Service) have

been the main features of the next-generation networks [158] such as 5G, CPS (Cyber Physic System), and IoT (Internet of Things). There are four different layers in the future network model, namely, the perception layer, the transportation layer, the aggregation layer and the application layer. Various means of attack have brought great threats and challenges to the network security in each layer. Aiming at the security requirements in different layers, security protocol, network defense, access control, privacy preservation and other security mechanisms have been studied to protect information security during the procedures of information collection, transmission, storage and service provision in the network system.

4.2 Network security mechanism

4.2.1 *Security protocols*

The network is built upon protocols. Consequently, security protocols spread across different layers of the network and form the basis of network security. According to the security requirements of different layers, many different types of security protocols have been proposed, based on formal security proof methodology.

In the perception layer, key distribution protocols are the basic protocols to realize node authentication and confidential communication. Because of the characteristics of sensor networks, such as large number of sensor nodes and limited energy, key pre-distribution schemes are the main mechanisms in wireless sensor networks. Typical protocols include the BROSK protocol [159], the ZigBee protocol [160] and the LKMS protocol [161]. These protocols are easy to deploy, but their security is weak. To overcome this shortcoming, a scheme has been proposed in which any two sensor nodes share a different secret key. This scheme [162] is strongly secure. However, it is expensive in terms of storage. In a compromise between security and efficiency, a key chain enables each node to store several secret keys, thus reducing the key size. Typical protocols based on key chains include Gupta's random key chain scheme [163] and Huang et al.'s key distribution scheme based on the head of the cluster [164]. Besides these, there are an improved scheme using a hash chain [165], the multi-path key discovery scheme [166] and the key redistribution scheme [167]. In terms of designing routing protocols for sensor networks, the main focus has been on overcoming specific attacks by extending standard routing protocols and thus ensuring secure data routing.

In the transmission layer, the design of security protocols, which uses the TCP/IP transmission protocol model, includes access authentication protocols, secure routing protocols, end-to-end secure transmissions, secure handover protocols and roaming protocols for heterogeneous networks. In access authentication, protocols are vulnerable to various attacks because of the openness of the wireless network, which is an important current research topic in the design of security protocols. Most authentication protocols in WLAN are based on the 802.1x access control framework [168] and the EAP (Extensible Authentication Protocol) [169]. There are several typical protocols in the IETF standards, such as EAP-MD5, EAP-TLS, EAP-PEAP and EAP-AKA [170]. EAP-MD5 is the simplest, but its security is weak. EAP-TLS uses PKI to protect the authentication process, which is considered to be the most secure method. However, the message exchange process is complex and the authentication cost is high. In order to overcome this flaw, Li et al. [171] proposed a four-step handshake protocol with only two rounds of exchanges, which improves the efficiency of the authentication process. The use of anonymous protocols has become an important research topic in this field because of the increased requirements on users' privacy [172,173]. In secure routing and end-to-end secure transmission, typical protocols are IPSec and SSL/TLS. Security functions for data routing are defined in IPSec. The key management protocol IKE is applied to realize dynamic authentication among different entities and to generate the session keys used for the following communication [174]. SSL/TLS uses the X.509 authentication framework and then uses the session key generated during the authentication to ensure end-to-end confidentiality and reliability between two applications [175]. Extensions and improvements to these two protocols have been produced based on different scenarios. In a secure handover and roaming protocol for heterogeneous networks, LTE-WLAN is the classic scenario that most researchers focus on. In this scenario, typical protocols include TS 33.234 [176] proposed by the 3GPP group, a fast authentication protocol [177] based on elliptic curve

cryptography and an anonymous access protocol based on WAPI [178]. ZHAO YunLei and Andrew [179] have designed a type of OAKE protocol that is more secure and effective than the MQV/HMQV protocol.

In the aggregation and application layer, network attacks are aimed mainly at the data and software. Network defense, access control and privacy-preserving mechanisms are applied to ensure information security, where a protocol is used to implement these mechanisms.

4.2.2 *Network defense*

The openness and sharing of networks and the security vulnerabilities in protocols and software mean that networks face multiple types of security attacks. Attacks can be categorized into two groups: protocol attacks and application attacks.

Network protocol attacks mainly focus on the perception layer and the transportation layer. In the perception layer, because of the limited energy and weak security mechanism, sensor nodes are vulnerable to these attacks, which include jamming, tampering, collision, exhaustion, selective forwarding, sinkhole attack, Sybil attack and wormhole attack [180–182]. These attacks can be defended against by authentication, encryption, monitoring, probing, transmitting redundant packets and multipath routing [183]. In the transportation layer, typical network attacks are SYN flooding and TCP session hijacking. A firewall with data detection and filter is an effective defense against SYN flooding [184]. Using a secure communication protocol, such as SSL, can effectively defend against TCP session hijacking.

Application attacks mainly focus on the aggregation layer and the application layer, including attacks against the application server and malware intrusions. Attacks against the application server include DOS and DNS cache poisoning [185]. Deployment of a firewall and configuration of security policy can protect the application server from network attacks. Malware includes viruses, worms, Trojans, rootkits and botnets [186]. Malware detection technology can protect the system from the threat of malware. and can be categorized into anomaly-based detection, specification-based detection and signature-based detection [187]. According to the different methodologies, there are three types of detection technology: static detection, dynamic detection and hybrid detection.

4.2.3 *Access control*

Access control has been studied and applied in many security areas. A network system with various types of users and resources is a complex distributed system, where different users of various resources (network, data, and services) have different operating authorities. Thus, we need to study appropriate security policies according to security requirements to ensure information security during the operation of the service process.

In the perception layer and the transportation layer, user access authentication uses mainly access control with security authentication protocols and user identity management, for example the 802.1x access control framework. In this framework, only authenticated users can properly use the appropriate network resources.

In the aggregation layer and application layer, access control verifies the authority of the user accessing data and service resources. In the study of access control mechanisms, security policy is the key point. According to different types of policies, common access control models include the role-based access control model (RBAC) [188] and the task-based and behavior-based access control model (TBAC) [189]. In the RBAC model, permissions are assigned based on user identity. TBAC adopts dynamic authorization and a proactive security model to dynamically manage rights based on a user's or a program's behavior. However, RBAC and TBAC are coarse-grained access control models, whose scalability is limited. To this end, Goyal et al. [190] proposed attribution-based access control (ABAC), which is based on flexible and scalable access control policies that take account of the dynamic properties of users, resources and network environment. It also makes anonymous access possible. In addition, with the arrival of the big data age, fine-grained access control under a multi-data-source information service will become an important research topic [191].

4.2.4 *Privacy preservation*

In recent years, with the development of city informatization, more attention has been paid to preservation of privacy. In this section, we divide privacy preservation into two categories: One is the privacy preservation with regard to network-link information (e.g., routing information and privacy information about sender/receiver), the other is privacy preservation with regard to the sensitivity of data in the network.

For preserving link information in the network, most work has concentrated on the perception layer and the transportation layer [192]. During information transmission, an adversary can obtain some private information about users through tracking the transmission path. Hence, many security routing protocols are designed to protect the user's privacy. Normally, privacy-preservation methods in routing protocols are based on the random routing strategy. This means that not all packets are transmitted from source node to sink node, but are transmitted in directions far away from the sink node by the forwarding node with a certain probability. At the same time, the routing path is not fixed, but is generated randomly. Hence, the adversary cannot get the actual routing path to obtain the user's privacy information.

For preserving sensitivity information, methods can be divided into two categories. On the one hand, sensitivity information can be protected by hiding the local or total information. These methods are principally k-anonymity [193], l-diversity [194] and differential privacy [195]. On the other hand, encryption is used to protect security information (e.g., homomorphic encryption and secure multi-party computation). In the perception layer, privacy information includes inner privacy between nodes and external privacy in the network [196]. In the aggregation layer, sensitivity information can usually be protected by k-anonymity, l-diversity and differential privacy. In the application layer, most existing work has aimed at privacy preservation during the service process (e.g., location privacy). With the development of service composition technology in recent years, information flow control technology can be used to protect privacy information during the process of interaction among different services [197].

4.3 Future research

With the wide application of the Internet, the development of network technology has led to ubiquitous interconnection, mobilization, intellectualization, customizability and high speed. Hence, the security challenges are different from those in traditional network environments, and need to be further studied with innovative technologies against new backgrounds. In this section, we discuss five representative directions regarding the network security, which provide the reference base for the future development of network security.

4.3.1 *Security of mobile terminals*

With improvements in hardware and software technology, a mobile terminal can provide similar or even the same functions as a personal computer, and can become a kind of personal smart system with powerful portability and computing capacity. By using multiple network access technologies, such as IEEE 802.11, Bluetooth, GSM, GPRS and UMTS, it is possible for a mobile terminal to interconnect with various devices and share data with them. However, multiple network access makes mobile terminals targets of malicious software and users. Currently, the primary attacks on mobile terminal include wireless attacks [198,199], break-in attacks [200,201], infrastructure-based attacks [202,203], worm-based attacks, botnets and user-based attacks [204,205].

4.3.2 *Security of network devices*

As network devices become more intelligent, they are being confronted by the traditional security issues existing in computing systems. For example, the operating system in a smart router can be attacked by malicious users, which will lead to routing misforwarding or failure. Taking the router as an example, the primary security issues include DDoS attack, Man in the Middle attack [206,207], TCP reset attack [208] and attack on OSPF [209–211].

4.3.3 *Security in SDN*

Since control logic and data forwarding are tightly coupled to network equipment in the traditional Internet, management of the network control plane is complex, and, in addition, it is difficult to deploy new technologies on existing networks, which performs poorly with regard to flexibility and scalability. However, in software-defined networking (SDN), the control logic is separated from data forwarding, which reduces the complexity of the functions in the network device and improves the flexibility and operability of the implementation and deployment of new technology and protocols. Hence, SDN provides a flexible and customizable network topology and a virtualized network device, which can also effectively monitor data transmission and support the installation and uninstallation of various network protocols.

However, flexibility also brings security threats to SDN. In [212], it was considered that security threats exist mainly between the application layer and the controlling layer, including application authorization, authentication and isolation, and resolution of strategic conflict. With regard to the first issue, [212,213] provide corresponding analysis and solutions. In [214], a security-enhanced operating system on the control plane is presented that can solve the issue of resolution of strategic conflict. In [215], a network secure application development environment, named FRESCO, for SDN, is presented that ensures the security of SDN-based application development.

4.3.4 *Security of CPS*

Cyber physical systems (CPS) have become a new generation of intelligent systems, implementing a tight coupling and harmonization of computing and physical resources via a deep fusion of computation, communication and control. A CPS is actually a dynamic hybrid system composed of various distributed and asynchronous heterogeneous systems running in different time and space regions. Since a CPS exhibits cross-layer features, heterogeneity and a high degree of interconnection, the security challenges become more complex. In [216] six security challenges faced by CPS are presented: confidentiality, context blur, secure aggregation, topology blur, extendable trust management and privacy aggregation. The main content of CPS security is elaborated in [217] from five aspects: CPS security objectives and threats, security requirements, primary means of attack, security concerns, and solutions to security issues. In [218–220], security issues in CPS design and operation are discussed with regard to the aspects of security policy, security platform and security protocol, and solutions are presented.

4.3.5 *Security of 5G network*

5G is neither a simple wireless access technology nor several new wireless access technologies, but an integration of multiple new wireless access technologies and existing wireless access technologies (4G backward evolution technologies). Hence, to some degree, 5G is in a real sense a fusion network. A 5G terminal has software-defined wireless transmission, modulation and a new error control mode. Terminals can access and visit multiple types of wireless networks simultaneously, and switch among these networks according to service access requirements. In [221] five primary security challenges are presented, including the design of reconfigurable, adaptive and lightweight protection mechanism, and means of preventing attacks from the application layer. 5G is a fusion of new communication and network technologies, and it is described in [222] how the security challenges facing the 5G network actually exist in its components, such as security of SDCN, wireless network fusion security, and security of D2D and M2M.

5 Information system security

5.1 New developments in trusted computing

5.1.1 *New developments in trusted computing in China*

In China, the start of trusted computing has not been delayed and its level is not low; indeed the current level of development of trusted computing is gratifying, and China is at the forefront of trusted computing worldwide [1,2,4,223,224].

1. Trusted computing standards of China. China announced the following three trusted computing technology specifications in 2013. These specifications reflect the new progress in trusted computing technology in China.

(a) Motherboard function and interface of trusted platforms (GB/T 29827-2013). The core innovation here is that we improve the TPM of the Trusted Computing Group (TCG) and design our trusted platform control module (TPCM) [4]. The TPCM's main technological innovations are as follows:

• The root of trust for measurement (RTM), root of trusted storage (RTS) and root of trusted report (RTR) are integrated into the TPCM, which acts as the root of trust of the platform. The TCG's RTM is the software code at the beginning of the BIOS. The RTM is vulnerable to malicious attacks because it is placed outside the TPM. Security is improved when it is put in the TPCM.

• Active measurement feature. When the trusted platform starts, the TPCM first gets control of the platform and executes integrity measurement to key components of the trusted platform. The RTM is executed first when the TCG's trusted computing platform starts. This execution is performed by the CPU. If the platform has not been measured, then the execution of the RTM may be not trusted. After adopting an active measurement mechanism, the TPCM is the first component to get control of the system, and the execution of the RTM and the integrity measurement are conducted by the TPCM, which can ensure the security of integrity measurement.

• China's commercial cryptography hardware engine has been adopted. The cryptography algorithm of the TPCM complies with China's "Trusted Computing Platform Encryption Scheme (TCM)", and the hardware engine of China's commercial cryptography algorithm (SM2 and SM3, SMS4) has been adopted, which improves the processing speed.

• In order to improve the support to the operating system and applications, the TPCM adopts a high-speed PCI or PCI Express bus as the connection between it and the system. The TCG's "Trusted PC specification" uses an LPC bus to achieve the connection between the TPM and the southbridge chip. We believe that this technological solution adopted by the TCG is compatible with existing computers. Because of the low speed rate of the LPC bus, the use of high speeds cannot be supported. The TPCM uses a high-speed PCI or PCI-E bus, which could provide more powerful support for the operating system and applications.

• Enhanced identity authentication feature: leveraging the 7816 bus to realize authentication combined with a password and smart card. Fingerprint authentication can also be implemented. When the trusted platform module has a 7816 bus, it can easily support a smart card, so it can realize two-factor authentication with a password and a smart card. This is beneficial to improving the security of the platform.

• Implementing the TPCM's control to computer resources through an I^2C or GPIO bus (such as I/O and network control equipment). China's information security strategy is "security and controllability". Therefore, the trusted platform module should be able to control the resources of the platform, which is the main motivation for the design of the TPCM.

These innovations in the TPCM have a solid practical basis. In 2003, Wuhan University and a commercial company cooperated and developed China's first trusted computer (the SQY14 embedded cryptographic computer) [225], which achieved the main innovative points of TPCM. The SQY14 uses an embedded security module (ESM) [226]. The ESM is composed of a J2810 chip and a Chinese commercial cryptographic chip module, so the ESM supports Chinese commercial cryptography. The ESM leverages a 7816 bus to control the smart card system, and the smart card is both the user's identity certificate and the carrier of the user key. The ESM leverages the I^2C bus to control the important resources of the computer (such as the BIOS) and all the I/O ports, and it achieves active control of the computer resources. The log is made up of two parts: One is stored in the ESM and the other in the hard disk. The use of this two-level log can improve log security. It has been shown in practice that these security measures are very effective in improving the security of the SQY14 embedded cryptographic computer [225].

(b) Trusted Connection Architecture (TCA) (GB/T 29828-2013). The trusted network connection (TNC) is an important specification for the TCG. The purpose of the TNC is to extend trust from the

trusted platform to the network, thereby ensuring that the network is trusted. Practice has shown that the TNC is open, secure and systematic and has other favorable characteristics. However, the TNC has some obvious shortcomings:

• It only supports verification from network server to terminal, and lacks verification from terminal to network server. Clearly, the network server and the access terminal are not equal in this regard.

• Multiple entities need a lot of information interaction in the TNC, but there is no corresponding security protocol. Only some information about how messages are transferred is introduced.

• The TNC architecture is relatively complex and is difficult to extend, and the cost of implementation is high.

Because the scope of applicability and the scenario for the use of the TCA are similar to those of the TNC, when the TCA specification was drawn up, the TNC specification and technical route were used for reference. The TCA is based on the merits of the TNC while paying attention to its shortcomings. The TCA has the following innovative aspects [4]:

(i) The TNC is essentially a two-element structure, in which the network server is the controller and the access terminal is in a passive position. Therefore, only the network server can verify the access terminal, while there is no verification from terminal to network server. The TCA uses a triple-element framework. The access requester (AR) and the access controller (AC) act as a peer entity, while the policy manager (PM) provides support for bidirectional identity authentication and platform trustworthiness evaluation between the AR and AC. The AR has the same control capacity to the connection as the AC. This triple-element framework also makes the protocol and control mode of the three levels of TCA architecture significantly different from those of the TNC.

(ii) The triple-element framework needs a trusted third party to carry out the identity authentication and platform trustworthiness evaluation for the two peer entities participating in the network. In the TCA, the policy manager is a trusted third party, to achieve a two-way authentication between network and network access. This method not only simplifies the identity management, policy management and certificate management mechanisms, but also ensures two-way authentication between the terminal and the network.

(iii) The TCA's architecture is based on the triple-element entity peer authentication and access control (TePA-AC) method, over which China has independent intellectual property rights. The TCA's architecture uses a triple-element authentication extensible protocol (TAEP) to implement entity authentication in the network access control layer and supports sequence TAEP authentication and tunnel TAEP authentication. The TePA-AC is used to realize port access control, which supports two kinds of implementation methods of full port control and partial port control.

In order to reduce the difficulties involved in system implementation, the TCA adopts a bottom-up design pattern and supports full implementation. The protocol of the TCA has been defined in a unified manner so that all functions of protocol and interface support have been included in one specification. The TCA protocol supports protocol extensions by way of customized and reserved fields. The TCA product design personnel are therefore easily able to understand all the interface definitions and protocol processes.

(c) Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing (GB/T 29829-2013). The TSS software stack is the software middleware between the upper layer and the TPM, and provides a bridge for the upper software using the TPM chip. Practice has shown that the TSS has the advantages of security and high efficiency, and it is a successful product that plays an important role in trusted computing. However, there are some deficiencies in the TSS:

(i) The TCG's TSS specification adopts the ideas of hierarchy and modularity in architecture, but the introduction of too many objects in the abstract layer results in complex relationships and causes difficulties in development. In addition, this architecture is too complex for the embedded environment, so it is not conducive to the application of embedded systems.

(ii) The main goal of the TSS is to use the general management and access to the TPM, which lacks a monitoring mechanism.

The Functionality and Interface Specification of Cryptographic Support Platform for Trusted Com-

puting describes the functional principle and requirements of a trusted computing cryptographic support platform and defines the service interface specification for the application layer provided by a trusted computing cryptographic support platform [4]. The main differences between it and the TSS specification are as follows:

(i) The use of a Chinese commercial cipher algorithm.

(ii) Reduction and change in the protocol:

• It uses a self-designed AP protocol instead of a multiple authorization protocol from the TCG (OIAP, OSAP).

• It uses a symmetric encryption algorithm to protect the secrecy of the request and response data.

• For storage protection, it uses a symmetric cipher algorithm and its primary storage key uses the symmetric key; there are corresponding changes in the key transfer protocol as well.

(iii) Reduction of certificate. The TCG's TPM1.2 specification uses five kinds of certificates, while the Chinese specification only uses two: a cipher module certificate and a platform identity certificate. The platform identity certificate is a double certificate including a signature certificate and an encryption certificate.

(iv) Reduction of key type. The TCG's TPM1.2 specification uses seven kinds of keys, while the Chinese specification only uses four: an endorsement key (EK), a platform identity key (PIK), a storage master key (SMK) and user keys (UKs).

2. China's TCM/TPM2.0 chip. Nationz Technologies Co., Ltd. developed the world's first TCM/TPM2.0 chip in 2012, which supports China's commercial cipher algorithm. This chip has been certificated by the China Cipher Management Bureau, and is widely used in China and abroad.

textbf3. China's Kylin operating system. The Chinese government decided not to purchase the Windows 8 operating system in 2013, so there was an urgent need for Chinese enterprises to provide a secure operating system. The Standard Software Co., Ltd. has developed a trusted cloud computing operating system named Kylin. Kylin's main technical features are support for trusted boot (TBOOT), for China's TCM/TPM2.0 chip and for China's commercial cipher, implementation of the full trust chain from TCM/TPM to VM, support for Intel TXT and OAT technology, implementation of remote platform attestation based on OAT, and implementation of trusted cloud management. It is hoped that the Kylin operating system will be able to be widely deployed after various improvements have been implemented.

5.1.2 *New developments in TCG's trusted computing*

1. From TPM1.2 to TPM2. With the development and application of trusted computing technology, especially in the context of China's TCM technology, the TCG recognized the shortcomings in the design of the TPM. The TCG began to consider developing a new specification for the TPM in 2008, and released a public TPM2.0 specification on October 23, 2012 after a few years of preparation. After further improvements to TPM2.0, the TCG proposed the application of TPM2.0 to ISO/IEC specification in 2013. In June 2015, ISO/IEC accepted the TPM2.0 standard as the new international standard [227]. The Chinese government has voted for this, which means that they accept TPM2.0.

Compared with TPM1.2, TPM2.0 has many improvements, the most important of which are those to the cipher configuration and application.

(a) Cipher configuration is more effective.

• It supports multiple cipher algorithms. TPM1.2 is only configured with the public key cipher, there is no clear allocation of the symmetric cipher, and the public key cipher only supports RSA. TPM2.0 not only supports a public key cipher, but also supports a symmetric cipher. For the public key cipher, RSA, ECC and other ciphers are supported. For the symmetric cipher, both AES and other passwords are supported. For the hash function, SHA-384, SHA-3, and other hash functions are supported.

• It supports cryptographic algorithm replacement. TPM1.2 does not support replacement of cryptographic algorithms. With the discovery by Chinese investigators of security vulnerabilities in SHA-1 [27–30], TPM1.2 has become less suitable for many uses. TPM2.0 supports cryptographic algorithm replacement.

• It supports cryptographic algorithm localization. Because TPM2.0 supports cryptographic algorithm replacement, it allows different countries to use their own cryptographic algorithms, which allows localization of the cryptographic algorithm. The TPM2.0 specification places special emphasis on the full support of China's commercial cipher SMx.

(b) Cipher performance is improved.

• TPM1.2 uses only RSA public key cryptography, without any use of symmetric cryptography, so encryption and decryption speeds are very slow, and there are many kinds of certificates for which application and management are inconvenient. TPM2.0 has absorbed the advantages of TCM in China, with a symmetric cipher being used to encrypt the data and public key cryptography for signatures and authentication; therefore, not only is the cipher processing speed enhanced, but also the number of types of certificate key is reduced, which makes key application and management easier.

• TPM1.2 supports only RSA public key cryptography. Because the size of the RSA key is large, the software and hardware implementation scales are also large, and the key processing speed is slow. TPM2 supports RSA, ECC and other cryptographic algorithms. As the size of the ECC key is small, the hardware and software implementation scales are also small, and the key processing speed is fast.

(c) Key management is more reasonable.

• Key hierarchy and type. From the level division, TPM2.0 sets three key levels: firmware layer, endorsement layer and storage layer. The firmware layer is used to invoke the cryptographic resource of the BIOS, thus enhancing the cryptographic function of TPM2.0; this layer does not exist in TPM1.2. From the function division, TPM2.0 has three types of keys: endorsement key (EK), storage key (SK) and authentication key (which includes the signature key and authentication key).

• Key and certificate types are reduced in number. TPM1.2 defines seven kinds of keys and five kinds of certificates. Because there are so many types of keys and certificates, both application and management are very complex. One reason is that TPM1.2 defines key functions by means of key type. In contrast, TPM2 defines key types by key functions, such as defining a signature key for all signatures, thereby reducing the number of types of key. Accordingly, the number of types of certificate is reduced.

• The key generation scheme is more effective. TPM2.0 has two different keys: an ordinary key and a master key. The ordinary key is generated by a random number generator (RNG). When generating the master key, a seed is first generated by a RNG in the TPM, and then a key derivation function (KDF) is used to generate the master key based on this seed. TPM2.0 uses two kinds of KDF: the SP800-56A ECDH based on elliptic curves and the SP800-108 KDF based on HMAC.

(d) Support for virtualization.

• Cloud computing needs virtualization, but TPM1.2 does not support virtualization. In order to enable trusted computing platforms to support cloud computing, TPM.2.0 supports virtualization.

(e) There is enhanced security for key use.

• In TPM1.2, if the authorized data of the key is of low entropy, it is vulnerable to violent attack and man-in-the-middle attack. Because the key's handle is not authorized, an attacker can use another key to steal authorization data, thereby endangering the security of the key. TPM2.0 adds an auxiliary secret (salt) in the authorization data, and the authorization of the key handle is also improved. These improvements enhance security for key use.

• In TPM2.0, the name of the key is added in the HMAC, which can prevent key substitution attacks, to improve the security of the key.

(f) Unified authorization framework:

• In TPM1.2, there are different authorization methods for application, delegation application and migration objects, which makes management more complex. The privacy protection model in TPM1. 2 is not consistent: Sometimes it is necessary to use the TPM to protect privacy, and sometimes it is assumed that the operation system is involved.

• TPM2.0 uses a unified authorization framework, and the authorization method is extended, which allows the use of signature and HMAC to authorize, and allows for a combination.

Although compared with TPM1.2, TPM2.0 is greatly improved, and its security and availability are enhanced, the following problems remain in TPM2.0:

• TPM2.0 has not yet been widely applied, and its security can be confirmed only after the test of practice.

• TPM2.0 supports cryptography algorithm replacement and localization, but its compatibility and security in this multi-cryptographic algorithm environment need to be analyzed and verified.

• TPM2.0 is not compatible with TPM1.2. Thus, the transition from TPM1.2 to TPM2.0 requires a longer time.

Because the TPM2.0 specification is new, it has yet to be the subject of much academic research. In [228] a formal analysis of the key management API was carried out, and the flexible and scalable features of the digital signature were studied in [229]. A security problem of TPM2.0 key replication mechanism has been found [228,230] and a security enhancement scheme has been proposed. A security defect in the TPM2.0 policy authorization mechanism has also been proposed [231] and an improved scheme has been proposed also. It has been pointed out in [232] that there is still a vulnerability in the replacement of the key data block in TPM2.0, although this problem can be alleviated to some extent by access control of the application.

In summary, the TPM2.0 specification is an inevitable outcome of the development of trusted computing technology, and it appears that it will promote the development of this technology. This shows the extent of China's influence on the TCG.

2. From VISTA to WIN-10. The lack of support from operating systems for trusted computing is one of the main reasons why trusted computing lacks applications [1,2]. Microsoft has long been committed to supporting trusted computing by its operating systems during the development from VISTA to WIN-10. Owing to its excessive emphasis on security, VISTA neglected the issue of ease of use, and users were reluctant to adopt it. The development of WIN-8 drew upon the experience and lessons of VISTA, and strove to improve convenience for the user in the context of security. WIN-8 fully supports trusted computing.

(a) TBOOT: Based on support by the UEFI BIOS and TPM2.0 chip, a trusted boot of the computing platform is realized. Moreover, trusted measurement in the trusted boot is enhanced from the simple HASH value measurement of the TCG specification to a digital signature verification, which improves security.

(b) Early launch of antimalware (ELAM): In the trusted boot process, it is ensured by a digital signature that only the WIN-8 OS loader is loaded, and the early launch of antimalware can improve security.

(c) Reputation-based access control: The user's reputation is involved in access control, which is conducive to regulation of user behavior and creates a harmonious environment for application.

(d) Bitlock disk encryption system: WIN-8 retains the Bitlock disk encryption system of WIN-7, and uses TPM2.0 to implement key management, so as to improve security.

As the operating system is the manager of system resources, it is the basis of information system security [1,2,4,7]. In order to ensure China's information security, the Chinese government decided not to buy WIN-8. This decision is conducive to the development of operating system technology by domestic industry.

Although WIN-8 fully supports trusted computing and enhances security, users are still not satisfied with it. Therefore, Microsoft develop WIN-10, which was released in July 2015. WIN-10 has improved security of identity authentication, data protection, threat prevention, device security and other aspects. In order to adapt to the Chinese market, WIN-10 supports China's TCM/TPM2.0 chip. Whether users will like WIN-10 or not will only become clear once it has become more widely adopted.

5.2 Security of cloud computing systems

Cloud computing is service-oriented and usually divided into infrastructure as a services (IaaS), platform as a service (PaaS) and software as a service (SaaS). Cloud computing makes computing a public basic resource (like water, electricity and oil). International industry generally believes that cloud computing is first among the top ten strategic technologies. The Chinese government takes cloud computing to be one of the national key development areas.

However, the results of a cloud maturity survey in 2012 show that 41% of users have refused to adopt the cloud, the main reason for this being information security and privacy protection issues in cloud computing. Thus, information security and privacy protection are the biggest obstacles to the development of cloud computing.

Since cloud computing is service-oriented, it is bound to adopt a resource-sharing approach. Resource sharing leads to many information security problems: There are almost unlimited computing resources, but users do not know whether these resources can be trusted; services are available almost everywhere, but users do not know if these services are trustworthy; there is almost unlimited storage space, but users cannot sense the existence of data and cannot control their own data. Therefore, users are worried about using cloud computing because their data could be damaged, leaked or tampered with.

Trusted computing is a type of information security technology that improves the trustworthiness of a computer system. It is particularly suitable for improving the trustworthiness of the infrastructure and platform of an information system. Therefore, it is an inevitable choice for enhancing the trustworthiness of cloud computing.

5.2.1 *IaaS security*

Current research is mainly focused on the following four aspects when leveraging trusted computing to enhance the security of the cloud computing system infrastructure:

1. Trust model of cloud computing system. The trust model is the basis of trusted computing technology. When adopting trusted computing to enhance the security of a cloud computing system, it is first necessary to build a trust model of the system. Therefore, the relationship and interactions between the components of the system in booting, loading software and executing applications should be analyzed, especially with regard to the internal entities in the virtual machine environment. The methods of trust transfer, measurement and verification should then be analyzed. A trust model of cloud computing system can then be established on this basis.

2. Trusted computing base (TCB) for a cloud computing system. First, the security threats to the cloud computing system should be analyzed, and this should be followed by a study of the protection method and system in the face of security threats. One of the core issues here is the construction of the trusted computing base (TCB), which serves as the basis for the security of the cloud computing system. With the TCB as the basis of trust, the trust relationship can be expanded gradually, and a trusted cloud computing system can be constructed.

3. In the construction of a trusted cloud computing system, some specific security problems must be addressed.

4. In the security monitoring of a cloud computing system, the monitoring mechanisms and methods must be adapted to the virtual and multi-tenant environment in order to ensure the operational safety of the cloud computing system.

The dynamic integrity measurement framework and protocol of IaaS have been studied in [233–235] and the feasibility of these methods has been demonstrated by experiments.

5.2.2 *PaaS security*

The cloud operating system, database and other basic software are important bases for ensuring the security of cloud computing. There is no doubt that the cloud operating system, database and other basic software should support trusted computing. This is a very difficult task, as can be seen from Microsoft's VISTA to WIN-10. Although it is difficult, it is being tackled, as can be seen from the development of Microsoft's Windows and China's successful operating system Kylin in its versions 5.1.1 and 5.1.2.

The construction of a trusted execution environment and the provision of a secure and reliable cloud platform are core tasks for the platform layer. The construction method of a trusted virtual machine based on trust expansion was described in [236]. A virtual trusted platform based on TPM2.0 and its security were studied in [237]. The construction of trusted execution environment (TEE) based on

vDRTM and supporting multiple security levels was described in [238]. Monitoring of program running behavior in TEE was considered in [239].

5.2.3 *SaaS security*

Data security and software security are the two most important issues in SaaS security.

Data security provides users with a sense of integrity, availability, security and controllability. This area is currently the most active in the field of cloud security. The main techniques involve the use of cryptography and error correction coding technology [85–88,145–148].

The application of a cipher cannot be done without key management. Traditional key agreement protocols, such as the DH key agreement protocol, all require the same calculations on both sides. However, for cloud computing, the cloud platform has huge computing power, whereas the cloud endpoints' computing power is limited, so there is an asymmetry in terms of computing power. Therefore, traditional key agreement protocols are not suitable for cloud computing systems. A non-symmetric key agreement protocol is presented in [240]. The cloud platform and the cloud endpoint can obtain the same key using different calculations, with the platform undertaking a large amount of calculation and the endpoint only a small amount.

Software security is a difficult problem in information security. To ensure software security, the following methods are generally adopted. The first is to write secure code, which is an active method. However, it is difficult to ensure that this is done well enough. The second is to carry out security tests on software to find and then repair software security flaws. The third is to implement security monitoring of the software in operation (see Subsection 5.3).

China has developed trusted cloud computing to the level of industrial application. China's first trusted cloud server has been developed by Wuhan University in cooperation with Huawei Technologies Co., Ltd. The main technical features are support for the TCM/TPM2.0 chip, support for a Chinese commercial cryptographic algorithm, trusted boot (TBOOT), support for trusted measurement from the BIOS to the VM, support for TXT multi-times measurement technology, support for software security protection in a virtual machine environment and support for trust management of the cloud system.

This trusted cloud server is configured to Huawei Technologies' FusionCloud system and is used in the trusted telecom cloud (NFV), the Huawei trusted computing pool (TCP), etc. After obtaining real benefits from the use of this trusted cloud server, Huawei Technologies is further developing trusted routers and other trusted network products, to open up a new road to network security with trusted networks.

Wuhan University is also cooperating with Inspur Co., Ltd. to develop a trusted cloud server for use in Inspur's trusted cloud system.

The application and practical use of these trusted cloud servers from Huawei and Inspur show that trusted computing technology has an important role to play in ensuring the integrity of cloud server resources, security of the virtual environment, security of data storage and defense against malware intrusions, among other aspects.

It must be pointed out that the adoption of trusted computing does not exclude the use of other information security technologies; indeed, by integrating other information security technology with trusted computing, one can achieve better security.

Cloud computing security assurance is a complex systems engineering task, and although various information security measures have been adopted, there is still much to be done and further research is ongoing.

5.3 Software security

Software (or program) behavior refers to the state evolution process when software runs. It can be described at different levels: from underlying binary instructions to high-level program statements, functions, system calls, etc. The behavior model of software considers the behavior state sequence and the state change depending on behavior information at a given level. It can characterize normal behavior of

software, as well as detecting abnormal behavior. If defects exist in software sources and the software execution environment cannot be trusted, then software will deviate from its expected behaviour under software hacker attacks or in an untrusted environment, resulting in unpredictable consequences. The aim of software security is to ensure that software behavior is as expected during the life cycle of the software.

The structure and behavior of software are analyzed from the point of view of software static analysis and dynamic analysis in [241]. In [242] a software assurance model is constructed from four dimensions: software state, software assurance service, software assurance measures and time.

5.3.1 *Software security threats*

Software security threats include denial of service, privacy leaks, privilege escalation, malicious code execution, and functional misuse, among others. A denial of service attack aims to exhaust the system's resources, such as through depletion of CPU, memory, network bandwidth, power and other resources. Privacy leaks in social networks and mobile devices are extremely common. In addition, side-channel attacks can also be used to obtain user's sensitive information, such as user's input, the current active window, sensitive input information [243,244] and mobile trajectory [245] from keystroke vibration. Privilege escalation can give an attack code a higher privilege, such as root privilege. If the attacker's component precedes the legal component, it will hijack this component, resulting in the privilege to upgrade [246]. Malicious code execution is one of the most malicious attacks, and an attacker can implant any code they want to execute, including common shellcodes, Trojans and worms, to hijack the normal execution flow of software. In feature misuse, an attacker can freely call to open API functions that are limited to the user, such as opening of browser plug-ins [247].

5.3.2 *Software security threat defense*

According to the principle of fault tolerance, N-version software technology can be used to achieve fault tolerance, which provides resistance to some attacks. In order to detect buffer overflow attacks, position and sequence were used in [248] to change the location or order of directives and data. Commonly used security defense techniques include address randomization, data randomization, instruction randomization and interface randomization. It should be noted that multi-version software technology can increase reliability and security, but also increases the cost of development and maintenance.

Software security detection is an important method to defend against threats to software security. The life cycle of shellcode includes three stages: the transmission phase, the loading phase and the execution phase. Therefore, detection of shellcode and defense against it can be carried out in three stages.

The detection of shellcode code and instructions contained in the network flow can allow shellcode to be found and blocked at the transmission stage. A signature-based detection method can be used for the detection of shellcode before loading. However, if shellcode uses ROP programming, the signature-based detection method is invalid. The integrity-based detection method is applied before shellcode execution. The execution of shellcode causes the program to deviate from its normal track and enter the illegal code area. If a legitimate PC (pointer program) jump table can be established, it is possible to detect shellcode. Behavior-based detection methods can be applied to the detection of shellcode, such as to the detection of an abnormal system API trace. It was shown in [249] that it is possible to identify the location of a user's action and a specific dialog box, and realize the user's intention and file association, so as to detect the download behavior of shellcode. Depending on a user's browsing behavior, it is possible to detect the download behavior of shellcode [247]. In addition, the exploit usage pattern detection method can detect shellcode by a certain exploit usage mode; for example, HeapSpray and HeapLib will allocate large heap memory in a short period of time and have a relatively fixed EIP jump address. It is also possible to detect shellcode by using the communication between exploit pattern detection modules [250]. This detection method depends on the vulnerability pattern, which is highly specific.

With regard to APT attacks, it is necessary to consider the overall security of a program over its whole life cycle, as in Microsoft's SDL (Security Development Lifecycle) process, involving requirements,

design, coding, testing, operation and maintenance security considerations, and also to consider the security assurance of the program running environment, including security assurance of the public library and the kernel library for program calls.

5.3.3 *Future research*

1. Design of secure and practical software security assurance mechanisms, including efficient fine-grained randomization schemes. Extending security defense from behavior monitoring to shellcode detection and advanced Trojan detection.

2. Designing new programming languages with easy markup codes, address and data randomization, access control to memory object resources, and memory object encryption and confusion. Programs can leverage these makeups to implement cooperative defense with operation system and security software.

3. For X86 systems, with loss of variable type information, a method that can accurately identify binary data structure should be designed, to restore semantic information of high-level programming languages in the binary layer and to construct an accurate and fine-grained software behavior profile.

4. Control flow analysis, data flow analysis, slice analysis and code instrumentation techniques should be combined to achieve a flexible and rich-feature vulnerability mining platform.

5.4 Embedded system security

5.4.1 *Industrial control system security*

In 2010, hackers successfully attacked an Iranian nuclear plant using an APT attack, which led to more than 70% of the uranium enrichment centrifuges being damaged and seriously affected Iran's nuclear program. This incident illustrates how a software attack can cause the destruction of hardware devices, and exposes the vulnerability of industry control systems. In this particular attack, the Stuxnet virus played a central role, and means to prevent such attacks have become a core issue in industrial control system security.

Industrial control systems are fundamentally important for national security and for people's livelihoods, so ensuring the security of China's industrial control systems has been an urgent strategic task.

Adopting trusted computing technology in industrial control systems is an effective measure to improve the trustworthiness of these systems [1,2,4,223,251]. However, compared with ordinary computer systems, industrial control systems have particular features that must be taken into account:

1. Industrial control systems require not only high security, but also high reliability.

2. Most industrial control systems must meet the requirements of timeliness, and therefore so must any security measures.

3. Many industrial control systems have the characteristic that once they are turned on they will run indefinitely. This imposes the requirements of multiple measurements on trusted computing, in contrast to the approach adopted, for example, to a PC.

5.4.2 *TrustZone*

TrustZone is a security technology that has been adopted by ARM to build a trusted execution environment (TEE) for systems [252]. The overall idea of TrustZone is that hardware and software resources are divided into two separate areas by the system architecture: the secure world and the normal world. Each area's work mode includes a user mode and a privileged mode. ARM leverages its bus system to ensure that the resources of the secure world are not accessible by the normal world. Software located in the normal world can only access the resources of the normal world, whereas software located in the secure world can access all the resources in both worlds. There is also a monitor mode in the secure world. This monitor mode is connected with the privileged modes of the two worlds. Monitor mode is used to achieve switching between the two worlds.

When the user mode of the normal world wants to obtain service from the secure world, first of all it needs to enter the privileged mode of the normal world, then the secure monitor call instruction is called and the processor will enter into monitor mode. The context of the normal world will be stored in

monitor mode, and then the privileged mode of the secure world will be loaded, in which the execution environment belongs to the secure world. After that, the user mode of the secure world is loaded and the corresponding service is provided.

After powering on the ARM, first the bootloader in ROM will initialize key peripherals, and then switch to the bootloader in flash memory, after which the OS in the secure world starts up. Finally, the bootloader of the normal world is activated to load the OS in the normal world. System startup is then complete. In the startup process, a signature verification protocol based on RSA is used for software authentication. In addition, during the startup process, the later-loaded components must pass verification by the loaded components, thus constituting a trust chain. Therefore, the bootloader in ROM is a trusted root. Thus, TrustZone uses a trusted computing mechanism.

According to the results of current research, TrustZone is generally secure, although an integer overflow defect has been found [253].

The following problems are worthy of further study. First, there has been insufficient security analysis of TrustZone. TrustZone security relies mainly on access control of the bus, which needs to be thoroughly studied. Second, although the TrustZone startup process uses the trusted chain technology of trusted computing, it lacks TPM and other trusted computing technology. Therefore, the possibility of combining TrustZone with TPM and other trusted computing technology should be investigated. Third, there have not been many practical implementations of TrustZone, and therefore possible applications should be sought, so that problems can be found and solved during practical use.

6 Security of information content

In the global information age, the Internet will developed in an open, heterogeneous, mobile and dynamic direction. Through this continuous evolution, the next-generation Internet, 5G mobile communication networks, the mobile Internet, networking, and other forms of new networks and cloud computing service models will arise. Meanwhile, with the global influence of the Industry 4.0 and China's implementation of the "Internet +" , the trend of deep integration of the Internet and traditional industries is irreversible. The Internet and its extended technology bring great convenience in information access, mutual communication and collaborative work. It directly contributes to the transformation and upgrading of related industries. However, the Internet has also brought some negative effects. Pornography and reactionary and other harmful information is spread largely via the Internet. Spam and similar misconduct has become rampant. Movie, music and software copyright infringements are conducted through the Internet. Network fraud, violence and terrorist attacks through phishing take place. Such behavior is a complete departure from the original intention of the originators of the Internet, and it is not in the interests of the majority of Internet users. Therefore, in the process of building the information society, it is an important part of national information construction to improve the level of guarantee of information security and the ability to monitor a variety of adverse information on the Internet.

Security of information content technology utilizes computers to automatically acquire, recognize and analyze specific security-related topics through the Internet, which acquires massive amounts of information and is subject to rapid changes. Depending on the network environment, this is also known as network content security. Security of information content is an important means to manage information dissemination. It is a core component of the network security system and of great significance for improving network efficiency, purifying the Internet space and ensuring social stability.

Devoting great efforts to promote informatization is a strategic measure of China's modernization, as well as an urgent requirement and an inevitable choice for implementing the scientific concept of development and building an innovation-originated nation and prosperous society. As a core technology of intelligent information processing in the context of network security, security of information content provides technical support for building advanced network culture and strengthening the online dissemination of advanced socialist culture, which is an important component of the national information security system. Therefore, research on security of information content is not only important from an academic perspective but also of great social significance.

6.1 Security threats to information content

In the Internet, telecommunication, television and other network information sharing environments, content security faces threats including leakage, spoofing, destruction and tampering [254–258]. In detail, these can be described as follows:

1. The network contains a lot of public information, such as persons' names, affiliations, e-mail addresses and phone numbers. Since the cost of acquisition of this public information is very low, it can be obtained with ease and could be abused in some cases. For example, some companies will sell such data as commercial information. Some scam groups will use this information to commit fraud. Therefore, information leakage on the network can also refer to the dissemination of specific information to a specific person or organization in order to hinder the normal life or work of that person or organization.

2. Openness and autonomy of a networks can lead to information being published and shared on the network by each organization autonomously. This gives rise to the threat of fraud. There is the possibility of fake network addresses and website content because networks cannot guarantee integrity of information (especially for information sources).

3. Information can be disseminated illegally. There are widespread breaches of intellectual property rights with regard to music and movies.

4. Information may be tampered with in the dissemination process. The purpose of information tampering may be to eliminate the source of information to prevent it from being traced. Information content can be forged. In addition, viruses or Trojans may be introduced into information, seriously endangering the security of computer information systems.

6.2 Network information content acquisition

6.2.1 *Acquisition process of network media information*

In contrast to network communication information acquisition for specific points, the scope of network media information acquisition links can be the whole of the Internet. Traditional network media information acquisition links are obtained from the initial network address set, which is fixed in advance. The initial network address set contains a certain number of URLs. First the published content corresponding to each network addresses of the initial set is obtained. On the one hand, the network media information acquisition link then selectively stores the initial network address information subject content in an Internet information database [259–261], according to a series of content-heavy sentence mechanisms. On the other hand, the network media information acquisition link further extracts embedded hyperlink network addresses of the acquired information. All hyperlink network addresses are placed in an awaiting acquire address queue. The "first in first out" method is used to individually extract the information for each network address in the queue. The network media information acquisition link cycle then carries out the following behavior until the required network range has been traversed: acquisition of the network address information from the awaiting acquire queue [262]; extraction of acquired information subject content [263,264]; heavy sentence and information storage [265–267]; extraction of acquired information on the embedded network address stored in the awaiting acquire address queue. The ideal acquisition process for network media information involves principally the initial URL set-information "seed" collection, the URL awaiting acquire queue, the information acquisition module, the information analysis module, the information heavy-sentence module and the Internet information database.

6.2.2 *Typical tools for network media acquisition*

A web crawler is the typical tool for the implementation of information acquisition on the Internet. A web crawler is a program or script that automatically captures Internet information according to a certain rule. Information published on the Internet is decentralized and independent, but different pieces of information are connected to each other [268–271]. The reason why web crawlers are also called spiders is that they shuttle through the Internet, which is built by hyperlinks.

There are huge information resources on the Internet. With limited network resources, Internet spiders must be selective. For different service objects, the behavior of web crawlers can be divided into two

categories. One class of web crawler serves search engines and other search applications. Its information-grasping rules cover as many Internet sites as possible, and the depth of search of a single site is not high. Another class of web crawler serves targeted information collection. For example, a public sentiment analysis system requires that its web crawler have a high search depth and a certain theme selection capability. A crawler with high search depth is called a path-traced crawler, and deeply and thoroughly examines the whole resources of a given site. A crawler with theme selection capability is called a theme crawler. Such a crawler will judge whether a resource is a user-specified topic, and will continue to search until it is able to grab a web page about a given topic.

Web crawlers generally use distributed mechanisms to ensure full and timely information acquisition. Because Internet resources are huge and downloading takes time, web crawlers use multiple processes, multiple threads and even distributed modes to download multiple network resources (text, picture, audio, video, etc.) at the same time. That is to say, this is group work, with crawlers gathering together to complete a task (which is why web crawlers are also called ants). In order to prevent media sites from judging a web crawler to be malicious, it needs to avoid too frequent acquisition of information. On the one hand, the periodic traversal time interval can be appropriately selected to prevent network media overload caused by information acquisition. On the other hand, in order to avoid denial of service to the target network media, periodic modifications are applied to the network client information request content.

6.3 Extraction and selection of information content and features

Representation of information content and selection of feature items is a basic problem of information retrieval in data mining, which quantifies the key words extracted from the information to represent text information. It translates them from a raw unstructured form into structured content that can be handled and recognized by a computer; in other words, it abstracts the information content scientifically and establishes a mathematical model to describe and replace the original information content. This enables the computer to calculate and operate with this model to recognize information content.

Because text is a kind of unstructured data, it must first be translated into a structured form that can be processed in order to tap useful information from a large amount of text. Text selection has a very important influence on the filtering, classification, clustering and automatic summary of text, on the discovery of user interest patterns and on knowledge discovery. It calculates scores for each characteristic according to a feature evaluation function, then sorts these features by the scores, and selects some of the highest of scores as feature words; this is feature selection [272,273]. Feature selection uses a number of well-established methods. Most of these are statistical in nature. The signal-to-noise ratio (SNR) is a tool from the field of signal processing; it indicates the difference between signal intensity and background noise. If we look at the feature item as a signal, then the SNR of the feature item can be treated as a measure of identification of the feature item when classifying the text. Information gain is often used in the field of machine learning, in particular to build decision tree classifiers. Information gain also uses the concept of entropy, as well as the statistical relationship between feature items and category labels as an evaluation index. Judgment using chi-square statistics is based on correlation between feature items and category labels. If a feature item and a category occur simultaneously, this indicates that the feature item provides a good representation of the category. When simple feature selection cannot meet the requirements of information representation, the feature needs to be reconstructed. Feature reconstruction takes the feature items as input and combines or converts them to generate a new set of items as output.

For audio content, it is very important that sufficient analysis and extraction be performed on physical characteristics (e.g., spectral characteristics), auditory characteristics (e.g., loudness and timbre) and semantic features (e.g., voice keywords, melody and rhythm) [274–276]. Audio retrieval can be divided into voice search, music search and music example search according to differences in search target and search method. For audio retrieval, the first step is to establish a database, extracting features from audio data and clustering the data by feature. The search engine then matches the feature vector and the cluster parameter set and sorts the data according to relevance, before sending the result to the user through

the query interface. Extraction of the characteristics of the audio signal, which means time-domain and frequency-domain feature extraction, is aimed at distinguishing audio data with different content. Therefore, the selected feature should be able to fully reflect the physical and auditory characteristics so as to adapt to changes in the environment. During audio feature extraction, audio is usually divided into segments of equal length. There is a divided frame in each segment. Thus, there are two types of feature extraction: fragment-based and feature-based.

Digital images contain large amounts of information and there is strong correlation between pixels compared with text messages. Therefore, the methods for processing digital image differ considerably from those for processing text. An image feature tray mainly includes the following aspects:

1. Color feature extraction of the image [277]: The color features of the image in the form of a feature vector can be used to represent the distribution of image color. Common expressions of color characteristics include color histograms, color coherence vectors and color moments, among others.

2. Texture feature extraction of the image [278]: Feature vectors can be used to represent the texture (brightness variation) characteristics. Texture information is a combination of brightness and spatial information, reflecting the changes in the brightness of the image. Common texture features are GLCM, Gabor wavelet features and Tamura texture features.

3. Other image features [279,280]: In addition to color and texture features, there are image classification and retrieval systems that use edge features and contour features.

6.4 Information content analysis and processing

The basic processing of huge amounts of information content involves matching, classification and filtering. Other problems with more complex processes can be dealt with by some combinations of these. For applications to information retrieval and text editing, the most common requirement is rapid matching of user-defined modes or phrases. In the process of text information filtering, matching algorithms are of great use. A highly efficient matching algorithm can allow fast and accurate information processing.

6.4.1 *Information content classification*

Classification algorithms have important applications in image classification, indexing and content understanding. Their main function is to divide images into different categories according to their content, through analyzing differences between various image features in different image categories [281,282]. Decades of research and practice have led to dozens of classification methods. Any classifier can be abstracted as a learning process, with learning consisting of supervised learning and unsupervised learning.

6.4.2 *Information filtering*

Information filtering is a typical operation in large-scale content processing. It filters the continuously arriving information, selecting information that meets users' demands. In that process, the desired information is saved, with the rest being filtered out [283]. Hanani gives another definition of information filtering from a novel viewpoint [284] in which information filtering can be considered as selecting information in line with users' interests from the dynamic information flow, assuming that users' interests are static, remaining unchanged over a long period of time. Information filtering often removes data from the input dataflow, rather than just finding them there.

In fact, in the field of content security, information filtering provides an efficient information flow, removing or reducing information overload, and disordered or inappropriate information. However, the development of information filtering is still in its early stages. Eliminating inappropriate information through information filtering is one of the most important tasks in content security. Information filtering technology involves many different classification methods. There is active information filtering and passive information filtering. Depending on the location of the filter, it can be divided into filtering in the information source, filtering on the server and filtering on the client. Depending on the filtering method, it can be divided into content-based filtering, user-interest-based filtering and Synergia filtering. Depending on the method of knowledge acquisition, it can be divided into explicit mode and implicit mode.

Information filtering can be applied to many fields, including search result filtering, user email filtering, server/news group filtering, browser filtering and user interest recommendation.

6.5 Monitoring and early warning for Internet public sentiment

A monitoring and early warning system can analyze magnanimity information on the Web and extract effective information that can be used as a basis for decisions by governments [285]. At present, both domestic and foreign departments of governments and research institution, especially in Western developed countries, have put significant resources into the development of the technology and application of these systems. As a result, this technology has developed in an all-round way [286]. A considerable amount of attention has been paid to capturing all kinds of political, military and cultural information through the Internet for the purposes of strategic planning. Taking the United States as an example, in order to improve the ability of governments to grasp information, John D. Negroponte was appointed as the first National Intelligence Director, with his main focus on the integration and expression of information.

The trends in Internet public sentiment monitoring technology can be summarized as follows:

1. Intensive collection of information based on information sources. The robot in a traditional search engine generally uses the breadth-first search policy to traverse the Web and download documents. The system maintains a hyperlink queue (or stack) that contains some starting URL. The robot starts from this URL and downloads the corresponding pages. It then puts a new hyperlink into the queue (stack). The processes is repeated recursively until the queue (stack) is empty. However, the search engine technologies represented by Google, Hotbot and Baidu, which are universally known as "Big search", cannot meet the requirements of an Internet public sentiment monitoring system. Concretely speaking, the main problem of "Big search" technology is that the rate of extracting information from fixed-point information sources on the Web (generally defined as bits extracted/total bits of information source) is quite low.

2. Fusion analysis of heterogeneous information. One of the essential characteristics of Internet information is its highly heterogeneous nature. This means that information exhibits great differences in coding, data format and structural composition. A prerequisite for analyzing and extracting magnanimity information is to organically integrate the information with an integrated representation or standard and obtain a valuable comprehensive analysis. At present, the fusion analysis of heterogeneous information can be divided into two categories. In one, the resource is integrated with a data format of high expansibility, such as XML(Extensible Markup Language). Another approach is to apply an abstract fusion analysis based on semantemes and other information in the application's upper layer, such as the RDF (Resource Description Framework).

3. Structured expression of unstructured information. Unlike the processed objects of a traditional information analysis system, a number of objects that are to be analyzed based on Web information are in the form of unstructured information. It is easy for a human reader to understand the unstructured information, but quite difficult for a computer information analysis system. After much effort by statisticians, artificial intelligence experts and computer systems professionals, many excellent methods have been developed to provide an accurate and effective analysis of unstructured data.

With the popularity of the Internet, the content available is varied, with both good and bad aspects. The traditional pure "Huge-crowd" strategy cannot meet the needs of media information monitoring. The job of Internet forum detectives is based on capturing and analyzing media content. First, it is necessary to ensure a sufficient rate of extraction of data from the target site, in other words, a high level of performance of the extraction part of the monitoring of information. In monitoring Internet forums, the monitors must be skilled at unearthing target information sources at depth, depending on the practical requirements of Internet censorship. In addition, the dynamic content that is generated by dynamic scripts is of supreme importance. Considering the functional totality and product availability, Internet media information monitoring work is performed with different structures and types of data source. The pick-up circuits of the relevant monitoring products should have the properties of universality and extensibity.

6.6 Integrated management and control for network information content

Network administrative techniques are a generic term for various means of supervising, organizing and controlling network communication services and processing information. The purpose of adopting network administrative techniques is to ensure that a computer network can continuously operate and solve problems immediately in exceptional situations. In order to ensure the security of information content systematically, it is necessary to implement integrated management and control for network information content [287]. With the development of new network applications and technologies, various security threats, such as illegal access and malicious attacks, are appearing and evolving. Firewalls, VPN, IDS, defensive methods against various attacks, identity authentication, data encryption, security audits and some management systems have been widely used in networks. These security products can play a role in some specific fields, but most of them cannot be used with the others: There is a "security island". Further, there is no efficient management scheduling mechanism for these security products, and because they cannot cooperate with each other, it is difficult for them to achieve their full application performance. From the perspective of security management of information content, it is necessary to monitor the running status of the various security products in a network from a unified interface, and uniformly summarize, analyze and audit the vast amount of log information or alarm messages, while updating these security products and alerting users or responding to attack events.

In addition, information content management and related security issues become more and more complicated in large networks. Network managers of information content must analyze information and events by combining all the relevant devices with the system, and only in this way can they handle the newer and more complex security issues that arise. Therefore, it is necessary for network managers to establish a new type of overall network security management system, with an integrated security management platform for information content. With this platform, it should be possible to control multifaceted and distributed security systems over the whole network while achieving centralized monitoring of various network security resources, together with unified management, intelligent audit and interaction among a variety of security function modules. Such a platform can efficiently simplify network security management for information content, enhance the level of security, improve controllability and manageability, and reduce financial costs.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant Nos. 2014CB340601, 61332019, 61379139, U1135002, U1405255, 61431008, 2013CB329603). We would like to thank the following for their help in writing this article: FU JianMin, ZHANG LiQiang, YUAN Wei, XI Ning, LU Di, WU Jun.

References

1 Shen C X, Zhang H G, Feng D G, et al. Information security survey (in Chinese). Sci China Ser E-Inf Sci, 2007, 37: 129–150
2 Shen C X, Zhang H G, Feng D G, et al. Survey of information security. Sci China Ser-F: Inf Sci, 2007, 50: 273–298
3 Zhang H G, Qin Z P. Introduction to Evolution Cryptology (in Chinese). Wuhan: Wuhan University Press, 2010
4 Zhang H G, Zhao B. Trusted Computing (in Chinese). Wuhan: Wuhan University Press, 2011
5 Zhang H G, Wang H Z, Yang C, et al. Post Quantum Cryptology (Translation in Chinese). Beijing: Tsinghua University Press, 2015
6 Zhang H G, Guan H M, Wang H Z. Current research of post quantum cryptography (in Chinese). Cryptography Development Report of China 2010. Beijing: Electronics Industry Press, 2011, 1–31
7 Information Security Professional Instruction Committee-Information Security Professional Specification Project Group. Information Security Majority Insructive Specification (in Chinese). Beijing: Tsinghua University Press, 2014
8 Zhang H G, Du R Y, Fu J M, et al. Information security discipline (in Chinese). Netw Secur, 2014, 56: 619–620
9 Zhang H G, Wang L N, Du R Y, et al. Information security discipline system structure research (in Chinese). J Wuhan Univ, 2010, 56: 614–620
10 Bar-On A, Dinur I, Dunkelman O, et al. Cryptanalysis of SP networks with partial non-linear layers. In: Proceedings

of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 315–342
11 Sun S W, Hu L, Wang P, et al. Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 158–178
12 Emami S, Ling S, Nikolić I, et al. Low probability differentials and the cryptanalysis of full-round CLEFIA-128. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 141–157
13 Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher. In: Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, Vienna, 2007. 450–466
14 Wu W L, Zhang L. LBlock: a lightweight block cipher. In: Proceedings of the 9th International Conference on Applied Cryptography and Network Security, Nerja, 2011. 327–344
15 Borghoff J, Canteaut A, Güneysu T, et al. PRINCE—a low-latency block cipher for pervasive computing applications. In: Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, 2012. 208–225
16 Albrecht M R, Driessen B , Kavun E B, et al. Block ciphers—focus on the linear layer (feat. PRIDE). In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 57–76
17 Gilbert H. A simplified representation of AES. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 200–222
18 Papakonstantinou P A, Yang G. Cryptography with streaming algorithms. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 55–70
19 Banegas G. Attacks in stream ciphers: a survey. http://eprint.iacr.org/2014/677.pdf
20 Ågren M, Löndahl C, Hell M, et al. A survey on fast correlation attacks. Cryptogr Commun, 2012, 4: 173–202
21 Hell M, Johansson T, Brynielsson L. An overview of distinguishing attacks on stream ciphers. Cryptogr Commun, 2009, 1: 71–94
22 Knellwolf S, Meier W. High order differential attacks on stream ciphers. Cryptogr Commun, 2012, 4: 203–215
23 Dinur I, Shamir A. Applying cube attacks to stream ciphers in realistic scenarios. Cryptogr Commun, 2012, 4: 217–232
24 Zhang J M, Qi W F, Tian T, et al. Further results on the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. IEEE Trans Inf Theory, 2015, 61: 645–654
25 Yang D, Qi W F, Zheng Q X. Further results on the distinctness of modulo 2 reductions of primitive sequences over $Z/(2^{32-1})$. Designs Codes Cryptogr, 2015, 74: 467–480
26 ETSI/SAGE TS 35.222-2011. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3. Document 2: ZUC Specification
27 Wang X Y, Yu H B, Yin Y L. Efficient collision search attacks on SHA-0. In: Proceedings of the 25th Annual International Cryptology Conference, Santa Barbara, 2005. 1–16
28 Wang X Y, Yin Y L, Yu H B. Finding collisions in the full SHA-1. In: Proceedings of the 25th Annual International Conference on Advances in Cryptology, Santa Barbara, 2005. 17–36
29 Wang X Y, Lai X J, Feng D G, et al. Cryptanalysis of the hash functions MD4 and RIPEMD. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 1–18
30 Wang X Y, Yu H B. How to break MD5 and other hash functions. In: Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques. Berlin/Heidelberg: Springer-Verlag, 2005. 19–35
31 Jian G, Peyrin T, Yu S, et al. Updates on generic attacks against HMAC and NMAC. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 131–148
32 Jian G, Yu S, Lei W, et al. Cryptanalysis of HMAC/NMAC-Whirlpool. In: Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, 2013. 21–40
33 Leurent G, Peyrin T, Wang L. New generic attacks against hash-based MACs. In: Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, 2013. 1–20
34 Peyrin T, Yu S, Lei W. Generic related-key attacks for HMAC. In: Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, 2012. 580–597
35 Catalano D, Fiore D. Practical homomorphic MACs for arithmetic circuits. In: Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, 2013. 336–352
36 Bogdanov A, Mendel F, Regazzoni F, et al. ALE: AES-based lightweight authenticated encryption. In: Proceedings of the 20th International Workshop on Fast Software Encryption, Singapore, 2013. 447–466
37 Bilgin B, Bogdanov A, Knežević M, et al. Fides: lightweight authenticated cipher with side-channel resistance for constrained hardware. In: Proceedings of the 15th International Workshop on Cryptographic Hardware and

Embedded Systems, Santa Barbara, 2013. 142–158
38 Hoang V T, Krovetz T, Rogaway P. Robust authenticated-encryption AEZ and the problem that it solves. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 15–44
39 Sarkar P. Modes of operations for encryption and authentication using stream ciphers supporting an initialisation vector. Cryptogr Commun, 2014, 6: 189–231
40 Lu X H, Li B, Jia D D. KDM-CCA security from RKA secure authenticated encryption. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015: 559–583
41 Joo C H, Yun A. Homomorphic authenticated encryption secure against chosen-ciphertext attack. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 173–192
42 Andreeva E, Bogdanov A, Luykx A, et al. How to securely release unverified plaintext in authenticated encryption. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 105–125
43 Wu S, Wu H, Huang T, et al. Leaked-state-forgery attack against the authenticated encryption algorithm ALE. In: Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, 2013. 377–404
44 Dinur I, Jean J. Cryptanalysis of FIDES. In: Proceedings of the 21st International Workshop on Fast Software Encryption, London, 2014. 224–240
45 Nandi M. Forging attacks on two authenticated encryption schemes COBRA and POET. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 126–140
46 Wang P, Wu W L, Zhang L T. Cryptanalysis of the OKH authenticated encryption scheme. In: Proceedings of the 9th International Conference on Information Security Practice and Experience, Lanzhou, 2013. 353–360
47 Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in Cryptology. New York: Springer-Verlag, 1985. 47–53
48 Boneh D, Franklin F. Identity-based encryption from the Wail pairing. In: Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, 2001. 586–615
49 Dan B, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext. In: Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin/Heidelberg: Springer-Verlag, 2005. 440–456
50 Waters B. Efficient identity-based encryption without random oracles. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 114–127
51 Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 22–41
52 Blazy O, Kiltz E, Pan J. (Hierarchical) identity-based encryption from affine message authentication. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 408–425
53 Al-Riyami S S, Paterson K G. Certificateless public key cryptography. In: Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, 2003. 452–473
54 Dan B, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Proceedings of the 25th Annual International Cryptology Conference, Santa Barbara, 2005. 258–275
55 Dan B, Waters B, Zhandry M. Low overhead broadcast encryption from multilinear maps. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 206–223
56 Sahai A, Waters B. Fuzzy identity-based encryption. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 457–473
57 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and Communications Security. New York: ACM, 2006. 89–98
58 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of the IEEE Symposium on Security and Privacy. Washington DC: IEEE, 2007. 321–334
59 Chen J, Gay R, Wee H. Improved dual system ABE in prime-order groups via predicate encodings. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 595–624
60 Garg S, Gentry C, Sahai A, et al. Witness encryption and its applications. In: Proceedings of the 45th Annual ACM Symposium on Theory of Computing. New York: ACM, 2013. 467–476
61 Gentry C, Lewko A B, Waters B. Witness encryption from instance independent assumptions. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 426–443
62 Waters B. Functional encryption: origins and recent developments. In: Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, 2013. 51–54
63 Barbosa M, Farshim P. On the semantic security of functional encryption schemes. In: Proceedings of the 16th

International Conference on Practice and Theory in Public-Key Cryptography, Nara, 2013. 143–161
64 Farràs O, Hansen T, Kaced T, et al. Optimal non-perfect uniform secret sharing schemes. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 217–234
65 Boyle E, Gilboa N, Ishai Y. Function secret sharing. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 337–367
66 Jarecki S, Kiayias A, Krawczyk H. Round-optimal password-protected secret sharing and t-pake in the password-only model. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 233–253
67 Cramer R, Damgård I B, Döttling N, et al. Linear secret sharing schemes from error correcting codes and universal hash functions. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 313–336
68 Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems. In: Proceedings of the 17th Annual ACM Symposium on Theory of Computing. New York: ACM, 1985. 291–304
69 de Santis A, Micali S, Persiano G. Non-interactive zero-knowledge proof systems. In: Proceedins of CRYPTO'87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, 1987. 52–72
70 BFM M B, Feldman P, Micali S. Non-interactive zero-knowledge proof systems and applications. In: Proceedings of the 20th Annual Symposium on Theory of Computing. New York: ACM, 1988. 103–112
71 Deng Y, Lin D D. Instance-dependent verifiable random functions and their application to simultaneous resettability. In: Proceedings of the 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, 2007. 148–168
72 Deng Y, Goyal V, Sahai A. Resolving the simultaneous resettability conjecture and a new non-black-box simulation strategy. In: Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science. Washington DC: IEEE, 2009. 251–260
73 Andrew C, Zhao Y L. Concurrent knowledge extraction in public key models. J Cryptol, 2014, doi: 10.1007/s00145-014-9191-z
74 Goyal V, Jain A, Ostrovsky R, et al. Constant-round concurrent zero knowledge in the bounded player model. In: Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, 2013. 21–40
75 Unruh D. Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 755–784
76 Kiltz E, Wee H. Quasi-adaptive NIZK for linear subspaces revisited. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 101–128
77 Yao A. Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, Washington DC: IEEE, 1982. 160–164
78 Goldreich O, Micali S, Wigderson A. How to play any mental game. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York: ACM, 1987. 218–229
79 Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: analysis and applications. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 281–310
80 Asharov G, Lindell Y, Schneider T, et al. More efficient oblivious transfer extensions with security for malicious adversaries. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 673–701
81 Goldwasser S. Multi party computations: past and present. In: Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM, 1997. 1–6
82 Kiyoshima S. Round-efficient black-box construction of composable multi-party computation. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 351–368
83 Ishai Y, Ostrovsky R, Zikas V. Secure multi-party computation with identifiable abort. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 369–386
84 Beimel A, Gabizon A, Ishai Y, et al. Non-interactive secure multiparty computation. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 387–404
85 Wang C, Ren K, Wang J. Secure and practical outsourcing of linear programming in cloud computing. In: Proceedings of 30th IEEE International Conference on Computer Communications, Shanghai, 2011. 820–828
86 Gentry C, Halevi S, Raykova M, et al. Outsourcing private RAM computation. In: Proceedings of the 55th Annual Symposium on IEEE Foundations of Computer Science, Philadelphia, 2014. 404–413
87 Sheng B, Li Q. Verifiable privacy-preserving sensor network storage for range query. IEEE Trans Mob Comput, 2011, 10: 1312–1326
88 Cui H, Mu Y, Au M H. Proof of retrievability with public verifiability resilient against related-key attacks. IET Inf Secur, 2014, 9: 43–49
89 Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Proceedings of the 16th Annual International Cryptology Conference, Santa Barbara, 1996. 104–113

90 Kelsey J, Schneier B, Wagner D, et al. Side channel cryptanalysis of product ciphers. In: Proceedings of the 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, 1998. 97–110

91 Dhem J F, Koeune F, Leroux P A, et al. A practical implementation of the timing attack. In: Proceedings of the 3rd International Conference, CARDIS'98, Louvain-la-Neuve, 2000. 167–182

92 Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults. In: Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, 1997. 37–51

93 Joye M, Lenstra A K, Quisquater J J. Chinese remaindering based cryptosystems in the presence of faults. J Cryptol, 1999, 12: 241–245

94 Kocher P, Jaffe J, Jun B. Differential power analysis. In: Proceedings of the 19th Annual International Cryptology Conference, Santa Barbara, 1999. 388–397

95 Quisquater J J. A new tool for non-intrusive analysis of smart cards based on electromagnetic emissions. Eurocrypt 2000 Rump Session, 2000

96 Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: concrete results. In: Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems, Paris, 2001. 251–261

97 Belaid S, Fouque P A, Gérard B. Side-channel analysis of multiplications in $GF(2^{128})$. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 306–325

98 Lomné V, Prouff E, Roche T. Behind the scene of side channel attacks. In: Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, 2013. 506–525

99 Petit C, Standaert F X, Pereira O, et al. A block cipher based pseudo random number generator secure against side-channel key recovery. In: Proceedings of the ACM Symposium on Information Computer and Communications Security. New York: ACM, 2008. 56–65

100 Dziembowski S, Pietrzak K. Leakage-resilient cryptography. In: Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science, Philadelphia, 2008. 293–302

101 Dachman-Soled D, Liu F H, Zhou H S. Leakage-resilient circuits revisited-optimal number of computing components without leak-free hardware. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 131–158

102 Dziembowski S, Faust S, Skorski M. Noisy leakage revisited. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 159–188

103 Longo J, Martin D P, Oswald E, et al. Simulatable leakage: analysis, pitfalls, and new constructions. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 223–242

104 Bitansky N, Dachman-Soled D, Lin H. Leakage-tolerant computation with input-independent preprocessing. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 146–163

105 Yu Y, Standaert F X, Pereira O, et al. Practical leakage-resilient pseudorandom generators. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010. 141–151

106 Standaert F X, Pereira O, Yu Y. Leakage-resilient symmetric cryptography under empirically verifiable assumptions. In: Proceedings of the 33rd Annual Cryptology Conference, Santa Barbara, 2013. 335–352

107 Chow S, Eisen P A, Johnson H, et al. White-box cryptography and an AES implementation. In: Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography, Newfoundland, 2003. 250–270

108 Xiao Y, Lai X. A secure implementation of white-box AES. In: Proceedings of the 2nd International Conference on IEEE Computer Science and its Applications, Jeju, 2009. 1–6

109 M ulder Y D, Roelse P, Preneel B. Cryptanalysis of the Xiao-Lai White-Box AES implementation. In: Proceedings of the 19th International Conference on Selected Areas in Cryptography, Windsor, 2013. 34–49

110 Garg S, Gentry C, Halevi S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits. In: Proceedings of the 54th IEEE Annual Symposium on Foundations of Computer Science, Berkeley, 2013. 40–49

111 Cherkaoui A, Fischer V, Fesquet L, et al. A very high speed true random number generator with entropy assessment. In: Proceedings of the 15th International Workshop on Cryptographic Hardware and Embedded Systems, Santa Barbara, 2013. 179–196

112 Fischer V, Lubicz D. Embedded evaluation of randomness in oscillator based elementary TRNG. In: Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems, Busan, 2014. 527–543

113 Ma Y, Lin J, Chen T, et al. Entropy evaluation for oscillator-based true random number generators. In: Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems, Busan, 2014. 544–561

114 Ravikanth P, Ben R, Jason T, et al. Physical one-way function. Science, 2002, 297: 2026–2030

115 Delvaux J, Gu D, Schellekens D, et al. Secure lightweight entity authentication with strong pufs: mission impossible. In: Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems, Busan, 2014. 451–475

116 Lu M X, Lai X J, Xiao G Z, et al. Symmetric-key cryptosystem with DNA technology. Sci China Ser-F: Inf Sci, 2007, 50: 324–333

117 Lai X J, Lu M X, Qin L, et al. Asymmetric encryption and signature method with DNA technology. Sci China Inf

Sci, 2010, 53: 506–514
118 Bennett C H. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. New York: IEEE, 1984. 175–179
119 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124
120 Barak B, Goldreich O, Impagliazzo R, et al. On the (im)possibility of obfuscating programs. J ACM, 2012, 59: 1–48
121 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM, 2012. 309–325
122 Böhl F, Hofheinz D, Jager T, et al. Practical signatures from standard assumptions. In: Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, 2013. 461–485
123 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. SIAM J Comput, 2014, 43: 831–871
124 Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis. J Cryptol, 2012, 25: 601–639
125 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
126 Pawlowski M, Brunner N. Semi-device-independent security of one-way quantum key distribution. Phys Rev A, 2011, 84: 010302
127 Vazirani U, Vidick T. Fully device-independent quantum key distribution. Phys Rev Lett, 2014, 113: 140501
128 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009. 169–178
129 Regev O. On lattices, learning with errors, random linear codes, and cryptography. J ACM, 2005, 56: 84–93
130 Peikert C. Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009. 333–342
131 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008. 197–206
132 Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis. J Cryptol, 2012, 25: 601–639
133 Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 22–41
134 Lyubashevsky V. Lattice signatures without trapdoors. In: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, 2012. 738–755
135 Micciancio D, Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller. In: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, 2012. 700–718
136 Ducas L, Durmus A, Lepoint T, et al. Lattice signatures and bimodal Gaussians. In: Proceedings of the 33rd Annual Cryptology Conference, Santa Barbara, 2013. 40–56
137 Böhl F, Hofheinz D, Jager T, et al. Practical signatures from standard assumptions. In: Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, 2013. 461–485
138 Zhang J, Zhang Z, Ding J, et al. Authenticated key exchange from ideal lattices. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 719–751
139 Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer. In: Proceedings of the 28th Annual International Cryptology Conference, Santa Barbara, 2008. 554–571
140 Lyubashevsky V, Micciancio D, Peikert C, et al. SWIFFT: a modest proposal for FFT hashing. In: Proceedings of the 15th International Workshop on Fast Software Encryption, Lausanne, 2008. 54–72
141 Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, 2010. 1–23
142 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009. 169–178
143 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans Comput Theory, 2014, 6: 169–178
144 Alperin-Sheriff J, Peikert C. Practical bootstrapping in quasilinear time. In: Proceedings of the 33rd Annual Cryptology Conference, Santa Barbara, 2013. 1–20
145 Alperin-Sheriff J, Peikert C. Faster bootstrapping with polynomial error. In: Proceedings of the 34th Annual Cryptology Conference, Santa Barbara, 2014. 297–314
146 Rohloff K, Cousins D B. A scalable implementation of fully homomorphic encryption built on NTRU. In: Proceedings of FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, 2014. 221–234
147 Kurt Rohloff. Enabling practical, secure computing through fully homomorphic encryption. DIMACS Workshop on Multicore and Cryptography, 2014, 22
148 Sahai A, Waters B. How to use indistinguishability obfuscation: Deniable encryption, and more. In: Proceedings of

the 46th Annual ACM Symposium on Theory of Computing. New York: ACM, 2014. 475–484
149 Hohenberger S, Sahai A, Waters B. Replacing a random oracle: full domain hash from indistinguishability obfuscation. In: Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, 2014. 201–220
150 Gentry C, Lewko A B, Sahai A, et al. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. IACR Cryptology ePrint Archive, 2014, 2014: 309
151 Ananth P, Gupta D, Ishai Y, et al. Optimizing obfuscation: avoiding Barrington's theorem. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2014. 646–658
152 Cheon J H, Han K, Lee C, et al. Cryptanalysis of the multilinear map over the integers. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015. 3–12
153 Hu Y P, Jia H W. Cryptanalysis of GGH Map. Cryptology ePrint Archive, Report 2015/301, 2015
154 Millan W, Clark A. Smart hill climbing finds better Boolean functions. In: Proceedings of the 4th International Workshop on Selected Areas in Cryptography, Ottawa, 1997. 50–63
155 Clark J A, Jacob J L. Two-stage optimisation in the design of Boolean functions. In: Proceedings of the 5th Australasian Conference on Information Security and Privacy, Brisbane, 2000. 242–254
156 Zhang H G, Feng X T, Qin Z P, et al. Evolutionary cryptosystems and evolutionary design for DES. J China Inst Commun, 2002, 23: 57–64
157 Zhang H G, Feng X T, Qin Z P, et al. Evolutionary cryptosystems and evolutionary design for DES. Chin J Comput, 2003, 26: 1678–1684
158 ITU-T, Y.3001. Future Networks: Objectives and Design Goals. 2011
159 Lai B, Kim S, Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. In: Proceedings of IEEE Workshop on Large Scale Real-time and Embedded Systems, Austin, 2002. 7
160 Alliance Z. Zigbee specification document 053474r06. v1.0. Technical Report, ZigBee Alliance, 2004. ITU-T, Y.300
161 Dutertre B, Cheung S, Levy J. Lightweight key management in wireless sensor networks by leveraging initial trust. Technical Report SRI-SDL-04-02, SRI International, 2004
162 Chan H, Gligor V D, Perrig A, et al. On the distribution and revocation of cryptographic keys in sensor networks. IEEE Trans Dependable Secur Comput, 2005, 2: 233–247
163 Gupta A, Kuri J. Deterministic schemes for key distribution in wireless sensor networks. In: Proceedings of the 3rd InternationalConference on Communication Systems Software and Middlewareand Workshops. Washington DC: IEEE, 2008. 452–459
164 Hwang D D, Lai B C C, Verbauwhede I. Energy-Memory-Security Tradeoffs in Distributed Sensor Networks. In: Proceedings of the 3rd International Conference, ADHOC-NOW 2004, Vancouver, 2004. 70–81
165 Shan T H, Liu C M. Enhancing the key pre-distribution scheme on wireless sensor networks. In: Proceedings of IEEE Asia-Pacific Services Computing Conference, Yilan, 2008. 1127–1131
166 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proceedings of IEEE Symposium on Security and Privacy. Washington DC: IEEE, 2003. 197–213
167 Law C F, Hung K S, Kwok Y K. A novel key redistribution scheme for wireless sensor networks. In: Proceedings of IEEE International Conference on Communications. Washington DC: IEEE, 2007. 3437–3442
168 IEEE. IEEE Standard for Local and Metropolitan Area Networks: Port-based Network Access Control. IEEE 802.1X-2004. 2004
169 IEEE. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Acess Control (MAC) Security. IEEE STD 802.11i/D4, 2003
170 Allen J, Wilson J. Securing a wireless network. In: Proceedings of the 30th Annual ACM SIGUCCS Conference on User Services. New York: ACM, 2002. 213–215
171 Li X, Bao F, Li S, et al. FLAP: an efficient WLAN initial access authentication protocol. IEEE Trans Parall Distrib Syst, 2014, 25: 488–497
172 Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. IEEE Trans Consum Electron, 2004, 50: 231–235
173 Jiang Q, Ma J, Li G, et al. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wirel Pers Commun, 2013, 68: 1477–1491
174 Doraswamy N, Harkins D. IPSec: the New Security Standard for the Internet, Intranets, and Virtual Private Networks. Englewood Cliffs: Prentice Hall, 2003
175 Rescorla E. SSL and TLS: Designing and Building Secure Systems. Boston: Addison-Wesley, 2001
176 Patil A, Sawant H K. Technical Specification Group Services and System Aspects, IP Multimedia Subsystem (IMS). Int J Electron Commun Comput Eng, 2012, 3: 234–238
177 Idrissi Y, Zahid N, Jedra M. Security analysis of 3GPP (LTE)WLAN interworking and a new local authentication method based on EAP-AKA. In: Proceedings of International Conference on Future Generation Communication Technology. Washington DC: IEEE, 2012. 137–142
178 Jiang Q, Ma J F, Li G S, et al. The amalgamation based on WAPI end WLAN. Chin J Comput2010, 33: 1675–1686
179 Yao C C, Zhao Y. OAKE: a new family of implicitly authenticated diffie-hellman protocols. In: Proceedings of ACM

SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013. 1113–1128
180 Raymond D R, Marchany R C, Brownfield M, et al. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. IEEE Trans Veh Technol, 2009, 58: 367–380
181 Wood A D, Stankovic J A. Denial of service in sensor networks. IEEE Comput, 2002, 10: 54–62
182 Hu Y C, Perrig A, Johnson D B. Wormhole detection in wireless ad hoc networks. Technical Report TR01384. Department of Computer Science, Rice University, 2002
183 Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Commun ACM, 2004, 47: 53–57
184 Needham A B Y R, Lampson B. Network Attack and Defense. White Paper, 2008
185 Trostle J, van Besien B, Pujari A. Protecting against DNS cache poisoning attacks. In: Proceedings of the 6th IEEE Workshop on Secure Network Protocols. Washington DC: IEEE, 2010. 25–30
186 La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices. IEEE Commun Surv Tutor, 2013, 15: 446–471
187 Idika N, Mathur A P. A survey of malware detection techniques. Department of Computer Science, Purdue University, 2007, 48
188 Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control. ACM Trans Inf Syst Secur, 2001, 4: 224–274
189 Thomas R K, Sandhu R S. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. In: Proceedings of the IFIP TC11 WG11.3 11th International Conference on Database Securty XI: Status and Prospects. London: Chapman & Hall, 1999. 166–181
190 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006. 89–98
191 Yang K, Jia X, Ren K, et al. Enabling efficient access control with dynamic policy updating for big data in the cloud. In: Proceedings of the 33rd Annual IEEE International Conference on Computer Communications, Toronto, 2014. 2013–2021
192 Jose J, Jose J, Princy M. A survey on privacy preserving data aggregation protocols for wireless sensor networks. J Comput Inf Technol, 2014, 22: 1–20
193 Sweeney L. k-anonymity: a model for protecting privacy. Int J Uncertain Fuzz Knowl-Based Syst, 2002, 10: 557–570
194 Machanavajjhala A, Kifer D, Gehrke J, et al. l-diversity: privacy beyond k-anonymity. ACM Trans Knowl Discov Data, 2007, 1: 1–52
195 Dwork C. Differential privacy. In: Proceedings of the 33rd International Colloquium, ICALP, Venice, 2006. 1–12
196 Jose J, Jose J, Princy M. A survey on privacy preserving data aggregation protocols for wireless sensor networks. J Comput Inf Technol, 2014, 22: 1–20
197 Xi N, Sun C, Ma J, et al. Secure service composition with information flow control in service clouds. Future Gener Comput Syst, 2015, 49: 142–148
198 Makhlouf A, Boudriga N. Intrusion and anomaly detection in wireless networks. In: Zhang Y, Zheng J, Ma M, eds. Handbook of Research on Wireless Security. Hershey: Information Science Publishing, 2008. 78–94
199 Haataja K. Security threats and countermeasures in Bluetooth-enabled systems. University of Kuopio, 2009
200 Xie L, Zhang X, Seifert J P, et al. pBMDS: a behavior-based malware detection system for cellphone devices. In: Proceedings of the 3rd ACM Conference on Wireless Network Security. New York: ACM, 2010. 37–48
201 Becher M, Freiling F C. Towards dynamic malware analysis to increase mobile device security. 2008
202 Traynor P, Lin M, Ongtang M, et al. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009. 223–234
203 Enck W, Traynor P, McDaniel P, et al. Exploiting open functionality in SMS-capable cellular networks. In: Proceedings of the 12th ACM Conference on Computer and Communications Security. New York: ACM, 2005. 393–404
204 Becher M, Freiling F C, Hoffmann J, et al. Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. In: Proceedings of IEEE Symposium on Security and Privacy. Washington DC: IEEE, 2011. 96–111
205 Becher M. Security of smartphones at the dawn of their ubiquitousness. 2010
206 Hepner C, Zmijewski E. Defending against BGP man-in-the-middle attacks. In: Proceedings of Black Hat DC Conference, Arlington, 2009
207 Waichal S, Meshram B B. Router attacks-detection and defense mechanisms. Int J Sci Technol Res, 2013, 2: 145–149
208 Weaver N, Sommer R, Paxson V. Detecting forged TCP reset packets. In: Proceedings of the 16th Network and Distributed System Security Symposium, San Diego, 2009
209 Nakibly G, Kirshon A, Gonikman D, et al. Persistent OSPF attacks. In: Proceedings of the 19th Network and Distributed System Security Symposium, San Diego, 2012
210 Jones E, Moigne O. OSPF security vulnerabilities analysis. Work in Progress, 2006
211 Shaikh A, Greenberg A. Experience in black-box OSPF measurement. In: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. New York: ACM, 2001. 113–125

212 Hartman S, Wasserman M, Zhang D. Security Requirements in the Software Defined Networking Model. IETF Draft (draft-hartman-sdnsec-requirements), 2013

213 Hardt D. The OAuth 2.0 authorization framework. 2012

214 Porras P, Shin S, Yegneswaran V, et al. A security enforcement kernel for OpenFlow networks. In: Proceedings of the 1st Workshop on Hot Topics in Software Defined Networks. New York: ACM, 2012. 121–126

215 Shin S, Porras P A, Yegneswaran V, et al. FRESCO: modular composable security services for software-defined networks. In: Proceedings of the 20th Network and Distributed System Security Symposium, San Diego, 2013

216 Anand M, Cronin E, Sherr M, et al. Security challenges in next generation cyber physical systems. National Meeting on Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, Pittsburgh, 2006

217 Shafi Q. Cyber physical systems security: a brief survey. In: Proceedings of the 12th International Conference on Computational Science and its Applications. Washington DC: IEEE, 2012. 146–150

218 Fletcher K K, Liu X F. Security requirements analysis, specification, prioritization and policy development in cyber-physical systems. In: Proceedings of the 5th International Conference on Secure Software Integration and Reliability Improvement Companion, Jeju Island, 2011. 106–113

219 Azab M, Eltoweissy M. Defense as a service cloud for Cyber-Physical Systems. In: Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, Orlando, 2011. 392–401

220 Lee G S, Thuraisingham B. Cyberphysical systems security applied to telesurgical robotics. Comput Stand Interfaces, 2012, 34: 225–229

221 Gohil A, Modi H, Patel S K. 5G technology of mobile communication: a survey. In: Proceedings of the International Conference on Intelligent Systems and Signal Processing, Gujarat, 2013. 288–292

222 Chin W H, Fan Z, Haines R. Emerging technologies and research challenges for 5G wireless networks. IEEE Wirel Commun, 2014, 21: 106–112

223 Shen C X, Zhang H G, Wang H M, et al. Trusted computing research and development (in Chinese). Sci Sin Inform, 2010, 40: 139–380

224 Zhang H G, Yan F, Fu J M, et al. Research on theory and key technology of trusted computing platform security testing and evaluation. Sci China Inf Sci, 2010, 53: 434–453

225 Zhang H G, Wu G Q, Qin Z P, et al. A new type secure computer (in Chinese). Wuhan Univ J Nat Sci, 2004, 50: 1–6

226 Zhang H G, Liu Y Z, Yu F J, et al. A new embedded security module. Wuhan Univ J Nat Sci, 2004, 50: 7–11

227 Trusted Platform Module Library. http//www.TCG.org.com

228 Zhang Q Y, Zhao S J, Qin Y, et al. Formal analysis of TPM2.0 key management APIs. Chin Sci Bull, 2014, 59: 4210–4224

229 Chen L, Li J. Flexible and scalable digital signatures in TPM 2.0. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013. 37–48

230 Xu Y, Zhao B, Milan H, et al. TPM2.0 key replication security enhancement scheme (in Chinese). Wuhan Univ J Nat Sci, 2014, 60: 471–477

231 Wu K, Zhao B. Security defects of TPM2.0 policy authorization mechanism and its improvement scheme (in Chinese). Wuhan Univ J Nat Sci, 2014, 60: 478–484

232 Yu F J, Zhang H G, Zhao B, et al. A formal analysis of Trusted Platform Module 2.0 HMAC authorization under DRM scenario. Secur Commun Netw, 2015, doi: 10.1002/sec.1193

233 Liu Z W, Feng D G. Dynamic integrity measurement framework based on trusted computing (in Chinese). Electron Inf Technol, 2010, 32: 875–879

234 Yan F, Shi X, Li Z H, et al. A design and implementation of UEFI based virtual machine dynamic security measurement framework (in Chinese). Sichuan Univ J Eng Sci, 2014, 46: 22–28

235 Hu H S. A design and implementation of IaaS dynamic measurement protocol (in Chinese). Dissertation of Master's Degree. Wuhan University, 2015

236 Wang L N, Yu R W, Gao H J. Trusted virtual machine execution environment construction method based on trust extension (in Chinese). J Commun, 2011, 32: 1–8

237 Yang S L. Virtual trusted platform and its security research based on TPM2.0 (in Chinese). Dissertation of Master's Degree. Wuhan University, 2015

238 Dai W, Jin H, Zou D, et al. TEE: a virtual DRTM based execution environment for secure cloud-end computing. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010. 663–665

239 Dai W Q, Zou D Q, Jin H, et al. TPMc: a virtual machine group-oriented TPM system for trusted cloud computing. Submitted to Annual Computer Security Applications Conference, 2015

240 Zhang H G, Mao S W, Wang Ho Z. Asymmetric-computing Type Shared Key Establishing Method Suitable for Cloud Computing and IoT. Patent: US14/724809

241 Mei H, Wang Q X, Zhang L, et al. Progress on software analysis techniques (in Chinese) . J softw, 2009, 32: 1697–1701

242 Fang B X, Lu T B, Li C. Progress on software assurance (in Chinese). J Commun, 2009, 30: 106–122

243 Marquardt P, Verma A, Carter H, et al. (sp) iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In: Proceedings of the 18th ACM Conference on Computer and Communications Security. New York: ACM, 2011. 551–562

244 Lin C C, Li H, Zhou X, et al. Screenmilker: how to milk your android screen for secrets. In: Proceedings of the 21st Annual Network and Distributed System Security Symposium, San Diego, 2014

245 Michalevsky Y, Nakibly G, Schulman A, et al. PowerSpy: location tracking using mobile device power analysis. arXiv:1502.03182

246 Fu J M, Du H, Peng B C. Dynamic detection of a component loading vulnerability (in Chinese). J Tsinghua Univ Sci Technol, 2012, 52: 1356–1363

247 Hsu F H, Tso C K, Yeh Y C, et al. BrowserGuard: a behavior-based solution to drive-by-download attacks. IEEE J Sel Areas Commun, 2011, 29: 1461–1468

248 Forrest S, Somayaji A, Ackley D H. Building diverse computer systems. In: Proceedings of the 6th Workshop on Hot Topics in Operating Systems, Cape Cod, 1997. 67–72

249 Lu L, Yegneswaran V, Porras P, et al. Blade: an attack-agnostic approach for preventing drive-by malware infections. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010. 440–450

250 Song C, Zhuge J, Han X, et al. Preventing drive-by download via inter-module communication monitoring. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2010: 124–134

251 Shen C X, Zhang H G, Wang H M, et al. Research on trusted computing and its development. Sci China Inf Sci, 2010, 53: 405–433

252 ARM Security Technology—Building a Secure System using TrustZone Technology. ARM Technical White Paper, 2005–2009

253 Rosenberg D. Qsee trustzone kernel integer over flow vulnerability. Black Hat Conference, 2014

254 Jeffrey M, Park S, Lee K, et al. Content security for IPTV. IEEE Commun Mag, 2008, 46: 138–146

255 Meike M, Sametinger J, Wiesauer A. Security in open source web content management systems. IEEE Secur Priv, 2009,7: 44–51

256 Li Q, Lui J C S, Chiu D M. On the security and efficiency of content distribution via network coding. IEEE Trans Dependable Secur Comput, 2012, 9: 211–221

257 Chen X X, Fang B X, Hu M, et al. A new field in security of internet information and content-network information penetration detection technology. J China Institut Commun, 2004, 25: 185–191

258 Ge L, Ji X S, Jiang T. Research on situation awareness model of information content security incidents in telecommunication network. Telecommun Sci, 2014, 2: 14–20

259 Balabanovic M, Shoham Y. Learning information retrieval agents: experiments with automated web browsing. Online working notes of the AAAI Spring Symposium Series on Information Gathering from Distributed, Heterogeneous Environments, 1995. 13–18

260 Teufel B, Schmidt S. Full text retrieval based on syntactic similarities. Inf Syst, 1988, 13: 65–70

261 Letsche T A, Berry M W. Large-scale information retrieval with latent semantic indexing. Inf Sci, 1997, 100: 105–137

262 Liu Y B, Shao Y, Wang Y, et al. A multiple string matching algorithm for large-scale URL filtering. Chin J Comput, 2014, 37: 1159–1169

263 Moulin P, Sullivan J A O. Information-theoretic analysis of information hiding. IEEE Trans Inf Theory, 2003, 49: 563–593

264 Du Q, Nekovei R. Implementation of real-time constrained linear discriminant analysis to remote sensing image classification. Patt Recognit, 2005, 38: 459–471

265 Zhang L F. Algorithm for judging duplicate real-time packet in massive database. Comput Eng, 2008, 34: 76–80

266 Shahri H H, Shahri S H. Eliminating duplicates in information integration: an adaptive, extensible framework. IEEE Intell Syst, 2006, 21: 63–71

267 Liu Z, Zhao Z G. An algorithm of detection duplicate information based on segment. In: Proceedings of International Conference on Computational Aspects of Social Networks, Taiyuan, 2010: 156–159

268 Heydon A, Najork M. Mercator: a scalable, extensible Web crawler. World Wide Web, 1999, 2: 219–229

269 Gautam P, Srinivasan P. Link contexts in classifier-guided topical crawlers. IEEE Trans Knowl Data Eng, 2006, 18: 107–122

270 Hai D, Hussain F K. Self-adaptive semantic focused crawler for mining services information discovery. IEEE Trans Ind Inf, 2014, 10: 1616–1626

271 Zhou D M, Li Z J. Survey of high-performance web crawler. Comput Sci, 2009, 36: 26–29

272 Mladenic D. Feature subset selection in text-learning. In: Proceedings of the 10th European Conference on Machine Learning. London: Springer-Verlag, 1998. 95–100

273 Joachims T. Learning to Classify Text Using Support Vector Machines: Methods, Theory and Algorithms. Norwell: Kluwer Academic Publishers, 2002

274 Wang J. Digital audio watermarking algorithm based on modular arithmetic using DWT. Comput Eng, 2004, 30:

44–52
275 Barry A, Lee B F F. An audio delay system using digital technology. J Audio Engr Soc, 1971, 19: 393–397
276 Johnston J D. Transform coding of audio signals using perceptual noise criteria. IEEE J Sel Areas Commun, 1988, 6: 314–323
277 Cinque L, Ciocca G, Levialdi S, et al. Color-based image retrieval using spatial-chromatic histograms. Image Vis Comput, 2001, 19: 979–986
278 Lu S W, Xu H. Textured image segmentation using autoregressive model and artificial neural network. Patt Recognit, 1995, 28: 1807–1817
279 Gonzalez R C, Woods R E. Digital Image Processing. 3rd ed. Englewood Cliffs: Prentice Hall, 2007
280 Xu Z Z, Li J H, Yang S T, et al. A new robust content-based image authentication scheme. J Shanghai Jiaotong Univ, 2003, 37: 1757–1762
281 Song Y, Treanor D, Bulpitt A J, et al. Unsupervised content classification based nonrigid registration of differently stained histology images. IEEE Trans Biomed Eng, 2014, 61: 96–108
282 Lu L, Zhang H J, Jiang H. Content analysis for audio classification and segmentation. IEEE Trans Speech Audio Process, 2002, 10: 504–516
283 Su G Y, Ma Y H, Li J H. One improved content based information filtering model. J Shanghai Jiaotong Univ, 2004, 38: 2030–2034
284 Hanani U, Shapira B, Shoval P. Information filtering: overview of issues, research and systems. User Model User-Adapt Interact, 2001, 11: 203–259
285 Nguyen V D, Varghese B, Barker A. The royal birth of 2013: analysing and visualising public sentiment in the UK using Twitter. In: Proceedings of IEEE International Conference on Big Data, Santa Clara, 2013. 46–54
286 Tan S, Li Y, Sun H, et al. Interpreting the public sentiment variations on Twitter. IEEE Trans Knowl Data Eng, 2014, 26: 1158–1170
287 Li J H. Close attention to the importance of new applications of Internet content security management. Netinfo Secur, 2008, 1: 23