Sept. 2006, Vol.21, No.5, pp.740–755 *J. Comput. Sci. & Technol.*

Progress and Prospect of Some Fundamental Research on Information Security in China

Deng-Guo Feng[1] (冯登国) and Xiao-Yun Wang[2] (王小云)

[1] *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences Beijing 100080, P.R. China*

[2] *School of Mathematics and System Science, Shandong University, Jinan 250100, P.R. China*

E-mail: fengdg@263.net

Received March 27, 2006; revised July 21, 2006.

Abstract With the development of network and information technologies, information security is more and more widely researched in China. To know where the work is and where it goes, we focus on comprehensively surveying the twenty years of important fundamental research by Chinese scholars, and giving, from our point of view, the significance as well as the outlook of future work. Some of the reviewed work, including the researches on fundamental theory of cryptography, cryptographic algorithm, security protocol, security infrastructure and information hiding, greatly advances the related sub-fields, and is highly recognized in and outside of China. Nevertheless, the overall work, we think, is still facing the problems of unbalanced development of sub-areas, limited scope of research, lack of systematic work and application, etc., leaving much room for improvement in the near future.

Keywords cryptology, security protocol, security infrastructure, information security

1 Introduction

With the rapid and global development of network and information technologies, information security becomes more and more influential and widely needed. Nowadays, government, business and industry, including banks, energy industry, transportation and telecommunication, are almost indispensable with network, making the research and application of information security a strategic issue of nations.

The leading industrial countries or organizations such as the United States, Russia, Japan and European Union, make their strategies of information security from the angle of national security. Aiming at building the assurance systems of information security, many effective efforts have been made to the various aspects of legislation, technical standards, monitoring system, security products, core technologies, controllable information products, talent training and consciousness culturing. To keep pace with them, Chinese government pays great attention to the area these years. In 2003, the National Informatization Leading Group, an agency of the central government, announced the official "*Advice on strengthening information security assurance*". By pointing out "adhering to the principle of active defense and integrated prevention, substantially improving the capability of information security protection and making social development benefit from the advance of information security and vise versa", the document serves as a guideline for China's development of information security.

Scientific and technological research plays a central role in advancing information security. In this survey, we focus on some important fundamental research on information security by Chinese scholars in the last twenty years, and giving some remarks on the achieved significance and international impact from our point of view. Most researches to be reviewed were funded by the National Natural Science Foundation of China (NSFC) directly or indirectly. In the sequel, the most important work recognized in and outside of China in the sub-fields of fundamental theory on cryptography, cryptographic algorithm, security protocol, security infrastructure and information hiding, is to be respectively reviewed with the prospect of possible future work.

2 Theory of Cryptography

Fundamental theory on cryptography serves as the groundwork of design and analysis of cryptographic algorithms. In China, the subfields being seriously researched cover cryptographic functions, cryptographic permutation, sequences (i.e., multi-sequences and arrays), theory of authentication codes, theory of finite automata, theory of secret sharing, optimization of cryptographic operations, etc.

2.1 Cryptographic Function and Permutation

Chinese scholars have acquired rich results on cryptographic functions. Many high quality papers[1−13] and books[14−16], to a certain extent, record the prominent work of the years. In this area, the most influential contribution is done by Prof. Guo-Zhen Xiao[1], who first found the spectral characterizations of correlation-immune functions. The result, called *Xiao-Massey theorem* by international peers, has induced a series of related researches and been cited frequently, establishing itself as one of the fundamentals in the research on correlation-

Survey

Supported by the National Natural Science Foundation of China under Grant No. 60025205.

immune functions. Thereafter, the work[5,7,14,16] on spectral characterization of correlation-immune functions in China became more in-depth and the results were extended to integer rings and finite fields. Moreover, [2, 3, 14–16] give many new constructions of cryptographic functions, e.g., correlation-immune functions and non-linear functions, and several new results on the non-existence of generalized bent functions were presented by using the class group of imaginary Abelian number fields in [9, 11].

Chinese scholars have made systematic efforts to study resilient functions. In [6] a number of methods for constructing new resilient functions from old ones are proposed, and the existence, construction and enumeration of resilient functions over finite fields are given in [10]. Particularly, [12] not only gives the lower bounds on the number of constructible correlation immune symmetric functions, but also exemplifies the constructions of 2 kinds of such new balanced functions, 1-resilient and 2-resilient respectively. It also refutes K. Gopalakrishnan *et al.*'s conjecture and proves the functions given by them are not 2-resilient.

In the area of correlation analysis, [4] investigates the maximum correlation analysis of nonlinear combining functions and designs the specific analysis algorithms. In addition, [4, 8] estimate the capability of resisting the analysis for the most widely used nonlinear functions and for some bent functions respectively.

As the core components of cryptographic algorithms and multi-output functions, cryptographic permutations often play irreplaceable roles in design. By thoroughly studying the S-Boxes in DES, [17] gives the permutation constructions with good cryptographic properties. In [18], some cryptographic properties of exponential functions are studied, and a series of permutations with the properties of strict avalanche criterion (SAC) and completeness are designed. In [19], an approach to the construction of linear orthomorphisms is given with the answer of the enumeration problem of such transforms. Based on Walsh Hadamard transform, [20] proposes an algorithm for improving the self-inverse S-Boxes.

2.2 Sequence and Sequence Synthesis

Sequences bring important resources to cryptographic design. In particular the generation and analysis of sequences with good randomness and cryptographic properties are very significant issues of research. Having contributed a series of innovative work[21−57], Chinese scholars gradually gain the leading position in the field. Undoubtedly the most influential work, came from Prof. Zong-Duo Dai. She systematically studied a class of sequences called *binary sequence derived from rings*[29] as well as their cryptographic properties, e.g., period, linear complexity, the statistical distribution, etc. The pioneer work, which also gives a new resource of nonlinearity, has induced many successive researches and been widely cited in the literature. Furthermore, Prof. Dai and her colleagues established the theory of multi-continued fraction[53], and, by applying the theory, solved some fundamental problems of multisequences. To acquire the best rational approximation in the research on pseudo-random sequences, they ever contributed a multi-continued fraction algorithm (m-CFA), and a multi-universal continued fraction algorithm (m-UCFA). The theory of multi-continued fractions is not only an effective tool in dealing with multisequences, but also applicable to many areas including number theory, numerical computation, communication, coding, etc. Based on it, Prof. Dai and her colleagues solved the difficult problems remaining for many years. For instance, they demonstrated that d-perfect multi-sequences are not always strongly d-perfect and gave an example to disprove C. P. Xing's conjecture[48,49] whereas they proved another conjecture on the normalized expected value of linear complexity of two-dimensional binary sequences[50]. Moreover, the asymptotic behavior of the normalized linear complexity of multisequences can also be studied in its multi-continued fraction expansion[46], and the generalized Berlekamp-Massey algorithm for linear synthesis of multisequences can be deduced naturally from a special representation of the multi-continued fraction algorithm[52].

Other researches on sequences in China are quite impressive also. Rueppel's linear complexity conjecture is proved by [23]. [30] solves the open problem of 2-dimension arrays presented by T. Nomura *et al.* in 1972. By giving the algebraic theory of m-arrays, the work discloses the structure of linear recurring m-arrays and proves that any such m-array can be generated by "folding" an m-sequence. In [32] and its successive work, the ways of analyzing the linear complexity, in case that a sequence over finite fields is substituted by one, two or any symbols, are proposed. In [37] the problem of whether q-ary Gordon-Mills-Welch (GMW) sequences are cyclically shift distinct is completely solved and a criterion for deciding the sequences of period $q^n - 1$ is given. [33, 41, 42] acquire a series of results on sequences over rings. In [54] a polynomial characterization of characteristic ideal of maximal periodic arrays over Galois rings is deduced and a polynomial-based construction for the ideals is given.

In the above work, sequence synthesis, another fundamental of the research, also interests Chinese researchers. In [26] the relation of continued fractions and the Berlekamp-Massey algorithm is revealed. [36, 39] give the fast algorithms for, given period, determining the linear complexity and the minimal polynomial of a sequence over finite fields. And [43] reduces multisequences synthesis to the problem of lattice basis over function fields, and proposes a synthesis method through the lattice basis reduction.

2.3 Theory of Authentication Codes

The key theoretic issues in research of authentication codes cover the lower bound, in information theory and combinatorics, of the probability of successful deception, new constructions of the codes and their struc-

tural characterization. Many good results[58−64] in the area were acquired by academician Zhe-Xian Wan and Prof. Ding-Yi Pei. Particularly, Pei's conclusions[61] on the information-theoretic lower bound of the probability of successful deception for general authentication codes are widely called *Simmons-Pei bounds* by international peers. In [58] the codes withstanding spoofing attacks of high order and the codes with secrecy are respectively constructed. [59] designs a series of Cartesian codes by adopting unitary geometry over finite fields. In [60] two constructions of Cartesian codes based on symplectic spaces are proposed. In [61] the information-theoretic lower bound of the probability of a successful spoofing attack for general codes is proved, and a sufficient and necessary condition for achieving the lower bound is given. By reducing the construction of optimal codes to combinatorial design, [62] proposes a class of optimal authentication codes based on normal curves over finite fields. In terms of combinatorial design [63] gives the composite structure of optimal authentication codes with arbitration.

2.4 Theory of Finite Automata

Finite automata theory has gained considerable attention in the literature after the public key cryptosystems based on finite automata were introduced. Prof. Ren-Ji Tao[65,66], a researcher with the Chinese Academy of Sciences, thoroughly studied the invertibility of finite automata, which finally serves as the fundamental of the finite automata-based public key cryptosystems proposed by him. To improve Tao's work, many Chinese scholars started related research[67,68]. Among them, Profs. Zong-Duo Dai and Ding-Feng Ye established the algebra theory on finite automata. Supported by the cryptology-orientated theory, they made a classification of weakly invertible linear automata, gave a characterization of the solution of nonlinear automata equation, and proposed several methods for decomposing the finite automata.

2.5 Theory of Secret Sharing

Secret sharing attracts much attention since it has not only wide applications but also rich theoretic models. A lot of efforts have been made in the field by Chinese scholars[69−73]. Especially, Prof. Mu-Lan Liu and her colleagues accomplished excellent work on the related fundamental theory. They gave a classification of ideal homomorphic key sharing schemes when the key space is a cyclic group[69]. By building the relation between a monotone span program and a linear multi-secret sharing scheme, they brought forward the optimal linear multi-secret sharing scheme[70]. In [71], the concept of secure parallel multi-party computation is given with a general construction of a parallel multi-party computation protocol from a linear multi-secret sharing scheme.

2.6 Comment and Prospect

Having yielded innovative fruits in fundamental theory of cryptography and solved many open problems, some Chinese scholars are highly recognized by international peers. Nevertheless, we think, as the origin of various cryptographic designs, fundamental theory of cryptography must have plentiful elements. Therefore the research should be further broadened in such a rich field. In the near future, we think that characterizing the structure of cryptographic modules, enriching the constructions of the modules, establishing better security measurement, searching for new design approaches, and developing new fundamentals of cryptographic function, cryptographic permutations, authentication codes, sequences, secret sharing, and so on will be the very important issues. Particularly, strengthening the research on theory of elliptic curve cryptography (ECC) and its implementation have special significance for China since ECC has been advocated by Chinese industry and academia.

3 Cryptographic Algorithm

Cryptographic algorithms, primarily including stream cipher , block cipher, public key encryption, hash function, are basic elements of a secure information system. Their research involves the design theory and analytic method of cryptographic algorithms. Chinese scholars have acquired a large number of original fruits in the field.

3.1 Stream Cipher

Many researches on the design and analysis of stream ciphers[74−82] have been accomplished by Chinese scholars. What should be specially mentioned is the work of Prof. Ken-Cheng Zeng *et al.* and that of Prof. Cun-Sheng Ding *et al.* The former proposed many effective ways for cryptanalysis of stream ciphers, including the linear syndrome method[74,76], linear consistency test[75], etc. The methods have deep influence on the research of stream ciphers. Prof. Ding *et al.* made a systemic and thorough pioneer research on the stability theory of stream ciphers[77].

Some very new stream ciphers have also been successfully attacked. By systematically analyzing $S1$, $S2$ and $S3$, proposed for encryption in GSM (Global System for Mobile communication), [83] shows that both $S1$ and $S2$ are vulnerable to known plaintext attacks, and $S3$ even cannot decrypt correctly. COSvd(2, 128) is a steam cipher proposed by E. Filiol *et al.* in ECRYPT SASC'04. The designers claimed the resistance against all known attacks. However, the divider-and-conquer attack proposed by [84] can recover the keys of COSvd(2, 128) with only $O(2^{26})$ bytes of known plaintext. The success rate is 93.4597%, and the complexity $O(2^{113})$, much lower than that of exhaustive search.

3.2 Block Cipher

Since block cipher has been widely used in commerce, the related research is largely driven by the standardization process. In recent years, however, Chinese scholars have contributed a lot of work[85−91] especially in the background of the AES (Advanced Encryption Standard) project of the United States and NESSIE (New European Scheme for Signatures, Integrity and Encryption) project of European Union. NUSH is a candidate block cipher submitted to NESSIE by Russian Cryptography Institute. [89] gives an attack by linear cryptanalysis. The result was considered to be the best one in the report of NESSIE and directly caused the cipher be ruled out. Camellia is a block cipher recommended for both NESSIE and standardization in Japan. By constructing the efficient distinguishers of 4-round Camellia, the collision cryptanalytic method[90] designed by the Chinese researchers is still the most effective one for analyzing the block cipher.

Some Chinese researchers had thoroughly investigated the operation modes of block cipher and tweakable block ciphers. A variable-input-length encryption mode is proposed in [92]. And [93] analyzes the modes of TBC (Tweakable Block Chaining) and TAE (Tweakable Authenticated Encryption) given by M. Liskov *et al.* in CRYPTO'02. It proves the security of TBC in the sense of indistinguishability but, with counterexamples, overturns the positive results of TAE.

3.3 Public Key Cryptosystem

Public key cryptosystems are building blocks of authentication infrastructure, e.g., public key infrastructure (PKI) or certificate authority (CA). It consists of two operational models, the encryption model and the signature model. In this subsection, the signature model only means the basic signature model since those with special functionality, we think, can be considered as the secure protocols. Chinese scholars have done much novel work on the design and analysis of the cryptosystems[94−107]. Based on the invertibility theory of finite automaton, as what we reviewed before, Prof. Ren-Ji Tao proposed finite automata public-key cryptosystems (FAPKC)[94,99,101]. His pioneer work not only brings about a new kind of public key cryptosystem but also exemplifies an application of the above invertibility theory. [97, 100, 103] investigate the security of FAPKCs and point out some weaknesses of them. Prof. Xin-Mei Wang proposed another kind of digital signature algorithm based on error-correcting codes[95]. Similarly, a series of security analysis and improvements[104,105,107] on the special kind of algorithms have been made thereafter. As one of the conclusions, [107] proves that there exists a fatal vulnerability in these algorithms, and it is difficult to design digital signature algorithms with high-level security by exploiting the difficulty of factorizing large matrices.

2R is considered a novel public key cryptosystem since it primarily deals with the low degree multivariate polynomials over small fields and avoids the modular operations of large integers. The security of 2R relies on its composition of 2 round operations. However, Prof. Ding-Feng Ye *et al.* proposed an effective attack for decomposing a 2-round 2R into two 1-round cryptosystems[102,103]. Their work attracted great interests in the cryptology community, and in the cryptography monograph "*asymmetrical cryptosystem based on multivariate polynomials over small fields*" edited by J. Patarin, the work is honored as one of the two most important new ideas in cryptanalysis of multivariate cryptosystem in the years. In addition, [106] makes a systematic cryptanalysis on ElGamal-like encryption schemes based on conic curves, constructs the isomorphism between the conic curve group, or rational group, and the finite field group, and proves that the schemes based on conic curve group is no more secure than the traditional ElGamal schemes.

3.4 Hash Function

Hash functions form another kind of core cryptographic algorithms used primarily for verifying the integrity of data and improving the efficiency of digital signature. Chinese scholars have made great breakthrough in the cryptanalysis of the functions. In CRYPTO'04, the astonishing ways of quickly finding collisions of MD4, MD5, RIPEMD and HAVAL were first displayed. The work[108], together with a series of successive researches[109−113] thereafter, brings a new cryptanalytic approach, called bit tracing, which is capable of efficiently analyzing and finding collisions of the most extensively used hash functions, including SHA-0, SHA-1, MD4, MD5, RIPEMD, etc. Since the cryptanalysis almost overturns the fundamentals of MD-x and SHA-x like hash functions, it is widely considered as having international impact on the community of cryptology as well as electronic commerce that depends greatly on digital signature.

3.5 Comment and Prospect

Chinese scholars' research on the design and especially the analysis of cryptographic algorithms have had great influence and received the recognition from international colleagues. However, compared with the work of cryptanalysis, the design of the algorithms seems much weaker. In our outlook for the area, four trends of future work might be as follows.

1) *Standardization Trend.* Most security applications require standardized cryptographic algorithms. As in the history of cryptographic algorithms, the standardization will be always making use of the fruits of cryptographic theory and techniques, and serving as the driving force in advancing the area.

2) *Theorization Trend Towards Perfection.* Pursuing the provable security of cryptographic algorithms is a fashion nowadays. What researchers have interests in

is no longer limited to the conventional cryptographic methods. Instead, they begin to study cryptography in view of information and complexity theory to prove the security under some models.

3) *Automation Trend of Security Evaluation.* The research on security test and evaluation of cryptographic algorithms needs to focus on the evaluation models, evaluation methods and measure criteria. They will help produce practical and automatic tools to effectively evaluate the security of cryptographic algorithms.

4) *Application Trend.* The fast development of electronic government and electronic commence need the support from cryptographic techniques. The situation brings not only the opportunities but also challenges to the applications of cryptography. From the angle of practice, the cryptographic techniques and their application skills still need improving in many aspects, e.g., secret key management, the optimization of software and hardware, and the design of cryptographic algorithms under specific circumstances.

4 Security Protocol

A security protocol, also called cryptographic protocol, is a protocol that makes use of cryptographic algorithms in dealing with messages. It is one of fundamental elements for building secure information systems. More precisely, cryptographic algorithms offers encryption, decryption, and other auxiliary algorithms, e.g., hash functions, for transmitting messages while a security protocol, based on the cryptographic building blocks, provides solutions to all kinds of security requirements. Running in computer network or distributed systems, a security protocol requires the participants, who have security requirements, to execute a series of steps, and it aims at achieving the objectives such as key distribution, entity authentication, secure electronic transaction, etc. There are primarily two aspects in the research. One is the theory of design, and the other the cryptanalysis. Though the research in this field was started relatively late in China, however, Chinese scholars now begin making progress.

4.1 Design Theory of Security Protocols

In designing security protocols, Chinese scholars proposed batches of novel proposals[114−145], including the protocols of key escrow[114], oblivious transfer[115,122,124,125], undeniable signature[116], blind signature[120], zero-knowledge proof[118,144], group signature[119,123,127,141], key agreement[121], threshold signature[126,128,130], signcryption[131,139], fair-exchange[129,134], ring signature[132], anonymous transmission[133], proxy signature[135,143], aggregate signature[136,142], quantum cryptographic[138], etc. In particular, the philosophy of provable security affects all the designs.

Some important work in the area might be as follows. Based on bilinear pairings, [117] gives an identity-based signature scheme and an identity-based ring signature scheme. A novel public-key model, called weak public-key (WPK) model, is proposed for resettable zero-knowledge (rZK) protocols in [118]. It also proposes a more efficient zero-knowledge protocol through the model. [128] proposes a new class of frameworks for designing threshold signature protocols, and constructs the concrete protocols which are not only flexible but also possesses the property to allow different signers having different privileges. Based on verifiably encrypted probabilistic signatures, a method for designing fair exchange protocols is proposed in [129], where a rigorous security model for identity-based fair exchange protocols is constructed and an efficient protocol with provable security is presented for identity-based optimistic fair exchange. The first threshold signature protocol is proposed in [130] and the first ring signature scheme in [132]. Both of them are provably secure under the standard model.

4.2 Methods for Analyzing Security Protocol

There are two mostly used approaches to analyzing the security protocols. One is the plain means, and the other is the formal means. They both have been seriously researched by Chinese scholars.

The plain analysis means is widely used and very practical. Mainly relying on one's experience and related knowledge or even inspiration, it seeks for flaws of a protocol from its security assumption or interaction. Many methods in this area come from Chinese scholars[146−153]. In [147], to introduce the generalized inverse of matrices in the design of security protocols, the authors proved a sufficient and necessary condition for a matrix that has generalized inverse, and then solved the partition, construction and enumeration problem for the matrices. In addition more cryptanalytic methods is proposed in [148] for the key escrow protocols presented in [114], etc.

The formal means for analyzing security protocols is axiomatic. By establishing security models based on computer science, the method makes use of logical reasoning or reduction to check or validate the security of a protocol. Chinese scholars have also done much work in this field[154−160]. Many researchers in the field of computer science joined the research and greatly advanced it. In [157], the authors proposed an algebraic model for security protocol, and its major feature is the capability of describing attack procedures on security protocols. The limitation of the strand space security model is pointed out in [158]. It also constructs a generalized strand space model, which can not only prove the correctness of a protocol but also help design attacks if the protocol fails to be secure. A succinct and flexible semantic model in abstract state model for authentication protocols is presented in [159]. It allows one specifying and analyzing complex protocols at different abstract levels, thus overcoming the drawback of existing security protocol analyzers that have difficulties analyzing complex protocols. Moreover, the model blends the authentication and

secrecy properties in verifying the security of an authentication protocol, and thus successfully avoids the potential flaws resulting from verifying the properties separately. With the Canetti-Krawczyk model, [160] proves that the forward secrecy against key generation center (KGC) cannot be achieved under the identity-based setting, and proposes an extension of it.

4.3 Comment and Prospect

Chinese scholars have made some progress in the design and analysis of security protocols. Their high-quality publications have influences on some issues. However, only few of the researches made significant breakthroughs since they largely focus on improving the design and analysis whereas little efforts have been made to study the pioneer and more fundamental methods.

Security protocols can solve a series of important problems, e.g., source authentication and destination authentication, integrity of a message, anonymous communication, resistance against denial of service, non-repudiation, authorization, etc. Nevertheless it is still challenging to analyze potential flaws of protocols, though there are many kinds of theory and methods to investigate them. Hence they need further developing and improving. In brief, we think, there are three trends in the future development of security protocols as follows.

1) *Practicality Trend in the Design.* It is always important to design and implement security protocols for specific applications. These protocols might include group key exchange protocols, key exchange protocols in multimedia communications, entity authentication protocols, their combination, etc.

2) *Theoretical Trend of Analysis.* Analysis theory for security protocols, especially the formal analysis methods, the theory of provable security, secure multiparty computation and zero-knowledge theory, will be still of significance in the field.

3) *Automation Trend for Checking and Evaluating Security Protocols.* The security check and evaluation of security protocols is another important issue. There has been much need to strengthen investigations on the related theory and methods as well as developing the tools which automatically do the work.

5 Security Infrastructure

Security infrastructure is a framework that provides security service for an entire organization or society, where it can be used by every application and object which needs the functionality of information security. The access point of security infrastructure must be as uniform and convenient as possible in order to accomplish the goal of universally supporting applications.

There are two kinds of security infrastructures. One is public key infrastructure (PKI) or key management infrastructure (KMI). It is largely used to generate, publish and manage keys and credentials such as certificates. The other is detection or response infrastructure such as an intrusion detection system (IDS), which is used to detect, identify network attacks and response in an effective way. Chinese academia and industry have done a great amount of work on PKI and IDS.

5.1 Public Key Infrastructure

As a widely applicable infrastructure, PKI borrows the conception and technology from public key cryptosystems in providing security services. It is also an approach to the solution of the trust and authorization issues in network environment, including the problems of the reality of identity, data integrity, non-repudiation, etc.

PKI technologies have been vastly developed in China. Many companies, e.g., Jilin University Info. Tech., Shanghai Wellhope, Shanghai Koal, Jinan Dean Computer Tech., etc., have their independent and widely deployed PKI products.

Instead of developing the technologies, Chinese academia paid more attention to the research on the structure and improvement of PKI[161−163]. The national standardization organization actively launched the research programs aiming at standardizing PKI, and published many relevant standards and criteria.

In particular, State Key Laboratory of Information Security (SKLOIS or LOIS) has developed an advanced and fully functional PKI system, called LOIS PKI system. It complies with international standards and is independently developed. A novel PKI model, which provides a way of solving the problem of interoperation and complexity of PKI, has been adopted in the system. And the laboratory introduced the architecture of dual layer intrusion tolerant system to give an approach to solving the problem of self-security of PKI. Moreover, the conception of *PKI Entities*, which are uniform objects to represent persons, devices, processes, etc., is introduced in the system for reducing the complexity of planning, applications and deployment.

5.2 Intrusion Detection System

An IDS combines data processing, security audit, pattern matching and statistics together into one organic system for detecting the behaviors that might violate the security strategy and compromise the system being protected. The mostly used methods for detection are analyzing the audit data and the data captured from network.

IDS is widely researched and developed in China. Many companies, like Lenovo, Venus Info. Tech., Nandasoft Tech., etc., have their IDS product. Many research groups have developed their IDS prototypes, and published many papers and books. Though the publications[164−168] are seldom listed in recognized journals or conferences, some work is much contributive. [164] proposes a novel structure combining affinity mutation to improve the performance of anomaly detection, and it also designs a basic system based on ar-

tificial immunology. By exploiting system calls, [165] gives a very helpful IDS prototype for monitoring the multi-processes. Based on unsupervised clustering (UC), [166] proposes an intrusion detection algorithm which supports vector machine, and [167] puts forward a compound detection model. In addition, a space-efficient algorithm based on improved DAWG (directed acyclic word graph) automaton, which can detect the occurrences of patterns in an out-of-order data stream, is designed in [168].

5.3 Comment and Prospect

As we see, the academia and industry of China have acquired many fruits on security infrastructure systems, with special advances in PKI and IDS. However, the research does not cover all necessary subjects and lacks of in-depth work. Since PKI is widely applicable to electronic commerce and electronic government, we think, the research needs much further work. From our point of view, the development of PKI implies four trends as follows.

1) *Trend of Application.* Under the current technical circumstance, PKI is still the best choice to solve the problem of trust and authorization in the environment of public network, and hence will be more widely used. Nevertheless some practical problems in application and the use of verification model should be further investigated.

2) *Trend of Standardization.* The wide use of PKI can introduce problems in interconnection and interoperation, making the standardization process and the implementation under the standards necessary and important.

3) *Trend of Self-Security.* With the development of information technologies, the security of PKI itself will be more and more important. The technologies, e.g., self-adaptation and intrusion tolerance, are effective in improving the self-security of PKI, though they still need further improving.

4) *Trends of Integration.* To implement more secure and flexible systems, the work on combing the novel technologies and applications, such as biometric identification, identity-based public key cryptography and trusted computing platform, etc., will obviously interest many researchers.

By years of development, the technologies of IDS have been improved in China. However, with the rapid change of network and attacks, they show much room for improvement. We think the future work can notice the following trends.

1) *Trend of High Speed.* High-speed networks, such as ATM, Gigabit Ethernet, etc., are more and more widely deployed. Hence the further research on large-scale distributed detection over various fast networks is urgently needed.

2) *Trend of Standardization.* An IDS has interoperation with other IDS or security products. The situation makes the standardization of IDS one of the development trends in the near future.

3) *Trend of Evolving into IPS (Intrusion Protection System).* IPS gives a way of improving IDS. From the angle of functionality, IPS is a container of IDS but, in addition, it provides the ability of a firewall as well as the seamless connection with the latter. Hence IPS, we think, will substitute IDS gradually and become the products in the mainstream.

6 Information Hiding

Information hiding has been extensively researched in China by institution as well as industry, though the recognized work is largely limited to watermarking. For instance, Beijing Huaqi Information Digital Technology Co., already put watermarking cameras on market, and many researchers, in the prestigious international journals and conferences, published important papers[169−187] which primarily focus on robust or fragile watermarking, steganalysis and the security issues.

6.1 Robust Watermarking

Robust watermarking is mostly intended for labeling copyright statement of an owner of digital content. Nevertheless, a watermark can also be used as a digital fingerprint that indicates a content buyer. The applications require that a watermark should be secretly embedded without degrading the perceptual quality of distributed content, and that, to achieve the robustness, the embedded watermark should be testable even after the distributed version was attacked to a certain extent. Chinese researchers have proposed many robust watermarking schemes, and some of the work to be briefly reviewed next wins wide recognition. To increase the embedded energy for improving the robustness but keeping the perceptual quality, [169] proposes a method that embeds a part of watermark even in direct component (DC) of DCT (Discrete Cosine Transform) domain, and [170] improves the watermark detection by introducing communication theory into the design. From another angle [171] gives an approach to better use of human visual system through linear prediction filtering. In order to improve the robustness through new ways of embedding, [172] suggests embedding a watermark into the singular value decomposition domain. By exploiting the different stages of VQ (Vector Quantization), [173] proposes a way of realizing robust and fragile watermarking in one scheme for protecting both copyright and content integrity. To improve the synchronization of watermark detection and its resistance to geometric attacks, [174], in DWT (Discrete Wavelet Transform) domain, proposes a scheme capable of amending the deformation by error-correcting codes and 2-dimention interleaving, and [175] further introduces DFT (Discrete Fourier Transform) in the design before the embedding. The revised scheme is called DWT-DFT composite scheme. It improves resistance to geometric attack and JPEG (Joint Photo-

graphic Experts Group) compression. Moreover in this area, [176] gives a method by testing the 2 channels of a color image.

6.2 Fragile Watermarking

In contrast to robust watermarking, fragile watermarking is primarily targeted on protecting the integrity of digital content other than the copyright. Compared with its cryptographic counterpart, the technique is simpler and supports more efficient protocol in practice. In addition it can localize the tampering instead of just detecting the existence, and through a semi-fragile watermark it can even give the so-called content-oriented protection, i.e., allowing the change of data representation but not the meaning of the content. In China, active efforts have also been made to design new or improve existing fragile watermarking schemes. Many of the researches to be briefly surveyed next are novel and important. Among them, [177] proposes a DWT-based semi-fragile scheme enduring JPEG compression. In tackling the vulnerability resulting from small blocks used for localization, [178], by adopting the reverse processing, proposes a way of construing the fragile schemes that do not partition an original signal into blocks. The results show the improvement of both security and localizability. To retrieve the perfect original content, [179] gives a reversible scheme based on integer wavelet transform.

6.3 Steganalysis and Watermarking Security

Steganalysis studies the ways of testing and deciding the existence or information of a hidden message, and watermarking security covers the issues pertaining to the scheme vulnerabilities that enable an attacker to mount more accurate attacks or deceptions. Likewise Chinese researchers have also made significant contributions to the fields. Among the most recognized researches, [180] discloses the possible inserter attack on watermarking systems and designs a countermeasure even in case that the users of embedding devices are dishonest. To improve the information hiding based on computing pixel-value difference (PVD), [181] reveals its vulnerability under the histogram based steganalysis and gives a remedy. Assuming a watermarking application does not require using a specified verification algorithm, [182] proves the existence of the reverse attack and, by linking a watermark with the algorithm that verifies it, the paper also gives a solution. In [183], the sample pair based steganalysis is improved by using the least square method, and an approach to more reliable steganalysis by exploiting the wavelet characteristic functions is proposed in [184]. To acquire the noninvertibility of public robust watermarking, which does not need the original in verification, [185] proposes a construction which adopts ill-posed operation in embedding and reverse processing in verification. Since an attacker makes more observational errors, the output of him or her is more severely perturbed. On investigating zero-knowledge watermark proof systems, [186] proves the prerequisites for constructing the systems, and gives a framework, with examples, for designing and verifying them. To resist the collusion attack on fingerprint, [187] suggests concatenating the spread-spectrum code with a convolutional code. The results demonstrate the improved resistance to the collusion attack even with a shorter fingerprint.

6.4 Comment and Prospect

In brief, Chinese researchers have made impressive progress in watermarking related fields whereas the work on other aspects of information hiding and digital right management (DRM) apparently lags behind. The under-researched areas, we think, primarily include software protection, program counter-tracing, key protection in DRM systems, anonymity, white-box encryption, covert channel, subliminal channel and counter-capture communication. Therefore it might be worth devoting more future work to them for both balancing and systemizing the research.

7 Some New Work and Advances

To give a more recent view, this section will introduce some of our new researches in sequence, stream cipher, block cipher, hash function, group cryptography, security protocol and PKI. Since most of them are unpublished so far, the names of the involved researchers, including ours and our colleagues', are to be given directly.

7.1 Sequence

The following progress in the area of sequence has newly been made by the cooperation of Deng-Guo Feng, post-doctor Hong-Gang Hu *et al.*:

1) *New Constructions.* Feng and Hu *et al.* constructed some periodic sequences over F_q with very large 1-error linear complexity by GDFT (Generalized Discrete Fourier Transform) of periodic sequences. More constructions of sequences with longer periods, larger linear complexities and lower correlations have been designed by applying the theory of Kummer extensions of function fields.

2) *Partial Period Properties.* The above researchers thoroughly analyzed the partial period properties of some binary sequences derived from rings, e.g., the Kerdock-code sequences and the highest level sequences of primitive sequences over rings. The results show that the partial period distributions and the partial period independent r-pattern distributions of these binary sequences are asymptotically uniform. Based on the observation, they gave the nontrivial upper bounds for aperiodic autocorrelation of the sequences.

3) 2-*Adic Complexity.* A significant difference between the linear complexity and the 2-adic complexity of periodic binary sequences is found by Feng and Hu. The concept of symmetric 2-adic complexity of periodic binary sequences is presented by the observation. They

also decided the expected value of the 2-adic complexity and derived a lower bound on the expected value of the symmetric 2-adic complexity of periodic binary sequences. Because the 2-adic complexity of periodic binary sequences is unstable, they introduced the concepts of k-error 2-adic complexity and k-error symmetric 2-adic complexity, and deduced the lower bounds of them. Moreover, they derived the expected value of the joint 2-adic complexity of periodic binary multisequences, and gave a nontrivial lower bound for the expected value of the joint symmetric 2-adic complexity.

7.2 Stream Cipher

Lately in the research on stream cipher, the joint work of Deng-Guo Feng, Bin Zhang *et al.* brings about the new attacks and keystream generator as follows.

1) *New Fast Correlation Attack.* Feng, Zhang *et al.* designed the multi-pass fast correlation attack on stream ciphers. By exploiting different kinds of parity-checks without increasing the asymptotic complexity, the attack restores the initial state part by part. Particularly it has no restriction on the weight of the underlying linear feedback shift register. Both theoretical analysis and simulation show that it is more efficient than all previously known fast correlation attacks.

2) *Guess-and-Determine Attack.* Feng, Zhang *et al.* also designed the guess-and-determine attack on self-shrinking generators (SSG). The inherent exibility of the attack enables one to smoothly deal with different attack conditions and requirements. For the SSG with a length L LFSR of arbitrary form, the attack can reliably restore the initial state respectively with the time and memory complexities $O(2^{0.556L})$ and $O(L^2)$ under $O(2^{0.161L})$-bit keystream, $L \geqslant 100$, and the complexities $O(2^{0.571L})$ and $O(L^2)$ under $O(2^{0.194L})$-bit keystream, $L < 100$. Hence the attack is regarded as being more powerful than the previously known ones on SSG.

3) *New Self-Shrinking Generators.* Based on the above work, the researchers presented a new variant of SSG. The construction inherits the simplicity and security properties of SSG, and all the known attacks on the SSG can be frustrated by the new design. In addition, its keystream has ideal distribution and its exibility allows efficient implementations of the generator.

7.3 Block Cipher

The group of Deng-Guo Feng, Wen-Ling Wu, Peng Wang *et al.* has researched block cipher for years. Recently, they completed some significant cryptanalysis and designs as follows.

1) *Cryptanalysis of ARIA and Camellia.* Having studied the security of block ciphers ARIA and Camellia under impossible differential attacks, the members of the group improved the existing such cryptanalysis of ARIA and Camellia. Although the designers of ARIA expected that no impossible differential exists in 4-round ARIA, however, the group found some nontrivial 4-round impossible differentials, which may lead to the potential attack on 6-round ARIA. Moreover, they found some nontrivial 8-round impossible differentials for Camellia, though only 7-round impossible differentials were previously known. By using the 8-round impossible differentials, they designed an attack on 12-round Camellia. With respective data and encryption complexities 2^{120} and 2^{181}, it is the first attack on 12-round Camellia that has the complexities less than those of the exhaustive search.

2) *Cryptanalysis of FOX.* The above group constructed some distinguishers for 3-round FOX, another block cipher. By adopting integral attack and collision search, the distinguishers are used to attack 4-, 5-, 6- and 7-round FOX64, and 4- and 5-round FOX128. The attack is more efficient than the previous integral attacks on FOX. Its complexities can be $2^{77.6}$ on 4-round FOX128 and $2^{205.6}$ on 5-round FOX128. For FOX64, they are respectively $2^{45.4}$ on 4-round FOX64, $2^{109.4}$ on 5-round FOX64, $2^{173.4}$ on 6-round FOX64, $2^{237.4}$ on 7-round FOX64. Hence 4-round FOX64/64, 5-round FOX64/128, 6-round FOX64/192, 7-round FOX64/256 and 5-round FOX128/256 are all not immune to the attack.

3) *Cryptanalysis of SMS4.* After studying SMS4, a block cipher adopted by the Chinese standard of WLAN (Wireless Local Area Network), the group found that the cipher is not immune to differential fault attacks. More specifically, a 6-round SMS structure is not pseudo-random, and a 7-round one lacks strong pseudo-random. Nevertheless, the properties can be achieved in 7- and 8-round SMS structures respectively.

4) *Secure Modes of Operation.* The group gave a new security model for the modes of operation, called IRS (Indistinguishable from Random String) model. The difference between IRS-CPA/CCA (IRS under Chosen Plaintext Attack/Chosen Ciphertext Attack) models and IND-CPA/CCA (Indistinguishable-CPA/CCA) models lies in the fact that the latter can choose the initial vector but the former cannot. IRS-CPA/CCA inherits the advantages of IND-CPA/CCA, e.g., the conciseness of directly proving and no problems resulting from IND-CPA/CCA's too strong security. The group also studied other relationship among the various IRS and IND models. In addition, also in the sub-area of operation modes, the group found that the composite model which allows authentication before encryption is incorrect. Two efficient attacks on MEM (Mask Encrypt Mask) mode, proposed by Chakraborty and Sarkar, were designed by Wang, Feng and Wu. The first attack uses only one encryption and one decryption query, and the other just needs one encryption query.

7.4 Hash Function

After Prof. Xiao-Yun Wang disclosed the collision results of hash functions MD4, MD5, HAVAL-128, and RIPEMD in CRYPTO'04 at Santa Barbara, California,

she and Hong-Bo Yu began the research towards breaking SHA-1. They successfully solved the impossible differential problem, which is an obstacle to designing effective differential attacks on SHA-like hash functions such as SHA-1 and SHA-0. Furthermore, they found several tens of conditions satisfied by the collided plaintext and acquired the complex technique of plaintext modification. Ultimately all the above work led SHA-1 to be totally broken.

7.5 Group Cryptography

Deng-Guo Feng and Chuan-Kun Wu recently designed a framework that uses symmetric key block ciphers for one-to-many or equivalently many-to-one encryption. The basic idea is to adopt a pre-processing which maps multiple keys into one encryption key, in case of many-to-one phase, or into one decryption key, in case of one-to-many phase. With the design, each of the key holders will have only one key, but when he or she is in the authorized decryption group, the encrypted message can always be decrypted correctly. The security of the schemes has also been fully investigated.

7.6 Security Protocol

The group of Deng-Guo Feng, Zhen-Feng Zhang, Jing Xu *et al.* freshly made the following progress in security protocols:

1) *Certificateless Signature Scheme.* The group presented a reasonable security model for certificateless public-key signature schemes, and then further proposed an efficient construction based on bilinear pairings. The security of the schemes can be proved to be equivalent to the computational Diffie-Hellman problem in the random oracle model with a tight reduction. In 2005, Al-Riyami and Paterson proposed a certificateless public-key encryption scheme and proved its security in the random oracle model but the above group disclosed its vulnerability to adaptive chosen ciphertext attacks. A countermeasure to overcome the flaw was also given.

2) *Verifiable Probabilistic Signature Scheme.* The group extended the paradigm of verifiably encrypted signature for fair exchange protocols to probabilistic signature, and called the prospective scheme verifiable probabilistic signature scheme. To investigate it, a security model with precise and formal definitions is introduced, and the collusion attacks are formalized for the first time. Finally the group proposed a novel RSA-based verifiable probabilistic signature scheme and showed that, in the random oracle model, it is provably secure. A semi-trusted off-line third party is still involved, whereas no registration between the trusted third party and users is needed. The approach works well with standard RSA signature scheme and any other hash-and-sign schemes, and the fair exchange protocols based on it are much concise, efficient, and practical.

3) *Key Agreement Protocol.* A series of new pairwise key agreement protocols based on Weil pairing have been proposed recently. In general their designers claimed that they have the attributes of known session key security, perfect forward secrecy, no key-compromise impersonation etc. The above group showed that these protocols are insecure against impersonation attack and man in the middle attack such that they cannot satisfy the requirements of key agreement protocols. To give a countermeasure, the group members designed a new two-party identity-based authenticated key agreement protocol based on bilinear pairing. They also acquired the analysis results of security and efficiency, all implying that the new protocol is more efficient than existing ones in terms of computational cost and storage requirement.

4) *Cryptanalysis of Smart Card Based Authentication.* There have been many remote user authentication schemes with smart cards so far. However, the group pointed out that subgroup attacks can be applied to these schemes to reveal the secret value maintained by the authentication server. They also found that a dynamic ID-based remote user authentication scheme using smart cards is vulnerable to password guessing attacks.

5) *ID-Based Partial Proxy Signature Scheme.* The group introduced a new and natural paradigm for fair exchange protocols, called ID-based partial proxy signature scheme. A security model with precise and formal definitions was presented, and an efficient and provably secure partial proxy signature scheme was proposed. Up to now, this is the first full ID-based optimistic fair exchange protocol, and unlike the majority of previously proposed protocols, the approach does not use any zero knowledge proof, thus avoiding most of the costly computation.

6) *Cryptanalysis of Password-Authenticated Key Exchange.* The client-to-client password-authenticated key exchange (C2C-PAKE) protocols allow two clients in different management domains agreeing on a session key using different passwords. Nevertheless the research group found that the protocols have a common vulnerability to key-compromise impersonation attacks. In contrast to some of the existing security claims, the group members also indicated the impossibility of a secure C2C-PAKE protocol in the current setting against key-compromise impersonation attacks.

7.7 PKI

To further improve the security of a CA system, Deng-Guo Feng and Yong Zhuang recently proposed a CA scheme, called autonomous and cooperative intrusion tolerant CA scheme. Based on traditional intrusion tolerant CA, the new scheme disposes of the key distribution center, and adopts a distributed algorithm to generate a shared CA key. Consequently any $T-1$ servers, where T is the threshold, cannot compromise the private key of the CA in both the initialization and running stages. Moreover the system can find wrong partial signatures online. Apparently all the above designs further enhance the reliability of an intrusion tolerant CA. And notably, SKLOIS has newly implemented the above

CA system.

8 Concluding Remarks

Having reviewed some fundamental research on information security in the past 20 years in China, we can see that, though much progress has been made, there still exist many problems. Some problems and the possible solutions we suggest are as follows.

1) *Unbalanced Advances.* The work on various areas is at different levels. Some researches, e.g., those on the fundamentals of cryptology, cryptographic algorithms and digital watermarking, are widely recognized whereas some others, e.g., those on secure protocol, PKI and IDS, etc., need improving. More future work, we think, should focus on the weak parts.

2) *Limited Scope of Research.* The researches in China can put too much concern in a limited number of directions but not even publish any paper in some other fields, including malicious codes, computer virus, trusted computing, applied security, etc. Hence some guidance might be in need for broadening the scope of research.

3) *Lack of Systematic Work.* Some unprofitable work needs persistent investment of money as well as participation of human beings. Due to various reasons, many researchers in China can only be supported by projects that are financially supported only in a period of time. As a result, it is often difficult to research in a systematic and persistent way. Undoubtedly the situation can only be improved through the reform of research system.

4) *Separated Research and Application.* Some researches, particularly the application-oriented ones, need the participation of researchers, designers and users. Therefore the activities of research, education and marketing must be further combined to meet the need of applications.

To sum up, we can see that the future research on information security in China should be oriented towards the grasp of more balanced knowledge, more advanced theory as well as more practical techniques.

It is worth particularly mentioning that, in writing of the survey, though some work is more properly selected and reviewed, some other important work might be inadvertently neglected or misrepresented. Please feel free to point them out.

Acknowledgements We would like to thank Dr. Xian-Feng Zhao *et al.* for their assistance in our writing of the survey.

References

[1] Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Info. Theory*, 1988, 34(3): 569–571.

[2] Yang Y X, Guo B A. Further enumerating Boolean functions of cryptographic significance. *J. Cryptology*, 1995, 8(3): 115–122.

[3] Liu M L, Lu P Z, Mullen G L. Correlation-immune functions over finite fields. *IEEE Trans. Info. Theory*, 1998, 44(3): 1273–1276.

[4] Feng D G, Pei D Y, Xiao G Z. Maximum correlation analysis of nonlinear combining functions. *Science in China* (*Series E*), 1998, 41(1): 31–36.

[5] Feng D G. Three characterizations of correlation immune functions over rings $Z(N)$. *Theoretical Computer Science*, 1999, 226(1-2): 37–43.

[6] Chen L S, Fu F W. On the constructions of new resilient functions from old ones. *IEEE Trans. Info. Theory*, 1999, 45(6): 2077–2082.

[7] Zhou J J, Chen W H, Gao F X. Best linear approximation and correlation immunity of functions over Z_m^*. *IEEE Trans. Info. Theory*, 1999, 45(1): 303–308.

[8] Zhang B D, Lü S W. I/O correlation properties of bent functions. *Science in China* (*Series E*), 2000, 43(3): 282–286.

[9] Liu F M, Ma Z, Feng K Q. New results on non-existence of generalized bent functions (II). *Science in China* (*Series A*), 2002, 45(6): 721–730.

[10] Hu Y P, Xiao G Z. Resilient functions over finite fields. *IEEE Trans. Info. Theory*, 2003, 49(8): 2040–2046.

[11] Feng K Q, Liu F M. New results on the nonexistence of generalized bent functions. *IEEE Trans. Info. Theory*, 2003, 49(11): 3066–3071.

[12] Wu C K, Dawson E D. Correlation immunity and resiliency of symmetric Boolean functions. *Theoretical Computer Science*, 2004, 312(2-3): 321–335.

[13] Teng J H, Li S Q, Huang X Y. The kth-order quasi-generalized Bent functions over ring Z_p. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.189–201.

[14] Feng D G. Spectral Theory and Its Applications in Cryptography. The Science Press, 2000. (in Chinese)

[15] Wen Q Y, Niu X X, Yang Y X. Boolean Functions in Modern Cryptography. The Science Press, 2000. (in Chinese)

[16] Li S Q, Zeng B S, L Y Z *et al. Logical Functions in Cryptography.* Beijing Zhongruan Electronic Press, 2003. (in Chinese)

[17] Yang J H, Dai Z D, Zeng K C. The data base of selected permutations (extended abstract). In *Proc. ASIACRYPT'91*, Fujiyosida, Japan, Nov. 11–14, 1991, *Lecture Notes in Computer Science 739*, Imai H *et al.* (eds.), Springer-Verlag, 1993, pp.73–81.

[18] Chang X G, Dai Z D, Gong G. Some cryptographic properties of exponential functions. In *Proc. ASIACRYPT'94, Wollongong*, Australia, November 28–December 1, 1994, *Lecture Notes in Computer Science 917*, Pieprzyk J, Safavi-Naini R (eds.), Springer-Verlag, 1995, pp.415–418.

[19] Dai Z D, Solomon W G, Gong G. Generating all linear orthomorphisms without repetition. *Discrete Mathematics*, 1999, 205(1-3): 47–54.

[20] Chen H, Feng D G. An evolutionary algorithm to improve the nonlinearity of self-inverse S-Boxes. In *Proc. ICISC'04*, Seoul, Korea, Dec. 2–3, 2004, *Lecture Notes in Computer Science 3506*, Park C, Chee S (eds.), Springer-Verlag, 2005, pp.352–361.

[21] Chen D, Dai Z D. On feedforward transforms and p-fold periodic p-arrays. In *Proc. EUROCRYPT'85*, Linz, Austria, April 1985, *Lecture Notes in Computer Science 219*, Pichler F (ed.), Springer-Verlag, 1985, pp.130–134.

[22] Liu M L, Wan Z X. Generalized multiplexed sequences. In *Proc. EUROCRYPT'85*, Linz, Austria, April 1985, *Lecture Notes in Computer Science 219*, Pichler F (ed.), Springer-Verlag, 1985, pp.135–141.

[23] Dai Z D. Proof of Rueppel's linear complexity conjecture. *IEEE Trans. Info. Theory*, 1986, 32(3): 440–443.

[24] Beth T, Dai Z D. On the complexity of pseudo-random sequences — Or: If you can describe a sequence it can't be random. In *Proc. EUROCRYPT'89*, Houthalen, Belgium, April 10–13, 1989, *Lecture Notes in Computer Science 434*, Quisquater J, Vandewalle J (eds.), Springer-Verlag, 1990, pp.533–543.

[25] Dai Z D, Zeng K C. Feedforward functions defined by de Brujin sequences. In *Proc. EUROCRYPT'89*, Houthalen, Belgium, April 10–13, 1989, *Lecture Notes in Computer Science 434*,

Quisquater J, Vandewalle J (eds.), Springer-Verlag, pp.544–548.

[26] Dai Z D, Zeng K C. Continued fractions and the Berlekamp-Massey algorithm. In *Proc. ASIACRYPT'90*, Sydney, Australia, January 8–11, 1990, *Lecture Notes in Computer Science 453*, Seberry J, Pieprzyk J (eds.), Springer-Verlag, pp.24–31.

[27] Cheng H, Xiao G Z. The linear complexity of binary sequences with period $(2n-1)k$. *IEEE Trans. Info. Theory*, 1991, 37(3): 672–673.

[28] Dai Z D, Yang J H. Linear complexity of periodically repeated random sequences. In *Proc. EUROCRYPT'91*, *Lecture Notes in Computer Science 547*, Davies D W (ed.), Springer-Verlag, Brighton, UK, April 8–11, 1991, pp.168–175.

[29] Dai Z D. Binary sequences derived from ML-sequences over rings, I: Periods of minimal polynomials. *J. Cryptology*, 1992, 5(3): 193–207.

[30] Lin D D, Liu M L. Structure and properties of linear recurring m-arrays. *IEEE Trans. Info. Theory*, 1993, 39(5): 1758–1762.

[31] Dai Z D, Feng X N, Liu M L, Wan Z X. Nonlinear feedforward sequences of m-sequences I. *Discrete Mathematics*, 1993, 123(1-3): 17–34.

[32] Dai Z D, Imamura K. Linear complexity for one-symbol substitution of a periodic sequence over GF(q). *IEEE Trans. Info. Theory*, 1998, 44(3): 1328–1331.

[33] Qi W F, Yang J H, Zhou J J. ML-sequences over rings $Z/(2e)^*$: I. constructions of nondegenerative ML-sequences II. injectiveness of compression mappings of new classes. In *Proc. ASIACRYPT'98*, Beijing, China, October 1998, *Lecture Notes in Computer Science 1514*, Ohta K, Pei D Y (eds.), Springer-Verlag, pp.315–326.

[34] Feng K Q, Shiue P J S, Xiang Q. On aperiodic and periodic complementary binary sequences. *IEEE Trans. Info. Theory*, 1999, 45(1): 296–303.

[35] Jiang S Q, Dai Z D, Imamura K. Linear complexity of a sequence obtained from a periodic sequence by either substituting, inserting, or deleting k symbols within one period. *IEEE Trans. Info. Theory*, 2000, 46(3): 1174–1177.

[36] Xiao G Z, Wei S M, Lam K Y, Imamura K. A fast algorithm for determining the linear complexity of a sequence with period p^n over GF(q). *IEEE Trans. Info. Theory*, 2000, 46(6): 2203–2206.

[37] Gong G, Dai Z D, Golomb S W. Enumeration and criteria for cyclically shift-distinct GMW sequences. *IEEE Trans. Info. Theory*, 2000, 46(1): 474–484.

[38] Tang X H, Fan P Z. A class of pseudonoise sequences over GF(p) with low correlation zone. *IEEE Trans. Info. Theory*, 2001, 47(4): 1644–1649.

[39] Wei S M, Xiao G Z, Chen Z. A fast algorithm for determining the minimal polynomial of a sequence with period $2p^n$ over GF(q). *IEEE Trans. Info. Theory*, 2002, 48(10): 2754–2758.

[40] Qi W F, Xu H. Partial period distribution of FCSR sequences. *IEEE Trans. Info. Theory*, 2003, 49(3): 761–765.

[41] Fan S Q, Han W B. Random properties of the highest level sequences of primitive sequences over $Z(2e)$. *IEEE Trans. Info. Theory*, 2003, 49(6): 1553–1557.

[42] Zhu X Y, Qi W F. Compression mappings on primitive sequences over $Z/(p^e)$. *IEEE Trans. Info. Theory*, 2004, 50(10): 2442–2448.

[43] Wang L P, Zhu Y F, Pei D Y. On the lattice basis reduction multisequence synthesis algorithm. *IEEE Trans. Info. Theory*, 2004, 50(11): 2905–2910.

[44] Dai Z D, Jiang S Q, Imamura K, Gong G. Asymptotic behavior of normalized linear complexity of ultimately nonperiodic binary sequences. *IEEE Trans. Info. Theory*, 2004, 50(11): 2911–2915.

[45] Feng X T, Dai Z D. Expected value of the linear complexity of two-dimensional binary sequences. In *Proc. 3rd Int. Conf. Sequences and Their Applications* (*SETA'04*), Seoul, Korea, October 24–28, 2004, *Lecture Notes in Computer Science 3486*, Helleseth T *et al.* (eds.), Springer-Verlag, pp.113–128.

[46] Dai Z D, Imamura K, Yang J H. Asymptotic behavior of normalized linear complexity of multi-sequences. In *Proc. 3rd Int. Conf. Sequences and Their Applications* (*SETA'04*), Seoul, Korea, October 24–28, 2004, *Lecture Notes in Computer Science 3486*, Helleseth T *et al.* (eds.), Springer-Verlag, 2005, pp.129–142.

[47] Hu H G, Feng D G. On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences. In *Proc. 3rd Int. Conf. Sequences and Their Applications* (*SETA'04*), Seoul, Korea, October 24–28, 2004, *Lecture Notes in Computer Science 3486*, Helleseth T *et al.* (eds.), Springer-Verlag, 2005, pp.185–196.

[48] Feng X T, Wang Q L, Dai Z D. Multi-sequences with d-perfect property. In *Proc. 2004 IEEE Int. Symp. Info. Theory* (*ISIT'04*), Chicago, Illinois, USA, June 27–July 2, 2004, pp.86–98.

[49] Feng X T, Wang Q L, Dai Z D. Multi-sequences with d-perfect property. *Theory of Complexity*, 2005, 21(2): 230–242.

[50] Feng X T, Dai Z D. The expected value of the normalized linear complexity of 2-dimensional binary sequences. In *Proc. 3rd Int. Conf. Sequences and Their Applications* (*SETA'04*), Helleseth T *et al.* (eds.), Seoul, Korea, October 24–28, 2004, pp.24–28.

[51] Gong G. Theory and applications of q-ary interleaved sequences. *IEEE Trans. Info. Theory*, 1995, 41(2): 400–411.

[52] Dai Z D, Feng X T, Yang J H. Multi-continued fraction algorithm and generalized B-M algorithm over F_2. In *Proc. Int. Conf. Sequences and Their Applications*, Seoul, Korea, October 24–28, 2004, *Lecture Notes in Computer Science 3486*, Helleseth T *et al.* (eds.), Springer-Verlag, 2005, pp.339–354.

[53] Dai Z D, Wang K P, Ye D F. M-continued fraction expansions of multi-Laurent series. *Advances in Mathematics*, 2004, 33(2): 246–248.

[54] Hu L, Pei D Y. Polynomial characterization of characteristic ideal of maximal periodic arrays over Galois rings. *Discrete Mathematics*, 2004, 278(1-3): 139–149.

[55] Tang X H, Udaya P, Fan P Z. A new family of nonbinary sequences with three-level correlation property and large linear span. *IEEE Trans. Info. Theory*, 2005, 51(8): 2906–2914.

[56] Bai E J, Liu X J, Xiao G Z. Linear complexity of new generalized cyclotomic sequences of order two of length pq. *IEEE Trans. Info. Theory*, 2005, 51(5): 1849–1853.

[57] Wei S M, Chen G L, Xiao G Z. A fast algorithm for determining the linear complexity of periodic sequences. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, December 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.202–209.

[58] Smeets B, Vanroose P, Wan Z X. On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order $L \geqslant 2$. In *Proc. EUROCRYPT'90*, Aarhus, Denmark, May 21–24, 1990, *Lecture Notes in Computer Science 473*, Damgård I (ed.), Springer-Verlag, 1991, pp.306–312.

[59] Wan Z X. Construction of Cartesian authentication codes from unitary geometry. *Designs, Codes and Cryptography*, 1992, 2(4): 333–356.

[60] Wan Z X, Ben J M S, Vanroose P. On the construction of Cartesian authentication codes over symplectic spaces. *IEEE Trans. Info. Theory*, 1994, 40(3): 920–929.

[61] Pei D Y. Information-theoretic bounds for authentication codes and block designs. *J. Cryptology*, 1995, 8(4): 177–188.

[62] Pei D Y. A problem of combinatorial designs related to authentication codes. *J. Combinatorial Design*, 1998, 6(6): 417–429.

[63] Pei D Y, Li Y Q, Wang Y J, Rei S N. Characterization of optimal authentication codes with arbitration. In *Proc. ACISP'99*, Wollongong, Australia, April 7–9, 1999, *Lecture Notes in Computer Science 1587*, Pieprzyk J *et al.* (eds.), Springer-Verlag, 1999, pp.303–314.

[64] Pei D Y. Authentication Codes and Combinatorial Designs. Boca Raton: Chapman & Hall/CRC, 2006.

[65] Tao R J. Invertibility of Finite Automata. The Science Press, 1979. (in Chinese)

[66] Tao R J. Invertibility of linear finite automata over a ring. In *Proc. ICALP'88*, Tampere, Finland, July 11–15, 1988, *Lecture Notes in Computer Science 317*, Lepistö T, Salomaa A (eds.), Springer-Verlag, 1988, pp.489–501.

[67] Bao F. Composition and Decomposition of finite automata. *Science in China* (*Series A*), 1993, 23(7): 759–765.
[68] Dai Z D, Ye D F. Weak invertibility of linear finite automata. *Science in China* (*Series A*), 1996, 39(6): 613–623.
[69] Liu M L, Zhou Z F. Ideal homomorphic secret sharing schemes over cyclic group. *Science in China* (*Series E*), 1998, 28(6): 524–533.
[70] Xiao L L, Liu M L. Linear multi-secret sharing schemes. *Science in China* (*Series F*), 2005, 48(1): 125–136.
[71] Zhang Z F, Liu M L, Xiao L L. Parallel multi-party computation from linear multi-secret sharing schemes. In *Proc. AISACRYPT'05*, Chennai, India, December 4–8, 2005, *Lecture Notes in Computer Science 3788*, Roy B (ed.), Springer-Verlag, 2005, pp.156–173.
[72] Zhou Z F. Classification of universally ideal homomorphic secret sharing schemes and ideal black-box secret sharing schemes. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, December 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.370–383.
[73] Ma W P, Zhang F T. New methods to construct cheating immune multisecret sharing scheme. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, December 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.384–394.
[74] Zeng K C, Huang M. On the linear syndrome method in cryptoanalysis. In *Proc. CRTPTO'88*, Santa Barbara, CA, USA, August 21–25, 1988, *Lecture Notes in Computer Science 403*, Goldwasser S (ed.), Springer-Verlag, 1990, pp.469–478.
[75] Zeng K C, Yang C H, Rao T R N. On the linear consistency Test (LCT) in cryptanalysis with applications. In *Proc. CRTPTO'89*, Santa Barbara, CA, USA, August 20–24, 1989, *Lecture Notes in Computer Science 435*, Brassard G (ed.), Springer-Verlag, 1990, pp.164–174.
[76] Zeng K C, Yang C H, Rao T R N. An improved linear syndrome algorithm in cryptanalysis with applications. In *Proc. CRTPTO'90*, Santa Barbara, CA, USA, August 11–15, 1990, *Lecture Notes in Computer Science 537*, Menezes A, Vanstone, S A (eds.), Springer-Verlag, 1991, pp.34–47.
[77] Ding C S, Xiao G Z, Shan W J. The Stability Theory of Stream Ciphers. *Lecture Notes in Computer Science 561*, Springer-Verlag, 1991.
[78] Hu Y P, Xiao G Z. Generalized self-shrinking generator. *IEEE Trans. Info. Theory*, 2004, 50(4): 714–719.
[79] Zhang B, Wu H J, Feng D G, Bao F. Security analysis of the generalized self-shrinking generator. In *Proc. ICICS'04*, Malaga, Spain, October 27–29, 2004, *Lecture Notes in Computer Science 3269*, Lopez J *et al.* (eds.), Springer-Verlag, 2004, pp.388–400.
[80] Zhang B, Wu H J, Feng D G *et al.* Chosen ciphertext attack on a new class of self-synchronizing stream ciphers. In *Proc. INDOCRYPT'04*, Chennai, India, December 20–22, 2004, *Lecture Notes in Computer Science 3348*, Canteaut A, Viswanathan K (eds.), Springer-Verlag, 2004, pp.73–83.
[81] Zhang B, Wu H J, Feng D G *et al.* Cryptanalysis of a knapsack based two-lock cryptosystem. In *Proc. 2nd Int. Conf. Applied Cryptography and Network Security* (*ACNS'04*), Yellow Mountain, China, June 8–11, 2004, *Lecture Notes in Computer Science 3089*, Jakobsson M *et al.* (eds.), Springer-Verlag, 2004, pp.303–309.
[82] Zhang B, Wu H J, Feng D G, Bao F. A fast correlation attack on the shrinking generator. In *Proc. CT-RSA'05*, San Francisco, CA, USA, February 14–18, 2005, *Lecture Notes in Computer Science 3376*, Menezes A (ed.), Springer-Verlag, 2005, pp.72–86.
[83] Zhang B, Feng D G. On the security of three stream cipher. *Journal of Software*, 2005, 16(7): 1344–1351.
[84] Zhang B, Feng D G. Security analysis of a new stream cipher. *Science in China* (*Series F*), 2006, 49(3): 1–16.
[85] Zeng K C, Yang J H, Dai Z D. Patterns of entropy drop of the key in an S-box of the DES. In *Proc. CRTPTO'87*, Santa Barbara, CA, USA, August 16–20, 1987, *Lecture Notes in Computer Science 293*, Pomerance C (ed.), Springer-Verlag, 1988, pp.438–444.
[86] Wu W L, Li B, Feng D G, Qing S H. Cryptanalysis of some AES candidate algorithms. In *Proc. ICICS'99*, Sydney, Australia, November 9–11, 1999, *Lecture Notes in Computer Science 1726*, Varadharajan V, Mu Y (eds.), Springer-Verlag, 1999, pp.13–21.
[87] Zhu F, Guo B A. A multiplication-addition structure against differential attack. In *Proc. ICICS'99*, Sydney, Australia, November 9–11, 1999, *Lecture Notes in Computer Science 1726*, Varadharajan V, Mu Y (eds.), Springer-Verlag, 1999, pp.247–257.
[88] He Y P, Qing S H. Square attack on reduced Camellia cipher. In *Proc. ICICS'01*, Xian, China, November 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.238–245.
[89] Wu W L, Feng D G. Linear cryptanalysis of NUSH block cipher. *Science in China* (*Series F*), 2002, 45(1): 59–67.
[90] Wu W L, Feng D G. Collision attack on reduced-round Camellia. *Science in China* (*Series E*), 2004, 34(8): 857–868.
[91] Wu W L, Feng D G, Chen H. Collision attack and pseudorandomness of reduced-round Camellia. In *Proc. SAC'04*, Waterloo, Canada, August 9–10, 2004, *Lecture Notes in Computer Science 3357*, Handschuh H, Hasan M A (eds.), Springer-Verlag, 2004, pp.252–266.
[92] Wang P, Feng D G, Wu W L. HCTR: A variable-input-length enciphering mode. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, December 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.175–188.
[93] Wang P, Feng D G, Wu W L. On the security of tweakable modes of operation: TBC and TAE. In *Proc. ISC'05*, Singapore, Sept. 20–23, 2005, *Lecture Notes in Computer Science 3650*, Zhou J Y *et al.* (eds.), Springer-Verlag, 2005, pp.274–287.
[94] Tao R J, Chen S H. A finite automation public key scheme and digital signature. *Chinese Journal of Computers*, 1985, (8): 401–409. (in Chinese)
[95] Wang X M. A digital signature scheme constructed with error-correcting codes. *IEE Electronics Letters*, 1990, 26(13): 898–899.
[96] Bao F. Increasing ranks of linear automata and the complexity of FAPKC. *Science in China* (*Series A*), 1994, 24(2): 193–200.
[97] Dai D W, Wu K, Zhang H G. Cryptanalysis of finite automata public key cryptosystem. *Science in China* (*Series A*), 1995, 25(11): 1226–1232.
[98] Xu M Z, Wang E F. The crack of public key cryptosystem PKCY. *Science in China* (*Series E*), 1997, 27(2): 171–178.
[99] Tao R J, Chen S H, Chen X M. FAPKC3: A new finite automation public key cryptosystem. *J. Computer Science and Technology*, 1997, 12(4): 289–305.
[100] Dai Z D, Ye D F, Lam K Y. Weak invertibility of finite automata and cryptanalysis on FAPKC. In *Proc. ASIACRYPT'98*, Beijing, China, October 1998, *Lecture Notes in Computer Science 1514*, Ohta K, Pei D Y (eds.), Springer-Verlag, 1998, pp.227–241.
[101] Tao R J, Chen S H. On finite automaton public key cryptosystem. *Theoretical Computer Science*, 1999, 226(1-2): 143–172.
[102] Ye D F, Lam K Y, Dai Z D. Cryptanalysis of "2R" schemes. In *Proc. CRYPTO'99*, Santa Barbara, CA, USA, August 15–19, 1999, *Lecture Notes in Computer Science 1666*, Wiener M J (ed.), Springer-Verlag, 1999, pp.315–325.
[103] Ye D F, Dai Z D, Lam K Y. Decomposing attacks on asymmetric cryptography based on mapping compositions. *J. Cryptology*, 2001, 14(2): 137–150.
[104] Ye D F, Yang J H, Dai Z D, Ou H W. Attacks on two digital signature schemes based on error correcting codes. In *Proc. ICICS'01*, Xian, China, November 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.84–89.
[105] Dai Z D, Yang J H, Ye D F, Gong G. Cryptanalysis of Wang's original and revised digital signature scheme. *IEE Electronics Letters*, 2001, 37(4): 220.
[106] Dai Z D, Ye D F, Pei D Y. Cryptanalysis of ElGamal type encryption schemes based conic curves. *IEE Electronics Letters*, 2001, 37(7): 426.

[107] Zhang Z F, Feng D G, Dai Z D. Cryptanalysis on AW digital signature scheme based on error-correcting codes. *Science in China* (*Series E*), 2003, 33(2): 164–167.

[108] Wang X Y, Feng D G, Lai X J, Yu H B. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. *Cryptology ePrint Archive*: Report 2004/199. Aug. 2004.

[109] Wang X Y, Yu H B, Yin Y Q L. Efficient collision search attacks on SHA-0. In *Proc. CRYPTO'05*, Santa Barbara, CA, USA, August 14–18, 2005, *Lecture Notes in Computer Science 3621*, Shoup V (ed.), Springer-Verlag, 2005, pp.1–16.

[110] Wang X Y, Yin Y Q L, Yu H B. Finding collisions in the full SHA-1. In *Proc. CRYPTO'05*, Santa Barbara, CA, USA, August 14–18, 2005, *Lecture Notes in Computer Science 3621*, Shoup V (ed.), Springer-Verlag, 2005, pp.17–36.

[111] Wang X Y, Lai X J, Feng D G *et al.* Cryptanalysis of the hash functions MD4 and RIPEMD. In *Proc. EUROCRYPT'05*, Aarhus, Denmark, May 22–26, 2005, *Lecture Notes in Computer Science 3494*, Gramer R (ed.), Springer-Verlag, 2005, pp.1–18.

[112] Wang X Y, Yu H B. How to break MD5 and other hash functions. In *Proc. EUROCRYPT'05*, Aarhus, Denmark, May 22–26, 2005, *Lecture Notes in Computer Science 3494*, Gramer R (ed.), Springer-Verlag, 2005, pp.19–35.

[113] Chen X F, Zhang F G, Kim K. Chameleon hashing without key exposure. In *Proc. ISC'04*, Palo Alto, CA, USA, Sept. 27–29, 2004, *Lecture Notes in Computer Science 3225*, Zhang K, Zheng Y L (eds.), Springer-Verlag, 2004, pp.87–98.

[114] Cao Z F. A threshold key escrow scheme based on public key cryptosystem. *Science in China* (*Series E*), 2001, 44(4): 441–448.

[115] Yang B, Zhu S X, Wang Y M. Unconditionally-secure oblivious transfer. In *Proc. ICICS'01*, Xian, China, Nov. 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.35–41.

[116] Wang G L, Qing S H, Wang M S, Zhou Z F. Threshold undeniable RSA signature scheme. In *Proc. ICICS'01*, Xian, China, Nov. 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.221–232.

[117] Zhang F G, Kim K. ID-based blind signature and ring signature from pairings. In *Proc. ASIACRYPT'02*, Queenstown, New Zealand, Dec. 1–5, 2002, *Lecture Notes in Computer Science 2501*, Zheng Y L (ed.), Springer-Verlag, 2002, pp.533–547.

[118] Zhao Y L, Deng X T, Lee C H, Zhu H. Resettable zero-knowledge in the weak public-key model. In *Proc. EUROCRYPT'03,* Warsaw, Poland, May 4–8, 2003, *Lecture Notes in Computer Science 2656*, Biham E (ed.), Springer-Verlag, 2003, pp.123–139.

[119] Ma W P, Lee M H. Group oriented cryptosystems based on linear access structures information security and cryptology. In *Proc. Int. Conf. Info. Security and Cryptology* (*ICISC'03*), Seoul, Korea, November 27–28, 2003, *Lecture Notes in Computer Science 2971*, Lim J I, Lee D H (eds.), Springer-Verlag, 2004, pp.370–376.

[120] Zhang F G, Safavi-Naini R, Susilo W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings. In *Proc. INDOCRYPT'03*, New Delhi, India, Dec. 8–10, 2003, *Lecture Notes in Computer Science 2904*, Johansson T, Maitra S (eds.), Springer-Verlag, 2003, pp.191–204.

[121] Yao G, Ren K, Bao F, Deng R H, Feng D G. Making the key agreement protocol in mobile ad hoc network more efficient. In *Proc. 1st Int. Conf. Applied Cryptography and Network Security* (*ACNS'03*), Kunming, China, Oct. 16–19, 2003, *Lecture Notes in Computer Science 2846*, Zhou J Y *et al.* (eds.), Springer-Verlag, 2003, pp.343–356.

[122] Wu Q H, Zhang J H, Wang Y M. Practical t-out-n oblivious transfer and its applications. In *Proc. ICICS'03*, Huhehaote, China, Oct. 10–13, 2003, *Lecture Notes in Computer Science 2836,* Qing S H *et al.* (eds.), Springer-Verlag, 2003, pp.226–237.

[123] Zhang J H, Wu Q H, Wang Y M. A Novel efficient group signature scheme with forward security. In *Proc. ICICS'03*, Huhehaote, China, October 10–13, 2003, *Lecture Notes in Computer Science 2836,* Qing S H *et al.* (eds.), Springer-Verlag, 2003, pp.292–300.

[124] Li H D, Ji D Y, Feng D G, Li B. Oblivious polynomial evaluation, *J. Computer Science and Technology*, 2004, 19(4): 550–554.

[125] Li H D, Yang X, Feng D G, Li B. Distributed oblivious function evaluation and its applications, *J. Computer Science and Technology*, 2004, 19(6): 942–947.

[126] Chen X F, Zhang F G, Konidala D M, Kim K. New ID-based threshold signature scheme from bilinear pairings. In *Proc. INDOCRYPT'04*, Chennai, India, December 20–22, 2004, *Lecture Notes in Computer Science 3348*, Canteaut A, Viswanathan K (eds.), Springer-Verlag, 2004, pp.371–383.

[127] Chen Z W, Wang J L, Wang Y M *et al.* An efficient revocation algorithm in group signatures. In *Proc. Int. Conf. Info. Security and Cryptology* (*ICISC'03*), Seoul, Korea, Nov. 27–28, 2003, *Lecture Notes in Computer Science 2971*, Lim J I, Lee D H (eds.), Springer-Verlag 2004, pp.339–351.

[128] Chen W D, Feng D G. A group of threshold group-signature schemes with privilege subsets. Progress on Cryptography: 25 Years of Cryptography in China, Chen K F (ed.), Kluwer academic Publishers, Netherlands, 2004. See also: Chen W D, Feng D G. A group of threshold group-signature schemes with privilege subsets, *J. Software*, 2004, 16(7): 1289–1295.

[129] Zhang Z F, Feng D G, Xu J, Zhou Y B. Efficient ID-based optimistic fair exchange with provable security. In *Proc. ICICS'05*, Beijing, China, December 10–13, 2005, *Lecture Notes in Computer Science 3783*, Qing S H *et al.* (eds.), Springer-Verlag, 2005, pp.14–26.

[130] Wang H, Zhang Y Q, Feng D G. Short threshold signature schemes without random oracles. In *Proc. INDOCRYPT'05*, Bangalore, India, December 10–12, 2005, *Lecture Notes in Computer Science 3797*, Maitra S *et al.* (eds.), Springer-Verlag, 2005, pp.297–310.

[131] Ma C S, Chen K F, Zheng D, Liu S L. Efficient and proactive threshold signcryption, In *Proc. ISC'05*, Singapore, September 20–23, 2005, *Lecture Notes in Computer Science 3650*, Zhou J Y *et al.* (eds.), Springer-Verlag, 2005, pp.233–243.

[132] Xu J, Zhang Z F, Feng D G. A ring signature scheme using bilinear pairings. In *Proc. 5th Int. Workshop Info. Security Applications* (*WISA'04*), Jeju Island, Korea, August 23–25, 2004, *Lecture Notes in Computer Science 3325*, Lim C H, Yung M (eds.), Springer-Verlag, 2005, pp.160–169.

[133] Yao G, Feng D G. A new k-anonymous message transmission protocol. In *Proc. 5th Int. Workshop Info. Security Applications* (*WISA'04*), Jeju Island, Korea, August 23–25, 2004, *Lecture Notes in Computer Science 3325*, Lim C H, Yung M (eds.), Springer-Verlag, 2005, pp.388–399.

[134] Zhang Z F, Feng D G. Efficient fair certified E-mail delivery based on RSA. In *Proc. Parallel and Distributed Processing and Applications—ISPA 2005 Workshops*, Nanjing, China, Nov. 2–5, 2005, *Lecture Notes in Computer Science 3759*, Chen G H *et al.* (eds.), Springer-Verlag, 2005, pp.368–377.

[135] Xu J, Zhang Z F, Feng D G. ID-based proxy signature using bilinear pairings. In *Proc. Parallel and Distributed Processing and Applications—ISPA 2005 Workshops*, Nanjing, China, November 2–5, 2005, *Lecture Notes in Computer Science 3759*, Chen G H *et al.* (eds.), Springer-Verlag, 2005, pp.359–367.

[136] Zhang Z F, Xu J, Feng D G. Efficient identity-based protocol for fair certified E-mail delivery. In *Proc. 4th Int. Conf. Cryptology and Network Security* (*CANS'05*), Xiamen, China, Dec. 14–16, 2005, *Lecture Notes in Computer Science 3810*, Desmedt Y *et al.* (eds.), Springer-Verlag, 2005, pp.200–210.

[137] Xu J, Zhang Z F, Feng D G. ID-based aggregate signatures from bilinear pairings. In *Proc. 4th Int. Conf. Cryptology and Network Security* (*CANS'05*), Xiamen, China, Dec. 14–16, 2005, *Lecture Notes in Computer Science 3810*, Desmedt Y *et al.* (eds.), Springer-Verlag, 2005, pp.110–119.

[138] Lu X, Feng D G. An arbitrated quantum message signature scheme. In *Proc. 1st Int. Symp. Computational and Info. Science* (*CIS'04*), Shanghai, China, December 16–18, 2004, *Lecture Notes in Computer Science 3314*, Zhang J *et al.* (eds.), Springer-Verlag, 2004, pp.1054–1060.

[139] Gu C X, Zhu Y F. An ID-based verifiable encrypted signature scheme based on Hess's scheme. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, December 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.42–52.

[140] Liao J, Xiao J F, Qi Y H *et al.* ID-based signature scheme without trusted PKG. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.53–62.

[141] Cheng X G, Zhu H F, Qiu Y, Wang X M. Efficient group signatures from bilinear pairing. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp128–139.

[142] Shao Z H. Enhanced aggregate signature from pairing. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.140–149.

[143] Zhou Y, Cao Z F, Chai Z C. Constructing secure proxy cryptosystem. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.150–161.

[144] Li H D, Li B. An Unbounded simulation-sound non-interactive zero-knowledge proof system for NP. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.210–220.

[145] Li F G, Gao J T, Hu Y P. ID-based threshold unsigncryption scheme from pairings. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.242–253.

[146] Feng D G. Verifiable signature sharing for the DSA with heuristic security. *IEE Electronics Letters*, 1996, 32(15): 1570–1571.

[147] Dai Z D, Zhang Y F. Partition, construction and enumeration of M-P invertible matrices over finite fields. *Finite Fields and Their Applications*, July 2001, 7(3): 428–440.

[148] Feng D G , Chen W D. Analysis on the two classes of robust threshold key escrow schemes. Progress on Cryptography: 25 Years of Cryptography in China, Chen K F (ed.), Kluwer Academic Publishers, Netherlands, 2004. See also: Feng D G, Chen W D. Analysis on the two classes of robust threshold key escrow schemes. *Chinese Journal of Computers*, 2004, 27(9): 1170–1176.

[149] Zhang Z F, Feng D G. Cryptanalysis of some signature schemes with message recovery. *Applied Mathematics and Computation*, 2005, 170(1): 103–114.

[150] Zhou Y B, Zhang Z F, Feng D G. Cryptanalysis of the end-to-end security protocol for mobile communications with end-user identification/authentication. *IEEE Communications Letters*, 2005, 9(4): 372–374.

[151] Li Y, Lipmaa H, Pei D Y. On delegatability of four designated verifier signatures. In *Proc. ICICS'05*, Beijing, China, Dec. 10–13, 2005, *Lecture Notes in Computer Science 3783*, Qing S H *et al.* (eds.), Springer-Verlag, 2005, pp.61–71.

[152] Gao F, Qin S J, Wen Q Y, Zhu F C. An effective attack on the quantum key distribution protocol based on quantum encryption. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.302–312.

[153] Cao T J, Lin D D. Security analysis of some threshold signature schemes and multi-signature schemes. In *Proc. 1st SKLOIS Conf. Info. Security and Cryptology* (*CISC'05*), Beijing, China, Dec. 15–17, 2005, *Lecture Notes in Computer Science 3822*, Feng D G *et al.* (eds.), Springer-Verlag, 2005, pp.233–241.

[154] Liu D X, Li X Y, Bai Y C. An intelligent intruder model for security protocol analysis. In *Proc. ICICS'01, Xian, China*, November 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.13–22.

[155] Song Z M, Qing S H. Applying NCP logic to the analysis of SSL 3.0. In *Proc. ICICS'01*, Xian, China, November 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.155–166.

[156] Li Y F. A new semantics of authentication logic. In *Proc. ICICS'01*, Xian, China, November 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2001, pp.476–482.

[157] Huai J P, Li X X. Algebraic model for security protocols and its security. *Science in China* (*Series E*), 2003, 33(12): 1087–1106.

[158] Ji Q G, Qing S H, Zhou Y B, Feng D G. Study on strand space model theory. *J. Computer Science and Technology*, 2003, 18(5): 553–570.

[159] Xue R, Feng D G. New semantic model for authentication protocols in ASMs. *J. Computer Science and Technology*, 2004, 19(4): 555–563.

[160] Li X H, Ma J F, Wen X G. Extension to the Canetti-Krawczyk model for the identity-based cryptosystem. *Science in China* (*Series E*), 2004, 34(10): 1185–1191.

[161] Jing J W, Liu P, Feng D G *et al.* ARECA: A highly attack resilient Certification Authority. In *Proc. ACM Workshop on Survivable and Self-Regenerative Systems*, Fairfax, VA, USA, Oct. 31, 2003, pp.53–63.

[162] Feng D G, Xiang J. Experience on intrusion tolerance distributed systems. In *Proc. 29th Annual Int. Computer Software and Applications Conf.*, Edinburgh, UK, July 26–28, 2005, pp.270–271.

[163] Zhang L W, Feng D G. Intrusion tolerant CA scheme with cheaters detection ability. In *Proc. Parallel and Distributed Processing and Applications—-ISPA 2005 Workshops*, Nanjing, China, Nov. 2–5, 2005, *Lecture Notes in Computer Science 3759*, Chen G H *et al.* (eds.), Springer-Verlag, 2005, pp.378–386.

[164] Luo W J, Cao X B, Wang X F. NIDS research based on artificial immunology. In *Proc. ICICS'01*, Xian, China, Nov. 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2005, pp.371–375.

[165] Li H P, Chang L L, Wang X M. A useful intrusion detection system prototype to monitor multi-processes based on system calls. In *Proc. ICICS'01*, Xian, China, Nov. 13–16, 2001, *Lecture Notes in Computer Science 2229*, Qing S H *et al.* (eds.), Springer-Verlag, 2005, pp.441–450.

[166] Luo M, Wang L N, Zhang H G, Chen J. A research on intrusion detection based on unsupervised clustering and support vector machine. In *Proc. ICICS'03*, Huhehaote, China, Oct. 10–13, 2003, *Lecture Notes in Computer Science 2836,* Qing S H *et al.* (eds.), Springer-Verlag, 2003, pp.325–336.

[167] Sun J H, Jin H, Chen H *et al.* A compound intrusion detection model. In *Proc. ICICS'03*, Huhehaote, China, Oct. 10–13, 2003, *Lecture Notes in Computer Science 2836,* Qing S H *et al.* (eds.), Springer-Verlag, 2003, pp.370–381.

[168] Zhang M, Ju J B. Space-economical reassembly for intrusion detection system. In *Proc. ICICS'03*, Huhehaote, China, Oct. 10–13, 2003, *Lecture Notes in Computer Science 2836,* Qing S H *et al.* (eds.), Springer-Verlag, 2003, pp.393–404.

[169] Huang J W, Shi Y Q, Shi Y. Embedding image watermarks in DC components. *IEEE Trans. Circuits and Systems for Video Technology*, 2000, 10(6): 974–979.

[170] Huang J W, Shi Y Q. Reliable information bit hiding. *IEEE Trans. Circuits and Systems for Video Technology*, 2002, 12(10): 916–920.

[171] Zhu X S, Wang Y S. Better use of human visual model in watermarking based on linear prediction synthesis filter. In *Proc. 3rd Int. Workshop on Digital Watermarking* (*IWDW'04*), Seoul, Korea, Oct. 30–Nov. 1, 2004, *Lecture Notes in Computer Science 3304*, Cox I J *et al.* (eds.), Springer-Verlag, 2005, pp.66–76.

[172] Liu R Z, Tan T N. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimedia*, 2002, 4(1): 121–128.

[173] Lu Z M, Xu D G, Sun S H. Multipurpose image watermarking algorithm based on multistage vector quantization. *IEEE Trans. Image Processing*, 2005, 14(6): 822–831.

[174] Kang X G, Huang J W, Shi Y Q. An image watermarking algorithm robust to geometric distortion. In *Proc. 1st Int. Workshop on Digital Watermarking* (*IWDW'02*), Seoul, Korea, Nov. 21–22, 2002, *Lecture Notes in Computer Science 2613*, Fabien A P P *et al.* (eds.), Springer-Verlag, 2003, pp.212–223.

[175] Kang X G, Huang J W, Shi Y Q, Lin Y. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. *IEEE Trans. Circuits and Systems for Video Technology*, 2003, 13(8): 776–786.

[176] Xue G, Lu P Z, Wang J L. A counter-geometric distortions data hiding scheme using double channels in color images. In *Proc. 3rd Int. Workshop on Digital Watermarking (IWDW'04)*, Seoul, Korea, Oct. 30–Nov. 1, 2004, *Lecture Notes in Computer Science 3304*, Cox I J *et al.* (eds.), Springer-Verlag, 2005, pp.42–54.

[177] Hu J Q, Huang J W, Huang D R, Shi Y Q. A DWT-based fragile watermarking tolerant of JPEG compression. In *Proc. 1st Int. Workshop on Digital Watermarking* (*IWDW'02*), Seoul, Korea, Nov. 21–22, 2002, *Lecture Notes in Computer Science 2613*, Fabien A P P *et al.* (eds.), Springer-Verlag, 2003, pp.179–188.

[178] Zhao X F, Wang W N, Chen K F. Multimedia tampering localization based on the perturbation in reverse processing. In *Proc. 4th Int. Conf. Web-Age Info. Management* (*WAIM'03*), Chengdu, China, August 17–19, 2003, *Lecture Notes in Computer Science 2762*, Dong G Z *et al.* (eds.), Springer-Verlag, 2003, pp.483–494.

[179] Xuan G R, Yang C Y, Zhen Y Z, Shi Y Q, Ni Z C. Reversible data hiding using integer wavelet transform and companding technique. In *Proc. 3rd Int. Workshop on Digital Watermarking* (*IWDW'04*), Seoul, Korea, Oct. 30 – Nov. 1, 2004, *Lecture Notes in Computer Science 3304*, Cox I J *et al.* (eds.), Springer-Verlag, 2005, pp.115–124.

[180] Zhang X P, Wang S Z. Watermarking scheme capable of resisting attacks based on availability of inserter. *Signal Processing*, 2002, 82(11): 1801–1804.

[181] Zhang X P, Wang S Z. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. *Pattern Recognition Letters*, 2004, 25(3): 331–339.

[182] Zhang X P, Wang S Z. Invertibility attack against watermarking based on forged algorithm and a countermeasure. *Pattern Recognition Letters*, 2004, 25(8): 967–973.

[183] Lu P Z, Luo X Y, Tang Q Y, Shen L. An improved sample pairs method for detection of LSB embedding. In *6th Int. Workshop on Info. Hiding* (*IH'04*), Toronto, Canada, May 23–25, 2004, *Lecture Notes in Computer Science 3200*, Fridrich J J (ed.), Springer-Verlag, 2004, pp.116–127.

[184] Xuan G R, Shi Y Q, Gao J J *et al.* Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions. In *7th Int. Workshop on Info. Hiding* (*IH'05*), Barcelona, Spain, June 6–8, 2005, *Lecture Notes in Computer Science* 3727, Barni M *et al.* (eds.), Springer-Verlag, 2005, pp.262–277.

[185] Zhao X F, Dai Y X, Feng D G. Towards the public but noninvertible watermarking schemes. In *Proc. 3rd Int. Workshop on Digital Watermarking* (*IWDW'04*), Seoul, Korea, Oct. 30–Nov. 1, 2004, *Lecture Notes in Computer Science 3304*, Cox I J *et al.* (eds.), Springer-Verlag, 2005, pp.218–231.

[186] Zhao X F, Dai Y X, Feng D G. A generalized method for constructing and proving zero-knowledge watermark proof systems. In *Proc. 3rd Int. Workshop on Digital Watermarking* (*IWDW'04*), Seoul, Korea, Oct. 30 – Nov. 1, 2004, *Lecture Notes in Computer Science 3304*, Cox I J *et al.* (eds.), Springer-Verlag, 2005, pp.204–217.

[187] Zhu Y, Feng D G, Zou W. Collusion secure convolutional spread spectrum fingerprinting. In *Proc. 4th Int. Workshop on Digital Watermarking* (*IWDW'05*), Siena, Italy, September 15–17, 2005, *Lecture Notes in Computer Science 3710*, Barni M *et al.* (eds.), Springer-Verlag, 2006, pp.67–83.

Deng-Guo Feng is a professor and Ph.D. supervisor with the Institute of Software (IOS), Chinese Academy of Sciences (CAS). He is also a member of the Consultative Committee of National Informatization Specialists and director of State Key Laboratory of Information Security. In 1995, he received his Ph.D. degree in communication and information system from Xidian University and began to work as a post-doctor with the Graduate School of University of Science and Technology of China. In 1997, he joined IOS and was elected into the project of One Hundred Talents of CAS. Prof. Feng's research interests are in the areas of cryptology and information security. He has published 8 books and more than 150 papers in the influential journals and conferences. He acquired more than 30 technical patents and software copyrights. In years of productive work, Prof. Feng has received awards or honor from the National Scientific and Technological Progress Award, CAS Scientific and Technological Progress Award, Beijing Science and Technology Award, Ten Prominent CAS Young Researchers Project, Award for Prominent Individuals of State Key Laboratories Program, Award of Ten Excellent Doctoral Dissertations of China, CAS Young Scientists Project, and in particular, the National Foundation of Prominent Young Researchers. Now he is a member of the editorial boards of more than 10 journals, including Chinese Science Bulletin, J. Comput. Sci. & Technol., etc., and also a committee member of international conferences, such as Intern. Conf. Info. and Comm. Security (ICICS), Intern. Conf. Cryptology and Network Security (CANS), etc.

Xiao-Yun Wang is a professor and Ph.D. supervisor with the School of Mathematics and System Science, Shandong University (SU). In the years of 1987, 1990 and 1993, she received her B.S., M.S. and Ph.D. degrees respectively, all in mathematics and from SU. Since 2004, she has been a professor in the project of Zhenning Yang Lectures with Tsinghua University. In 2005, she was granted the National Foundation of Prominent Young Researchers. Prof. Wang's research interests are in the theory of cryptology. Among lots of achievements, the most recognized work of her and her group is the breaking of a series of widely used hash functions, on which she successfully gave the effective collision attacks. The work has been awarded by the Award for Advances in the Science and Technology of Cryptology. Prof. Wang has authored some papers having impact. 4 of them about the breaking of MD5 and SHA-1 received the awards for the best paper from the most influential conferences in the field, including EUROCRYPT, CRYPTO, etc.