Mathematical Problems of Computer Science 34, 2010.

Construction of Irreducible, Normal and Primitive Polynomials over Finite Fields

Melsik Kyureghyan
Institute for Informatics and Automation Problems

Cryptography has been experiencing a drastic development in contemporary times. This is highly conditioned by fast growth of network systems and progress of communication technologies for which information security has become a problem of special importance.

Secure, trustworthy and reliable delivery of information is a central problem in information theory and coding theory with applications in computer science and telecommunication. As a rule, error correcting/detecting codes used to provide reliable transmission of data over an unreliable communication channel are unstable and do not ensure required data protection. This has necessitated employment of joint coding: cryptographic coding for data encryption and error correcting/detecting coding to improve reliability of communication on a channel. Both types of coding are applied sequentially, guaranteeing security of information during communications.

Modern cryptography intersects the disciplines of mathematics, computer science and telecommunication, and is a cornerstone of computer and communications security. It addresses a wide range of problems, such as:

a) Electronic signatures are commonly used for signing digital documents and ensuring that downloaded applications are provided by a trusted source, and are central to the operation of public key infrastructures and many network security schemes.
Development of easy-realizable fast algorithms for electronic signature is one of hard problems.
b) Modern block ciphers are widely used to provide encryption of quantities of information, and/or a cryptographic checksum to ensure the contents have not been altered.
Design of easy-realizable fast algorithms for block ciphers remains a problem of high importance.

The problem of explicitly constructing irreducible, normal and primitive polynomials over Galois fields is one of the challenging problems in computer algebra, coding theory, cryptography and theory of finite fields and plays a major role in modern engineering, primarily due to wide use of such polynomials in variety of coding, cryptographic and computational applications. Moreover, recent advances in these areas have awakened an even more interest to the subject of such polynomials.

Researchers of Data Coding laboratory have conducted research on the theoretical foundations of cryptography, the application of cryptography to network and system security. Some theoretic and practical problems in this area have been attacked, particularly:

1. Several recurrent methods of constructing irreducible polynomials over finite fields have been proposed recently [1].
2. Some effective algorithms, employing recurrent methods to construct primitive polynomials over finite fields have been considered [1-2].
3. Security characteristics of block ciphers SAFER+ and SAFER++ of SAFER family have been investigated from theoretical and practical point of view. The coordinate permutation chosen for use in both ciphers SAFER+ and SAFER++ is the "Armenian Shuffle", which is used in place of 'Hadamard Shuffle' employed in the previous ciphers of the SAFER family. 'Armenian Shuffle' not only provides even better diffusion of SAFER+ and SAFER++ and enhances strength of these ciphers against both differential and linear cryptanalysis, but also runs significantly faster as it allows fewer number of encryption rounds in the cipher. This property enables building new cryptosystems, equivalent to SAFER+ and SAFER++ by their crypto characteristics, which would exceed previous ciphers in speed and would be similarly strongly secure against cryptanalysis [4-5].
4. New public-key encryption and public-key digital signature schemes have been proposed based on discrete logarithm problem. For the public-key encryption scheme it has been shown that the given algorithm has an advantage over well known El-Gamal public-key encryption scheme in terms of complexity of implementation and bandwidth efficiency. The specific of presented digital signature scheme is that the signature is addressed from a given user with a given public key to another user with a different public key so that only the recipient will be able to verify the signature from a specified user. The complexity of implementation is similar to Digital Signature Standard Algorithm (DSA) [3].

References

[1]M. K. Kyuregyan and G. M Kyureghyan. Irreducible compositions of polynomials over finite fields, ArXiv: 1008.18637v1 [math.NT] 11 August 2010. Accepted for publication in Designs, Codes and Cryptography, an International Journal, Editors-in-Chief: D. Jungnickel; J.D. Key; P. Wild.

[2] M. K. Kyuregyan. "Iterated constructions of irreducible polynomials over finite fields with linearly independent roots", *J. Finite Fields and Their Applications*, vol. 10, issue 3 (2004), pp. 323-341.

[3] Khachatrian G., Kyuregyan M., New Public Key Encryption and Signature Scheme. Proceedings of Russian-German- Armenian Workshop Applications of Information Theory, Coding and Security. Yerevan, Armenia April 14-16, 2010 pp. 31-34. http://ipia.sci.am/web/WAITSC2010.htm

[4] J. L. Massey, G. H. Khachatrian and M. K. Kuregian, Nomination of SAFER+ as Candidate algorithm for the Advanced Encryption Standard (AES), Submission document from Cylink Corporation to NIST, June 1998.

[5] J. L. Massey, G. H. Khachatrian and M. K. Kuregian, Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE), Submission document from Cylink Corporation, 2000.