20th International Crimean Conference
"Microwave & Telecommunication Technology"
13-17 September 2010, Sevastopol, Ukraine

Public key of cryptography over extended Galois fields

G. C. Bodyan, D. G. Bodyan, T. V. Shestakov

https://doi.org/10.1109/CRMICO.2010.5632471

Abstract

RSA-like public-key cryptosystem that allows high-speed encryption and decryption is developed. The security of a system is based on the complexity of finding of irreducible polynomials over extended Galois fields.

Keywords: cryptosystems, Galois fields, encryption, decryption

References

1. Rivest R., Shamir A., Adleman L. A method of obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. Vol.21. No. 2. P. 120-126.
CrossRef Google Scholar
2. David J. P., Kalach K., Tittley N. Hardware complexity of modular multiplication and exponentiation // IEEE Transactions on Computers. 2007. Vol. 56. No. 10. P. 1308-1319.
View Article Google Scholar
3. Wu C.-L., Lou D.-C., Chang T.-J. Computational complexity analysis of modular arithmetic for RSA cryptosystem // The 23 Workshop on Combinatorial Mathematics and Computation Theory. 2006. P. 215-224.
Google Scholar
4. Kravitz D. W., Reed I. S. Extension of RSA Crypto-Structure: a Galois Approach // Electronic Letters. 1982. Vol. 18. No.6. P. 255-256.
CrossRef Google Scholar
5. Delsarte P., Piret P. Comment on Extension of RSA Crypto-Structure: a Galois Approach // Electronic Letters. 1982. Vol.18. No.6. P. 582-583.
CrossRef Google Scholar
6. Knuth D. The art of Computer programming, Vol. 2: Semi-numerical algorithms (3-ed.) Addison-Wesley, 1997. 762 p.
Google Scholar
7. Ferguson N., Schneier B., Kohno T. Cryptography engineering. John Wiley & Sons, 2010. 784 p.
Google Scholar