УДК 312.26.004

Ю. А. Биленко, А. Е. Жуков

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА ПРЕОБРАЗОВАНИЙ, ЛЕГКО РЕАЛИЗУЕМЫХ НА СТАНДАРТНЫХ PC-ПРОЦЕССОРАХ

Приведен поиск отдельных преобразований, легко реализуемых на стандартном PC-процессоре, проанализированы их свойства с точки зрения эффективности их использования для построения стойких высокоскоростных программно-ориентированных алгоритмов шифрования.

Cryptographic properties of transformations easily realised on standard PC-processors / Yu.A. Bilenko, A.E. Zhukov // Vestnik MGTU. Priborostroenie. 2000. No. 2. P. 92–105.

Search of transformations easily realised on standard PC-processor, is considered. Their features are predicted from the viewpoint of their effective application for building the durable high-speed program-oriented cryptooperation algorithms. Figs.2. Tabs.2. Refs.12.

СПИСОК ЛИТЕРАТУРЫ

1. Lai X., Massey J. A proposal for a new block encryption standard. Proc. Eurocrypt–90 // Lect. Notes Comput. Sci. – 1991. – No. 473. – P. 389–404.
2. Кузнецов Ю. В., Шкарин С. А. Коды Рида–Маллера (обзор публикаций) // Математические вопросы кибернетики. – Вып. 6. – М.: Наука, 1996. – С. 5–50.
3. Feistel H. Cryptography and computer privacy. Scientific America. – 1973. – 228. No. 5. – P. 15–23.
4. Kam J. B., Davida G. I. Structured design of substitution-permutation encryption networks. IEEE Trans. Comput. – 1979. – V. 28. No. 10. – P. 747–753.
5. Meier W., Staffelbach 0. Nonlinearity criteria for cryptographic functions. Proc. Eurocrypt-89 // Lect. Notes Comput. Sci. – 1990. – No. 434. – P. 549–562.
6. Rothaus O. S. On “bent” functions. J. Comb. Theory (A). – 1976. – V. 20. – P. 300–305.
7. Rueppel R. A. Analysis and design of stream ciphers. – N.Y.: Springer-Verlag, 1986.
8. Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory. – 1984. – V. 30. – P. 776–780.
9. Xiao G. Z., Massey J. L. A spectral characterization of correlation- immune combining functions. IEEE Trans. Inform. Theory. – 1988. – V. 34. – P. 569–571.
10. Preneel B., Van Leekwijk W., Van Linden L., Govaerts R., Vandewalle J. Propagation characteristics of boolean functions. Proc. Eurocrypt-90 // Lect. Notes Comput. Sci. – 1991. – No. 473. – P. 161–173.
11. Webster A. F., Tavares S. E. On the design of S-boxes. Proc. Crypto-85 // Lect. Notes Comput. Sci. – 1986. – No. 218. – P. 523–534.

12. F o r r e R. The strict avalanche criterion: spectral properties of boolean functions and an extended definition. Proc. Crypto-88, Berlin, Heidelberg, New York: Springer-Verlag, 1990. – P. 450–468.

Статья поступила в редакцию 28.12.1999

Алексей Евгеньевич Жуков родился в 1952 г., окончил в 1974 г. МГУ им. М.В. Ломоносова. Канд. физ.-мат. наук, доцент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Имеет более 50 научных работ в области защиты информации.

A.E. Zhukov (b. 1952) graduated from the Lomonosov Moscow States University in 1974. Ph. D. (Phys.-Math.), ass. professor of “Information Security” Department of the Bauman Moscow State Technical University. Author of more than 50 publications in the field of protection of information.

Юрий Александрович Биленко родился в 1975 г., окончил МГТУ им. Н.Э. Баумана в 1998 г., инженер-программист ЗАО “ЦНТ Телеком-Сервис”. Специализируется в области защиты информации.

Yu.A. Bilenko (b. 1975) graduated from the Bauman Moscow State Technical University in 1998. Specialises in the field of information security.