ELLIPTIC CURVE CRYPTOGRAPHY

Высоцкий Г.В., Супринович И.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Рогачевская А.И. — ст. преп.

Elliptic curve cryptography (ECC) is an actual topic in cryptography. Analysis of the algorithms used in ECC is required in terms of minimizing their computational complexity in hardware implementation and their implementation on modern processors. This paper attempts to present this area and its main concepts.

Computer technologies are widely used in our daily life nowadays. It is difficult to imagine an enterprise or a company that can exist without personal computers. It is nearly impossible to keep all the information in your head or on paper, that is why computer technology is so valuable in our specific digital world. The aim of computer technologies is to help humanity, but alongside with it all their unlimited possibilities they can bring new problems. The main one is protecting information from unauthorized access and it is a more important process than the development of new information technologies. However, with improvement of security systems, hacking algorithms are constantly being improved. And this in turn requires immediate improvement and increased reliability of the protection of personal data.

The main direction of cryptology is cryptography, that studies the mathematical methods of protecting information. It is cryptography that studies the methods of converting information to ensure its confidentiality and integrity. [2]

These methods can be applied in any field of human activity. They are used both for protection and for hiding genuine information that is transmitted through any communication channel. [1]

Modern cryptography implements many different encryption methods, most of which are used in modern devices.

In this paper, I examine various encryption algorithms (in public key cryptosystems). Numerical values were selected as information for encryption and decryption. And the elliptic curves were chosen as the main means for the design and implementation of encryption algorithms.

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems were secure due to the fact that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element provided a publicly base point is known is infeasible: this is the “elliptic curve discrete logarithm problem” (ECDLP). The security of elliptic curve cryptography depends on possibility to compute a point multiplication and impossibility to compute the multiplicand given by the original and product points. The size of elliptic curve determines the difficulty of the problem.

ECC (Elliptic Curve Cryptography) is currently widely used in public key cryptography applications (e.g. TLS (Transport Layer Security), ECDSA (Elliptic Curve Digital Signature Algorithm), OpenPGP, SSH (Secure Shell Transport Layer), cryptocurrencies). Analysis of the algorithms used in ECC is necessary to minimize their computational complexity in hardware implementation and their implementation in modern processors. ECC requires smaller keys compared to non-EC cryptography (based on Galois fields) to provide equivalent security. [4]

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. They can also be used for encryption by combining the key agreement with a symmetric encryption scheme and in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as elliptic-curve factorization method (ECM).

The purpose of this paper is the analysis of ECC algorithms to provide recommendations for their practical application in implementation on 32-bit and 64-bit processors.

ECC based methods help to increase the speed of generating and verifying digital signatures. These methods are used due to the growing requirements for hardware performance to achieve the required high overall throughput of data processing systems. Reducing the computational complexity of algorithms will improve the performance of computing systems based on existing hardware platforms or develop more efficient specialized computing systems based on performance-optimized solutions in 32-bit and 64-bit processors.

References:

1. Barichev, S.G. Fundamentals of modern cryptography: a manual / S.G. Barichev, R.E.Serov. – Telecom, 2002.
2. Bolotov, A.A. An elementary introduction to elliptical cryptography. Cryptography protocols on elliptic curves / A.A.Bolotov, S. B. Gashkov, A.B. Frolov A.B. – KomKniga, 2006.
3. Ryabko B.Ya. Cryptographic methods of information security / B.Ya.Ryabko, A.N.Fionov. – Telecom, 2005.
4. Knepp E. Elliptic curves / E.Knepp. – Factorial Press, 2004