Elliptic Curves –
Strong cryptography efficiently implemented

Uwe Krieger, cv cryptovision gmbh

New cryptoalgorithms make their way: In symmetric procedures, AES is the successor of the DES, and in the Public Key area, ECC endeavors to replace RSA as standard algorithm.

Modern cryptoalgorithms can roughly be devided into two classes: Symmetric and asymmetric procedures, also known as Public Key algorithms. The most popular example in the field of symmetric ciphers is DES, which was developed by IBM in the mid-seventies. Although its design is still considered pioneering, it is now no longer considered to be secure due to its short key length of 56 Bit. Therefore, the U.S. *National Institute of Standards and Technology* (NIST) set forth to determine a replacement. The key data for this algorithm called AES (*Advanced Encryption Standard*) defines new standards for security of cryptographic algorithms. Candidates of the upcoming standard are required to employ key lengths of 128, 192 and 256 Bit.

Today most hybrid methods were implemented using a fast, symmetric cipher for encryption and an asymmetric mechanism for key exchange or key transmission. Because the IT infrastructure and machines are rapidly developing, the asymmetric algorithms must also meet this new requirements. e.g.: RSA requires to employ key lengths of 4,096 up to more than 10.0000 Bit to maintain the same security level. This is no longer practicable.

There are alternatives. The most popular method is encryption based on elliptic curves (*Elliptic Curve Cryptography*, ECC). This class of procedures reduces key lengths, significantly speeds up calculation time, and simplifies key management. A look at standardization efforts of the past years shows, that ECC is not a proprietary solution: In all documents dealing with Public Key protocols (e.g. by ANSI, IEEE, ISO) algorithms based on ECC are of significant importance.

As the encryption basis of the RSA algorithm is the factorization of a number into its prime factors, the algorithms based on elliptic curves deal with the so-called problem of discrete logarithm (DL problem). This is based on the fact that in certain structures the reversion of a defined operation (exponentiation) is not possible for certain parameter sizes. The identification of this problem formed the basis for the key exchange procedure proposed by and named after W. Diffie and M. Hellman in 1977.

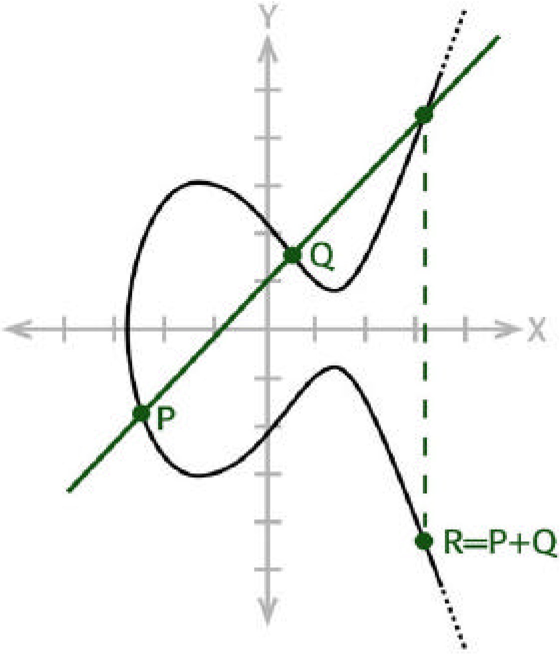
In 1985, two mathematicians, N. Koblitz and V. Miller, discovered independently that a known, intensively researched structure in mathematics is suitable for employment in cryptography. In the group of points of elliptic curves, a group law can be developed (see illustration) in which all protocols existing for the DL problem can be easily transfered and which rules out all possibilities of attack usually available to the attacker.

ECC's advantages in comparison to RSA are convincing: less memory requirement and computation time. Key lengths of 160 Bit as in ECC ensure the security of a RSA key of 1024 Bit, which is used as a standard today. With greater key lengths, the advantages of ECC compared to RSA increase intensively. While RSA would have to double its key lengths, ECC only needs a few Bit to achieve the same level of security. The RSA procedure currently changes its key length to 2048 Bit. As a result, ECC algorithms only have to increase its key length to 192 Bit.

The differences between the individual key lengths become fully apparent for the implementation in restricted environments. Devices like smartcards or USB-dongles normally use processors which are hardly capable to accomplish the conversion to a higher key length.

But the efficiency of algorithms is not the only decisive factor. Other issues are the secure creation and distribution of cryptographic keys. Also for this problems, ECC offers a lot of advantages against other algorithms. All in all, this is a family of algorithms which has proved its practical suitability and which has a lot of interesting features.

Picture:



The rule for the addition of two points on an elliptic curve.

40-digit credit about company and author:

cryptovision is the developer of cryptographic solutions. With its cv act product family the company provides modularly structured software solutions for security problems as well as implementations of algorithms for specific hardware platforms. More information can be found on http://www.cryptovision.com.