Curve25519 ECDH

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is one of the most powerful but least understood types of cryptography in wide use today.

**Curve25519** is an [elliptic curve](https://en.wikipedia.org/wiki/Elliptic_curve_cryptography) offering 128 bits of security and designed for use with the [elliptic curve Diffie–Hellman](https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman) (ECDH) key agreement scheme. It is one of the fastest ECC curves and is not covered by any known patents.

**The dawn of public key cryptography**

In 1977 [RSA algorithm](http://en.wikipedia.org/wiki/RSA_(algorithm)) and the [Diffie-Hellman](http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange" \t "_blank) key exchange algorithm were introduced. These new algorithms were revolutionary because they represented the first viable cryptographic schemes where security was based on the theory of numbers. Public key cryptographic system is a set of algorithms that is easy to process in one direction, but difficult to undo.

In the case of RSA, the easy algorithm multiplies two prime numbers. If multiplication is the easy algorithm, its difficult pair algorithm is factoring the product of the multiplication into its two component primes. Algorithms that have this characteristic — easy in one direction, hard the other — are known as [Trap door Functions](http://en.wikipedia.org/wiki/Trapdoor_function). Finding a good Trapdoor Function is critical to making a secure public key cryptographic system.

### Not a perfect Trapdoor

RSA and Diffie-Hellman were so powerful because they came with rigorous security proofs. The authors proved that breaking the system is equivalent to solving a mathematical problem that is thought to be difficult to solve. Factoring is a very well known problem and has been studied since antiquity (see [Sieve of Eratosthenes](http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes)).

 factoring is not the hardest problem on a bit for bit basis. Specialized algorithms like the [Quadratic Sieve](http://mathworld.wolfram.com/QuadraticSieve.html) and the [General Number Field Sieve](http://en.wikipedia.org/wiki/General_number_field_sieve) were created to tackle the problem of prime factorization and have been moderately successful. These algorithms are faster and less computationally intensive than the naive approach of just guessing pairs of known primes.

These factoring algorithms get more efficient as the size of the numbers being factored get larger. The gap between the difficulty of factoring large numbers and multiplying large numbers is shrinking as the number (i.e. the key's bit length) gets larger. As the resources available to decrypt numbers increase, the size of the keys need to grow even faster. This is not a sustainable situation for mobile and low-powered devices that have limited computational power. The gap between factoring and multiplying is not sustainable in the long term.

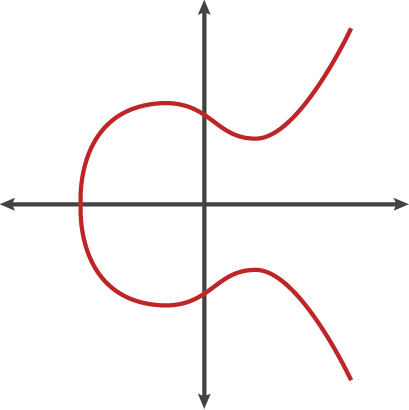
All this means is that RSA is not the ideal system for the future of cryptography. In an ideal Trapdoor Function, the easy way and the hard way get harder at the same rate with respect to the size of the numbers in question. We need a public key system based on a better Trapdoor.

### Elliptic curves: Building blocks of a better Trapdoor

An elliptic curve is the set of points that satisfy a specific mathematical equation. The equation for an elliptic curve looks something like this:

y2 = x3 + ax + b

An elliptic curve is the set points satisfying an equation in two variables with degree two in one of the variables and three in the other.



ECDH (Elliptic Curve Diffie-Hellman) is the version of Diffie-Hellman key exchange algorithm for elliptic curves, which determines the method how two communication participants A and B can generate key pairs and exchange their public keys via insecure channels. The algorithm determines only the method how key pairs are generated, the user defines the relation between encryption keys and data to be encrypted [7, 12]. After the keys have been exchanged it is common to use symmetric encryption methods. In practice, ECDH crypto system can be successfully adapted to different data security solutions [7]. The ECDH algorithm: Given an elliptic curve over finite prime field E(Fp). Communication participants A and B agree on a point Q ∈ E(Fp) , which is freely available in the communication medium. The participant A secretly chooses probabilistic positive integer kA, calculates kAQ and sends it to the party B. The member B also selects probabilistic positive integer kB, calculates kBQ and sends it to the participant A. The shared secret P = kA kBQ. The participant A calculates P, by multiplying the received point kBQ with the secret private key kA. The participant B respectively calculates P by multiplying the received point kAQ with the secret private key kB [12]. After the public key exchange, one of the most typical methods how the encrypted messages are synchronized is the version of ElGamal crypto system for elliptic curves [1]. As the set E(Fp) is finite there is a limited set of information which could be encrypted by using points of the curve [1]. Also, there are no practical methods available to deterministically generate points of the given curve [1]. The problem can be solved by creating relation between the x-coordinate of given curve point P ∈ E(Fp) and a field Fp element that may not be a point on the curve [1]. There are algorithms Compress Point and Decompress Point available which allow reduction of the amount of memory required for storing the curve points in the computer memory by two times. It is possible to clearly identify the curve point P = (xy) by specifiying the x-coordinate of point P and parity bit b. b ≡ y (mod 2)

Summary

Despite the several decades long history of the elliptic curve cryptography, there is still a lack of research. The popular RSA crypto system is more widely studied. A significant lack of research is one of the main reasons why elliptic curve based crypto systems have showed low popularity nowadays. It is possible to conclude that the lack of research is related to the relatively complex mathematical foundation of elliptic curves and lack of interest from the systems developers. It is expected that elliptic curves will play a growing role in various implementations. As mentioned, the discrete logarithm problem is algorithmically harder than the integer factorization problem, allowing a significant reduction in the public key cryptographic key size, thus speeding up a variety of cryptographic operations. Elliptic curve based crypto systems can be effectively used on low resources and power system solutions such as smart cards, mobile devices, sensors and so on. The vast majority of implementation issues of elliptic curve based crypto systems are not directly related to the fundamental security backgrounds. These issues are related to the factors such as faulty software, inappropriate system components, inadequate private key protection, usage of defective random number generators and cryptographic hash functions etc. Implementation options: • The most used crypto systems such as ECDH and ECDSA are standardized and patent free. They are free to use. • There are available NIST standardized elliptic curves for various security requirements. • Free access to the extensive information on algorithms for elliptic curves based crypto systems. Benefits of elliptic curve based crypto systems versus RSA crypto system: • Key size. The key of an elliptic curve based crypto system takes significantly less memory. The ratio increases rapidly with the increase of security levels. For instance, RSA crypto system with the key length of 1024 bits, is equivalent to an elliptic curve crypto system with the key length of 163 bits. • Cryptographic operations performance. Thanks to the smaller size of keys, the cryptographic operations such as key and digital signature generation are carried out significantly faster. For instance, an elliptic curve crypto system with the key length of 233 bits corresponds to RSA crypto system with the key length of 2240 bits. In the first case the key is generated approximately 40 times faster. 42 K. Magons • Resource savings. Due to the smaller key sizes, algorithms of an elliptic curve based crypto systems can be executed on very limited resources. Disadvantages of elliptic curve based crypto systems versus RSA crypto system: • Significantly more complex mathematical backgrounds. • Relatively large group of weak elliptic curves. • Lack of research.

## Elliptic Curve

ECC stands for Elliptic Curve Cryptography, which is an approach to public key cryptography based on elliptic curves over finite fields. Cryptographic algorithms usually use a mathematical equation to decipher keys; ECC, while still using an equation, takes a different approach.

SSL/TLS Certificates most commonly use RSA keys and the recommended size of these keys keeps increasing (e.g. from 1024 bit to 2048 bit a few years ago) to maintain sufficient cryptographic strength. An alternative to RSA is ECC. Both key types share the same important property of being asymmetric algorithms (one key for encrypting and one key for decrypting). However, ECC can offer the same level of cryptographic strength at much smaller key sizes - offering improved security with reduced computational and storage requirements.

**In Use Today?**- Yes. [NIST has recommended 15 elliptic curves](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf) that can be used as standard. Some argue that it is weak because vulnerabilities have been found that allow an attacker to execute certain types of attack although there are ways to combat these. Other reasons for a lack in popularity are to do with the random key generator created by NIST, dubbed [Dual Elliptic Curve Deterministic Random Bit Generator or DUAL\_EC\_DRBG](https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/) for short. Some believed that the generator (developed by the NSA) wasn’t as random as you might think – it was later discontinued.

**Elliptic Curve**

Elliptic Curve Cryptography (ECC) is a newer alternative to public key cryptography. ECC operates on elliptic curves over finite fields. The main advantage of elliptic curves is their efficiency. They can offer the same level of security for modular arithmetic operations over much smaller prime fields. Thus, the relative performance of ECC algorithms is significantly better than traditional public key cryptography.

ECDH is a method for key exchange and ECDSA is used for digital signatures. ECDH and ECDSA using 256-bit prime modulus secure elliptic curves provide adequate protection for sensitive information. ECDH and ECDSA over 384-bit prime modulus secure elliptic curves are required to protect classified information of higher importance.