Ethereum format, as hex with prefix `02` or `03`) is: `0x02f54ba86dc1ccb5bed0224d23f01ed87e4a443c47fc690d7797a13d41d2340e1a`. In this format the public key actually takes 33 bytes (66 hex digits), which can be optimized to exactly 257 bits.

Curves and Key Length

ECC crypto algorithms can use different underlying **elliptic curves**. Different curves provide different level of **security** (cryptographic strength), different **performance** (speed) and different **key length**, and also may involve different algorithms.

ECC curves, adopted in the popular cryptographic libraries and security standards, have **name** (named curves, e.g. `secp256k1` or `Curve25519`), **field size** (which defines the key length, e.g. **256-bit**), security **strength** (usually the field size / 2 or less), **performance** (operations/sec) and many other parameters.

ECC keys have **length**, which directly depends on the underlying curve. In most applications (like OpenSSL, OpenSSH and Bitcoin) the default **key length** for the ECC private keys is **256 bits**, but depending on the curve many different ECC key sizes are possible: 192-bit (curve `secp192r1`), 233-bit (curve `sect233k1`), 224-bit (curve `secp224k1`), 256-bit (curves `secp256k1` and `Curve25519`), 283-bit (curve `sect283k1`), 384-bit (curves `p384` and `secp384r1`), 409-bit (curve `sect409r1`), 414-bit (curve `Curve41417`), 448-bit (curve `Curve448-Goldilocks`), 511-bit (curve `M-511`), 521-bit (curve `P-521`), 571-bit (curve `sect571k1`) and many others.

ECC Algorithms

Elliptic-curve cryptography (ECC) provides several groups of algorithms, based on the math of the elliptic curves over finite fields:

- ECC **digital signature** algorithms like **ECDSA** (for classical curves) and **EdDSA** (for twisted Edwards curves).
- ECC **encryption** algorithms and hybrid encryption schemes like the **ECIES** integrated encryption scheme and **EEECC** (EC-based ElGamal).
- ECC **key agreement** algorithms like **ECDH**, **X25519** and **FHMQV**.

All these algorithms use a **curve** behind (like `secp256k1`, `curve25519` or `p521`) for the