Elliptische-Kurven-Kryptografie

ECC

Elliptic Curve Cryptography

Asymmetrisches Kryptosystem

Operationen auf elliptischen Kurven über endlichen Körpern

z. B. wird mit einer Schlüssellänge von 160 Bit eine ähnliche Sicherheit erreicht wie bei RSA mit 1024 Bit

eignet sich daher besonders dann, wenn die Speicher- oder Rechenkapazität begrenzt ist

kann bei einem vergleichbaren Sicherheitsniveau schneller sein

in Reisepässen und Personalausweisen in Deutschland

- Passive Authentication
- Extended Access Control

Patente

- prinzipiell patentfrei
- da bereits aus 1994
- RFC 6090

Firefox, Thunderbird

- min. 256 Bit Key-Länge

ab Windows Vista unterstützt

www.wenzlaff.info

Quelle: Elliptic Curve Cryptography – Wikipedia