Implementation of an ECC with M-511

CS488 - Introduction to IT Security

Who? Yoann Kehler, Duong Ta

When? April 12, 2017

Outline

- Why is non-elliptic curve cryptography not enough?
- What is an elliptic curve?
- Why M-511?

The Discrete Logarithm Problem[7]

Finite abelian Group, with multiplication

$$(P, Q) \mapsto P \cdot Q$$

The Discrete Logarithm Problem[7]

Finite abelian Group, with multiplication

$$(P, Q) \mapsto P \cdot Q$$

An element P generates a cyclic Subgroup with order n

$$\langle P \rangle = \{P^k : k \in \mathbb{Z}\}$$

$$n = ord(P) = |\langle P \rangle|$$

The Discrete Logarithm Problem[7]

Finite abelian Group, with multiplication

$$(P, Q) \mapsto P \cdot Q$$

An element P generates a cyclic Subgroup with order n

$$\langle P \rangle = \{P^k : k \in \mathbb{Z}\}$$

$$n = ord(P) = |\langle P \rangle|$$

The Discrete Logarithm Problem (DLP):
For a given P and $Q \in \langle P \rangle$ determine k s.t.

$$Q = P^k$$

The Discrete Logarithm Problem[7]

Finite abelian Group, with addition

$$(P, Q) \mapsto P + Q$$

An element P generates a cyclic Subgroup with order n

$$\langle P \rangle = \{kP : k \in \mathbb{Z}\}$$

$$n = ord(P) = |\langle P \rangle|$$

The Discrete Logarithm Problem (DLP):
For a given P and $Q \in \langle P \rangle$ determine k s.t.

$$Q = kP$$

Finding the right abelian group

Choose the abelian group s.t. the DLP becomes *difficult* to solve. Obviously n must be big enough.

$(\mathbb{F}_p, \cdot)$ is used in:

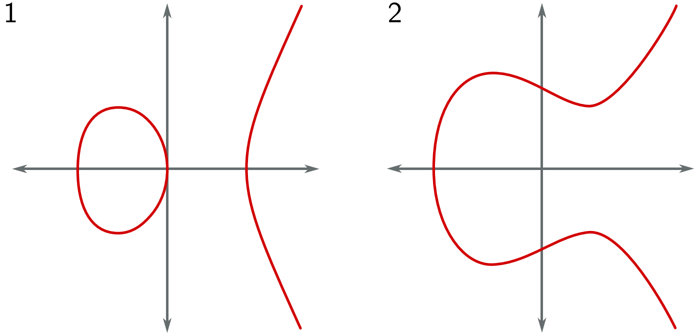
- Digital Signature Algorithm (DSA)
- Diffie-Hellman (DH)
- El-Gamal
- RSA (on IFC)

RSA & DSA Keysize

Security strength	Symmetric algorithm	FFC(DSA)	IFC(RSA)
≤ 80	2TDEA	$L = 1024$ $N = 160$	$K = 1024$
112	3TDEA	$L = 2048$ $N = 224$	$K = 2048$
128	AES-128	$L = 3072$ $N = 256$	$K = 3072$
192	AES-192	$L = 7680$ $N = 384$	$K = 7680$
256	AES-256	$L = 15360$ $N = 512$	$K = 15360$

Table: Security Strength of DSA and RSA from NIST[2]

Continuous Eliptic Curve Cryptography

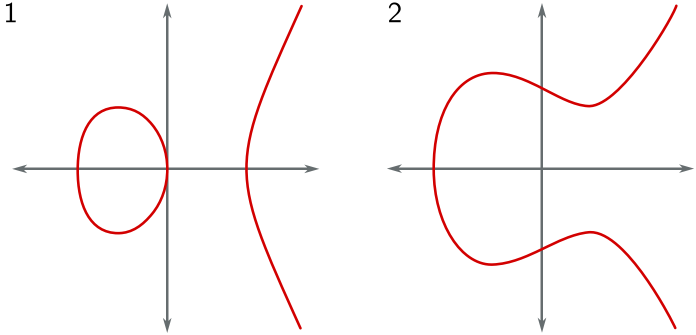


$y^2 = x^3 - x$ $\qquad$ $y^2 = x^3 - x + 1$

Figure: Two eliptic curves over $\mathbb{R}$ [6]

Elements: points on the curve

Continuous Eliptic Curve Cryptography



$y^2 = x^3 - x$ $\qquad$ $y^2 = x^3 - x + 1$

Figure: Two eliptic curves over $\mathbb{R}$ [6]

Elements: points on the curve

- Rounding errors
- Not suitable for cryptography

Eliptic curves over finite fields

- Make it discrete!
- "Random" jumps through a set of points

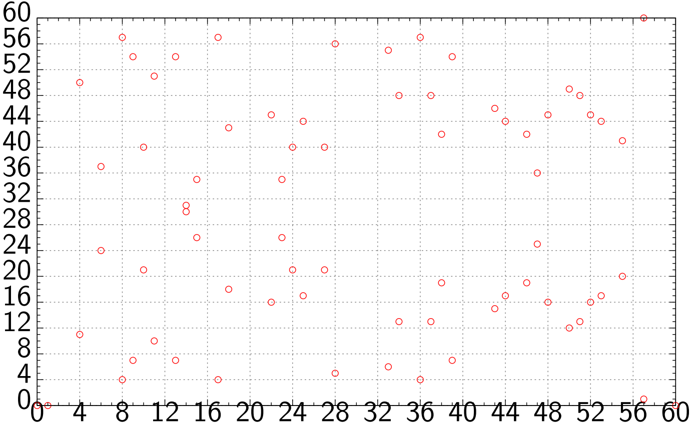


Figure: Set of affine points of elliptic curve $y^2 = x^3 - x$ over finite field $\mathbb{F}_{61}$.

ECC key sizes

Security strength	IFC(RSA)	ECC
≤ 80	$k = 1024$	$f = 160 - 223$
112	$k = 2048$	$f = 224 - 255$
128	$k = 3072$	$f = 256 - 383$
192	$k = 7680$	$f = 384 - 511$
256	$k = 15360$	$f = 512+$

Table: Security Strength of ECC compared to RSA[2]

Handshake size of ECC compared to RSA

RSA key (bits)	X.509 certificate (bytes)	Handshake, no chain (bytes)	Handshake, chain (bytes)
1024	589	1225	2073
2048	845	1481	2585
3072	1101	1737	3097
4096	1357	1993	
ECC key (bits)	**X.509 certificate (bytes)**	**Handshake, no chain (bytes)**	**Handshake, chain (bytes)**
160	291	959	1277
224	315	983	1317
256	331	999	1349
288	347	1015	

Table: Sizes of handshakes and certificates with ECC and RSA[5]

NIST-Curves

The National Institute for Standards and Technology (NIST) proposed some cryptographic curves in 1999.

- Special characteristics for efficiency
- Chosen "randomly"

ECC is not as hard as ECDLP!
Some attacks can be performed on special classes of curves.

- Surprise! Attacks on NIST-Curves have been found
- NIST-Curves were probably not chosen at random

[4]

Alternatives: Curve25519, M-511, M-383, ...

Curve25519:

- Proposed by Daniel Bernstein [3]
- No security flaws found until today
- De facto standard implemented in most libraries

M-511, M-383, M-221, E-521, E-382, E-222:

- Proposed by Diego F. Aranha et. al. [1]
- No security flaws found until today

Term Project

Goals for the semester:

- understand the maths behind ECC
- implement a library with M-511 with:
  - key generation
  - en-/decryption
  - signature and verification

"Never implement your own crypto"

We will not:

- Implement a library for real-world use
- Care about side-channel attacks

References I

- Diego F. Aranha et al. *A note on high-security general-purpose elliptic curves*. Cryptology ePrint Archive, Report 2013/647. http://eprint.iacr.org/2013/647. 2013.
- Elaine Barker et al. "Recommendation for key management part 1: General (revision 4)". In: *NIST special publication* 800.57 (2016), pp. 1–147.
- Daniel J Bernstein. "Curve25519: new Diffie-Hellman speed records". In: *International Workshop on Public Key Cryptography*. Springer. 2006, pp. 207–228.
- Daniel J. Bernstein and Tanja Lange. *SafeCurves: choosing safe curves for elliptic-curve cryptography.* URL: https://safecurves.cr.yp.to (visited on 03/13/2017).

References II

- Frédéric Cuppens et al. *FPS 2014: 7th International Symposium on Foundations and Practice of Security: revised selected papers*. 2015.
- Yassine Mrabet. URL: https://en.wikipedia.org/wiki/Elliptic_curve#/media/File:ECClines-3.svg (visited on 03/13/2017).
- Annette Werner. *Elliptische Kurven in der Kryptographie*. Springer-Verlag, 2013.