Elliptic Curves and Their Usage in Cryptography From a Programmer's Perspective

Vojtěch Fiala

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

April 15, 2024

- Mathematical equation satisfying

$$y^2 = x^3 + ax + b$$

- Coefficients a, b must satisfy

$$4a^3 + 27b^2 \neq 0$$

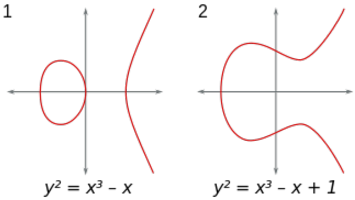

Figure: Example of elliptic curves[1]

[1] Image taken from
https://en.wikipedia.org/wiki/Modular_elliptic_curve

- Addition
  - Identity
  - Negative point
  - Doubling
  - Addition

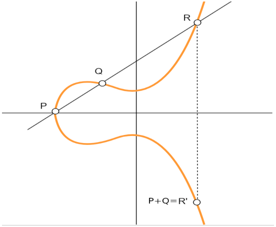

Figure: Geometric addition[2]

- Multiplication – based on repeated addition

[2] Image taken from https://www.educative.io/answers/what-is-elliptic-curve-cryptography

- Key exchange – ECDH
- Signature generation/verification – ECDSA
- Encryption – ECIES

Implementation Issues

- Curve selection – each curve has different parameters and each implementation has different requirements, such as:
  - Power requirements
  - Performance
- Public key generation – $pubKey = privKey \cdot G$ – issues with RNGs
- Point validation – before computing anything on a key that is provided by the other side of the communication, the point needs to be validated. This includes, for example, check that the point is not the identity element or that the point lies on the curve at all.

Algorithm 1 Double-And-Add Algorithm

Input: point P, n $\in \mathbb{N}$, k = number of bits in n
Output: n $\cdot$ P

```
R ← ∞ ▷ Point at infinity, represented as zero in practice.
▷ Move downwards across bit representation of n
for i in range (k − 1, 0, −1) do
    R ← 2 · R
    if n_i == 1 then
        R ← R + P
    end if
end for
return Q
```

(a) Double-And-Add Algorithm

Algorithm 2 Double-And-Add-Always Algorithm

Input: point P, n $\in \mathbb{N}$, k = number of bits in n
Output: n $\cdot$ P

```
R_0 ← ∞
for i in range (k − 1, 0, −1) do
    R_0 ← 2 · R_0
    R_1 ← R_0 + P
    R_0 ← R_{k_i}
end for
return Q_0
```

(b) Double-And-Add-Always Algorithm

- Brute-Force attack
- Side-Channel attack – SPA & DPA. SPA example: Double-And-Add issue

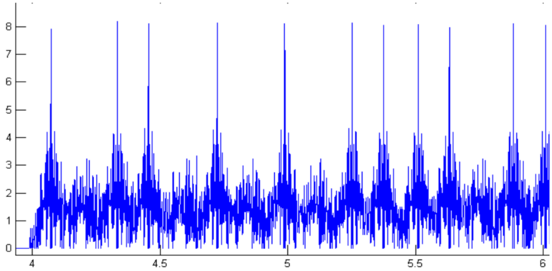

Figure: Power consumption[3]

- Zero-Value attack

[3] Image taken from https://cosade.telecom-paristech.fr/presentations/s2_p2.pdf

Conclusion

- Deep mathematical background needed to fully understand
- For actual implementations, mathematics are not needed as much
- Lack of direct curve comparisons

Discussion