Bundesamt für Sicherheit in der Informationstechnik

ROHDE&SCHWARZ

secunet

Requirements for Elliptic Curves for High-Assurance Applications

Manfred Lochter, **Johannes Merkle**,
Jörn-Marc Schmidt, Torsten Schütze

Background

- NIST curves widely deployed
  - » Public debate on trustworthiness
  - » However: No security issues known
- In Germany, deployment of Brainpool curves
  - » E.g. passports, ID cards, smart meter
- Recent efforts in IETF / CFRG for standardization of new curves
  - » Triggered by TLS working group
  - » Strong focus on software and performance
  - » Montgomery and Edwards curves selected

Bundesamt für Sicherheit in der Informationstechnik
ROHDE&SCHWARZ secunet

ECC Application Scenarios

1. Protected environment
   - » E.g. Certification Authorities
   - » Side-channels hardly exploitable

2. Network environment
   - » E.g. Web server
   - » Timing attacks, cache attacks

3. Potentially Hostile Environments
   - » E.g. Smart cards, embedded devices
   - » All kind of implementation attacks (power analysis, fault injection, EM)

Bundesamt für Sicherheit in der Informationstechnik
ROHDE&SCHWARZ
secunet

Our Focus

- High Assurance and hardware applications
  - » Scenario 3
  - » Resistant to various side-channel attacks
  - » Typically hardware or embedded crypto
  - » Often certifications required, e.g. FIPS 140 or Common Criteria
- Importance increases
  - » IoT, ID cards, smart meter, sensor networks, Car2X communication
- Transition to hardware crypto even advisable for scenario 2
  - » Heartbleed, etc.

Finite Field Primes

- Special primes (with sparse binary rep.)
  - » High speed software implementations possible
- High assurance (hardware) implementations
  - » Higher implementation costs
  - » Longer development cycles
- Typically, general modular multiplier
  - » Usable for all curves and RSA
  - » No advantages for special primes

Finite Field Primes

- Countermeasures against SCA, esp. DPA/DEMA
  - Popular: scalar blinding (Coron)

- For general primes, at least 64 bit blinding factor recommended
- For special primes, blinding less efficient
  - Long runs of zeros / ones in group order
  - Minimum length: approx. n/2 bits (Schindler-Wiemers 2015)

- For high-assurance ECC, we prefer verifiably pseudo-random primes as in Brainpool curves

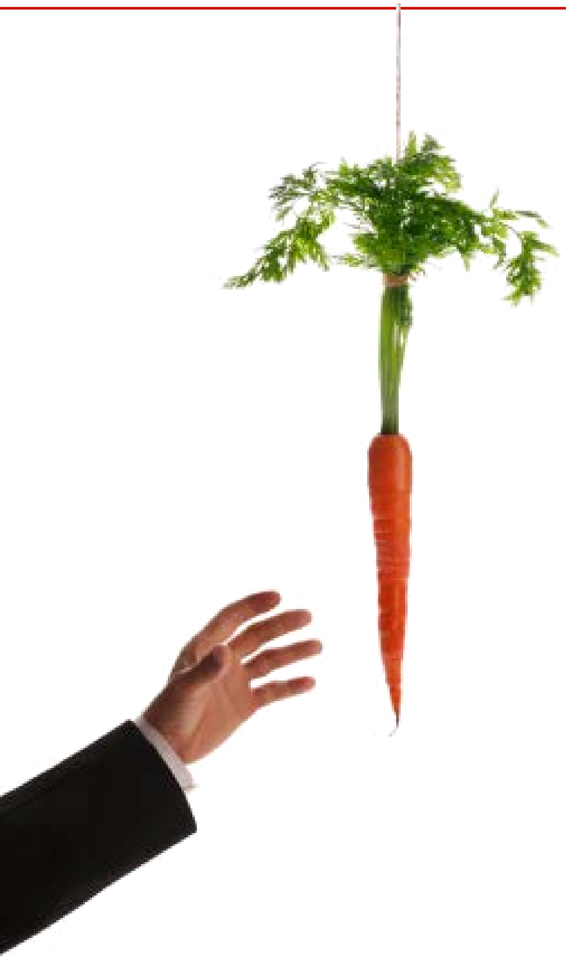
Cofactor

- Most standard curves have cofactor 1
  - » High assurance implementations exist

- Montgomery/Edwards curves have cofactor ≥ 4
  - » Advantages in software
    - » Simple, time-constant, efficient arithmetic
  - » Unclear, if these advantages also apply to high-assurance ECC
  - » (X,Z)-Brier-Joye ladder for general curves is commonly used in SCs

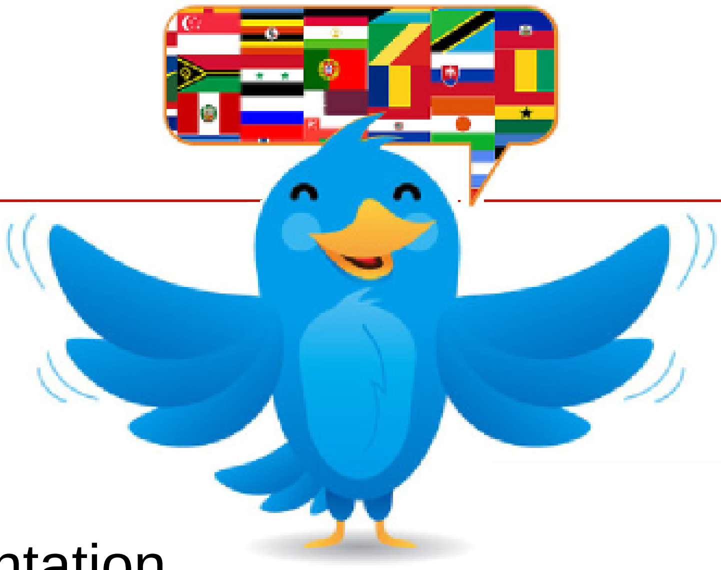
- For high-assurance ECC, cofactor = 1 is preferable
  - » Minimize attack surface
  - » Re-use existing hardware implementations

Rigid Selection of Curve Parameters



- Transparent process without wiggle room
- Two approaches:
  1. Verifiably pseudo-random generation
  2. Choose curves with (some) minimal property
- Both allow very limited flexibility
- However: Agree on curve properties first

Interoperability



- Short Weierstrass format is used by
  - » NIST, ANSI, ISO, IETF, W3C, ...
- Montgomery / (twisted) Edwards representation can be easily converted from/to short Weierstrass
- Affine or compressed affine Weierstrass points on wire (exchange format)
  - » Computations may be performed in arbitrary representations (projective, Jacobian, etc.)
- Backward-compatibility reduces implementation costs

Conclusions

- Do not only focus on software performance
- Different demands for:
  - » High speed in software
  - » High assurance
- Two sets of curves necessary
  - » Provide flexibility and agility
- Flexibility also needed in FIPS-140
  - » E.g. for verifying foreign passports with FIPS-approved hardware

Bundesamt für Sicherheit in der Informationstechnik
ROHDE&SCHWARZ secunet

Requirements for Elliptic Curves for High-Assurance Applications

Manfred Lochter, **Johannes Merkle**,
Jörn-Marc Schmidt, Torsten Schütze