Auxiliary elliptic curves for Maurer's algorithm for Russian standardized elliptic curves

Mariia Utekhina

CryptoPro LLC

CRYPTOPRO

2024 CTCRYPT

Relationship between CDH and DLP

Importance of CDH:

Many cryptosystems, like ElGamal encryption, require the hardness of the CDH assumption.

How well has CDH been studied?

Over the last 25 years:

- > 40 papers about solving DLP
- 0 papers about solving CDH

Maurer’s algorithm

Maurer’s algorithm: solves DLP via CDH algorithm.

Why is the relationship between CDH and DLP still an open question?

The stumbling block of Maurer’s reduction: an auxiliary elliptic curve is needed.

Group G, in which we want to solve DLP, of order q.  We need an auxiliary curve $\hat{E}(F_q)$.

Maurer's algorithm

- Let $\hat{E}(F_q)$ be of order $\hat{q} = \prod_{i=1}^{n} p_i^{e_i}$

- Complexity of Maurer's algorithm:

$$\sum_{i=1}^{n} \left\lfloor \frac{p_i^{e_i}}{2} + 1 \right\rfloor \cdot \left(\log p + \log \left(\frac{p_i^{e_i}}{2} \right) + 1 \right) + 14 \log q + 6 + \log \left(\frac{\hat{q}}{\min_i p_i^{e_i}} \right) (2 \log q + 16) + 7(n-1) \log \hat{q}$$

memory size — operations

- CDH calls:

$$11 \log \left(\frac{\hat{q}}{\min_i p_i^{e_i}} \right) + 14(n-1) \log \hat{q}$$

CRYPTOPRO

Previous results

❗ We need curves with smooth order: all $p_i^{e_i} < 2^B$

"Dlog is Practically as Hard (or Easy) as DH –Solving Dlogs via DH Oracles on EC Standards"
- Alexander May and Carl Richard Theodor Schneider, 2023

Curve from Example 1 in GOST R 34.10–2012

Base curve $E(\mathbb{F}_p)$	q [bit]	Samples	B [bit]
Anomalous	204	71311	33
ANSSIFRP256v1	256	156841	39
BLS12-381	255	3829640	36
BN(2,254)	254	7060	39
brainpoolP256t1	256	498440	39
Curve25519	253	104806	37
$F_p - 256$ (GM/T 0003.2-2012)	256	514595	39
GOST R 34.10	256	113350	37
M-221	219	229513	37
NIST P-224	224	76980	38
NIST P-256	256	437088	37
secp256k1	256	991302	37
SM2	256	840273	39

Table 1. B-smoothness achieved for the constructed auxiliary curves.

Results for Russian curves

We are considering Russian standardized curves from:

- [1] R 50.1.11420 “Elliptic Curve Parameters for Cryptographic Algorithms and Protocols”
- [2] “Scheme of formation and verification of verification code”

Short (170 bit) curve from [2]	2^{25} smoothness	429 MB
Curve id-tc26-gost-3410-2012-256-paramSetA	2^{35} smoothness	0,72 TB
Curve id-tc26-gost-3410-2012-256-paramSetB	2^{40} smoothness	18,8 TB
Curve id-tc26-gost-3410-2012-256-paramSetC	2^{36} smoothness	1,62 TB
Curve id-tc26-gost-3410-2012-256-paramSetD	2^{39} smoothness	7,84 TB

Calculations are in progress...

Thank you for your attention!

utekhina@cryptopro.ru

CRYPTOPRO