Common Points on Elliptic Curves:

The Achilles' Heel of Fault Attack Countermeasures

Alberto Battistello

April 12, 2014

oberthur TECHNOLOGIES THE M COMPANY

Overview

1. Introduction
2. A Simple Fault Attack
3. Our New Attack
4. Conclusion

oberthur TECHNOLOGIES THE M COMPANY

Overview

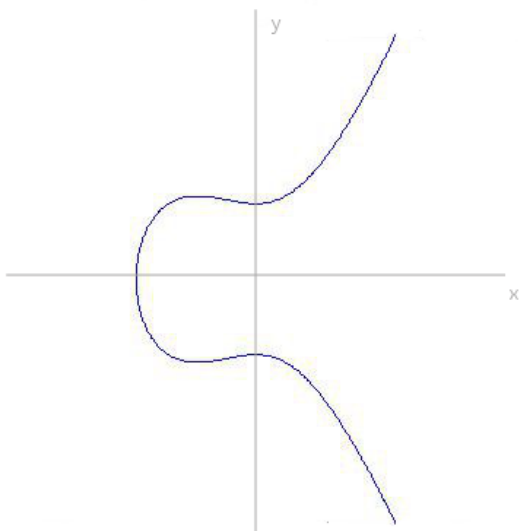
oberthur TECHNOLOGIES THE M COMPANY

Short Weierstrass Equation

Curve Equation

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + \mathbf{a} \cdot x + \mathbf{b} \bmod p$$

$$P = (x_p, y_p)$$



oberthur TECHNOLOGIES THE M COMPANY

Short Weierstrass Equation

Curve Equation

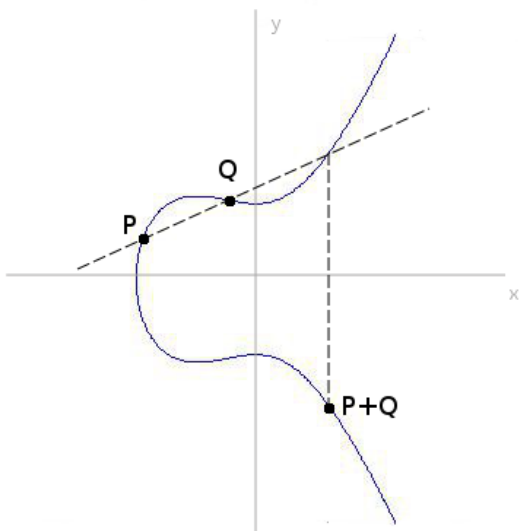
$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + \mathbf{a} \cdot x + \mathbf{b} \bmod p$$

$P = (x_p, y_p)$

Addition/Doubling

- $P + Q = f_A(P, Q, \mathcal{E})$
- $P + P = f_D(P, \mathcal{E})$

b is never used.



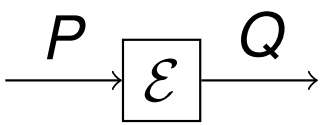
oberthur TECHNOLOGIES THE M COMPANY

Scalar Multiplication

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

Scalar Multiplication

$$[d]P = \underbrace{P + P + P + P}_{\text{d times}} = Q$$



oberthur TECHNOLOGIES THE M COMPANY

ECDLP

ECDLP

Given $P, Q \in \mathcal{E}(\mathbb{F}_p)$ find d such that $Q = [d]P$.
The ECDLP complexity depends on the order of P over $\mathcal{E}(\mathbb{F}_p)$.

Order of Point

$Ord_{\mathcal{E}}(P) = \prod q_i^{\alpha_i}$.

max $q_i \leq$ 112-bit $\Rightarrow$ ρ-Pollard.

The same point on another curve may have a weaker order.

oberthur TECHNOLOGIES THE M COMPANY

Overview

oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

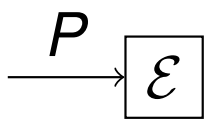
$\boxed{\mathcal{E}}$

oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$

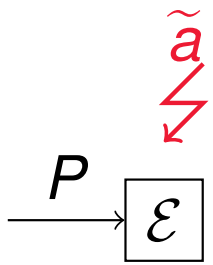


oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a

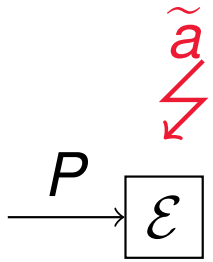


oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. $\widetilde{b} = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$

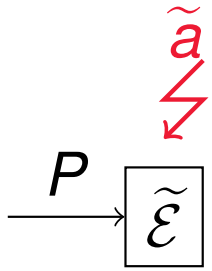


oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + \widetilde{b} \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. $\widetilde{b} = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$

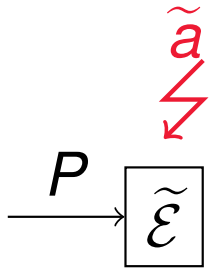


oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + \widetilde{b} \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. $\widetilde{b} = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
4. $Ord_{\widetilde{\mathcal{E}}}(P) \neq Ord_{\mathcal{E}}(P)$

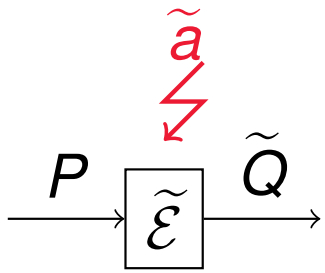


oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + \widetilde{b} \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. $\widetilde{b} = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
4. $Ord_{\widetilde{\mathcal{E}}}(P) \neq Ord_{\mathcal{E}}(P)$
5. $\widetilde{Q} = [d]P$

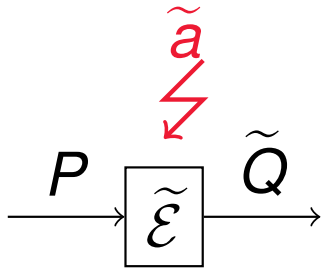


oberthur TECHNOLOGIES THE M COMPANY

A Simple Fault Attack

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + \widetilde{b} \bmod p$$

1. Input $P = (x_p, y_p) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. $\widetilde{b} = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
4. $Ord_{\widetilde{\mathcal{E}}}(P) \neq Ord_{\mathcal{E}}(P)$
5. $\widetilde{Q} = [d]P$
6. $\widetilde{Q} \Rightarrow d$



oberthur TECHNOLOGIES THE M COMPANY

Two simple countermeasures

Parameters checksums

Checksum of all parameters $(a, b, p, x_p, y_p, \ldots)$ checked before output.

$CRC(\widetilde{a}) \neq CRC(a)$

oberthur TECHNOLOGIES THE M COMPANY

Two simple countermeasures

Parameters checksums

Checksum of all parameters $(a, b, p, x_p, y_p, \ldots)$ checked before output.

$CRC(\widetilde{a}) \neq CRC(a)$

Point on curve test

- Initial test $y_p^2 = x_p^3 + a \cdot x_p + b \bmod p$
- Final test $y_q^2 = x_q^3 + a \cdot x_q + b \bmod p$

$y_q^2 \neq x_q^3 + \widetilde{a} \cdot x_q + b \bmod p$

oberthur TECHNOLOGIES THE M COMPANY

Question

The two tests have been considered equivalent . . .

up to NOW

oberthur TECHNOLOGIES THE M COMPANY

Overview

1 Introduction

2 A Simple Fault Attack

3 Our New Attack

4 Conclusion

oberthur TECHNOLOGIES THE M COMPANY

Common Points

$$y^2 = x^3 + a \cdot x + b \bmod p$$

oberthur TECHNOLOGIES THE M COMPANY

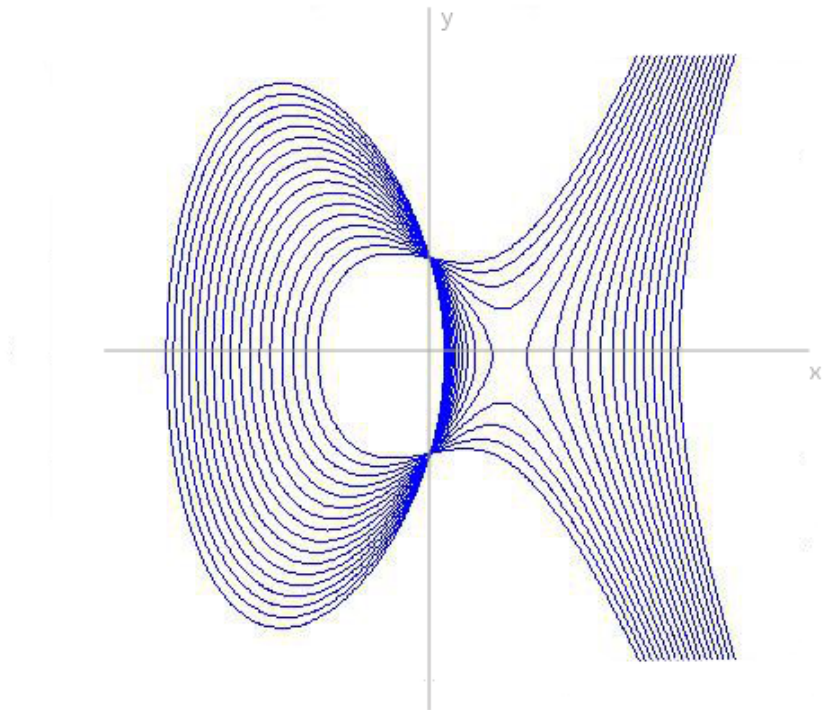
Common Points

$$y^2 = x^3 + a \cdot x + b \bmod p$$

oberthur TECHNOLOGIES THE M COMPANY

Common Points

$$y^2 = x^3 + a \cdot x + b \bmod p$$



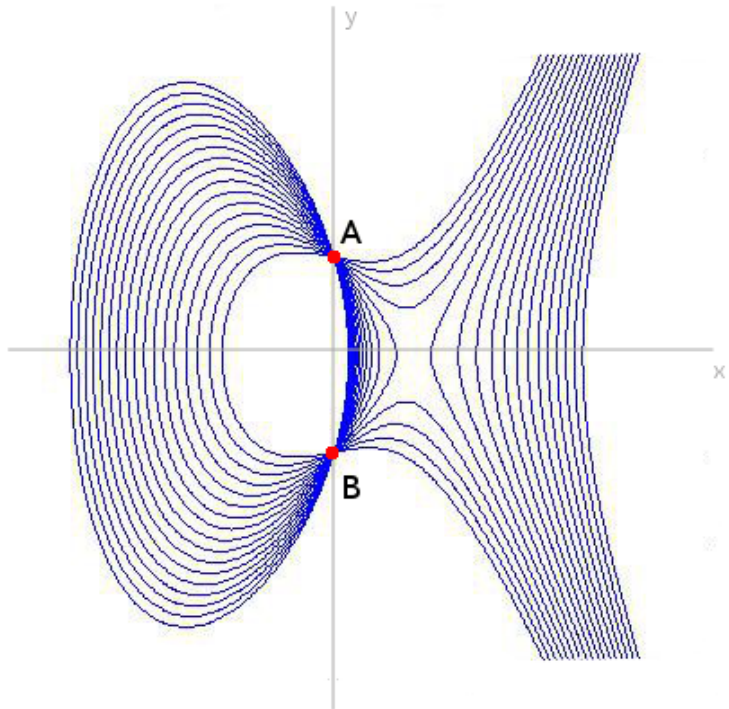
oberthur TECHNOLOGIES THE M COMPANY

Common Points

$$y^2 = x^3 + a \cdot x + b \bmod p$$

Common Points:

$$A, B : (0, \pm\sqrt{b})$$



oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

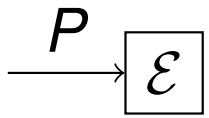
$\boxed{\mathcal{E}}$

oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$

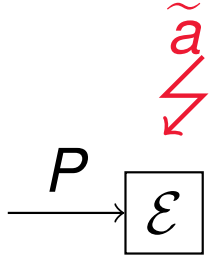


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a

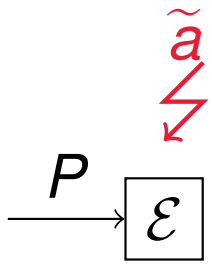


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$

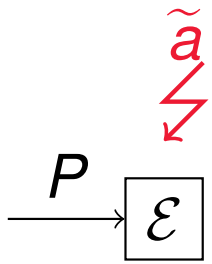


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓

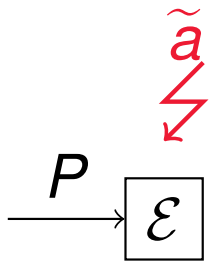


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\mathcal{E}(\mathbb{F}_p) : y^2 = x^3 + a \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓
4. $b = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$

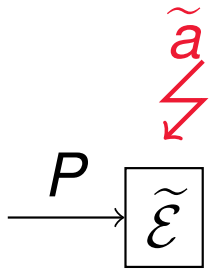


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓
4. $b = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$

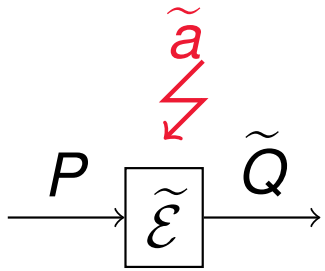


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓
4. $b = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
5. Test: $y_q^2 = x_q^3 + \widetilde{a} \cdot x_q + b \bmod p$

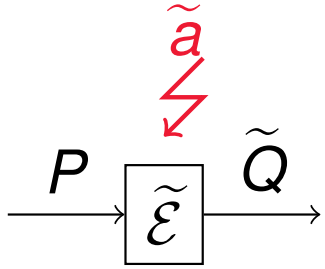


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓
4. $b = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
5. Test: $y_q^2 = x_q^3 + \widetilde{a} \cdot x_q + b \bmod p$ ✓

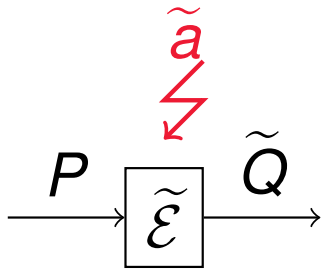


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + b \bmod p$$

1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓
4. $b = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
5. Test: $y_q^2 = x_q^3 + \widetilde{a} \cdot x_q + b \bmod p$ ✓
6. $Ord_{\widetilde{\mathcal{E}}}(P) \neq Ord_{\mathcal{E}}(P)$

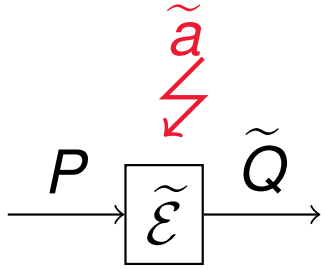


oberthur TECHNOLOGIES THE M COMPANY

Attack PoC tests

$$\widetilde{\mathcal{E}}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{a} \cdot x + b \bmod p$$

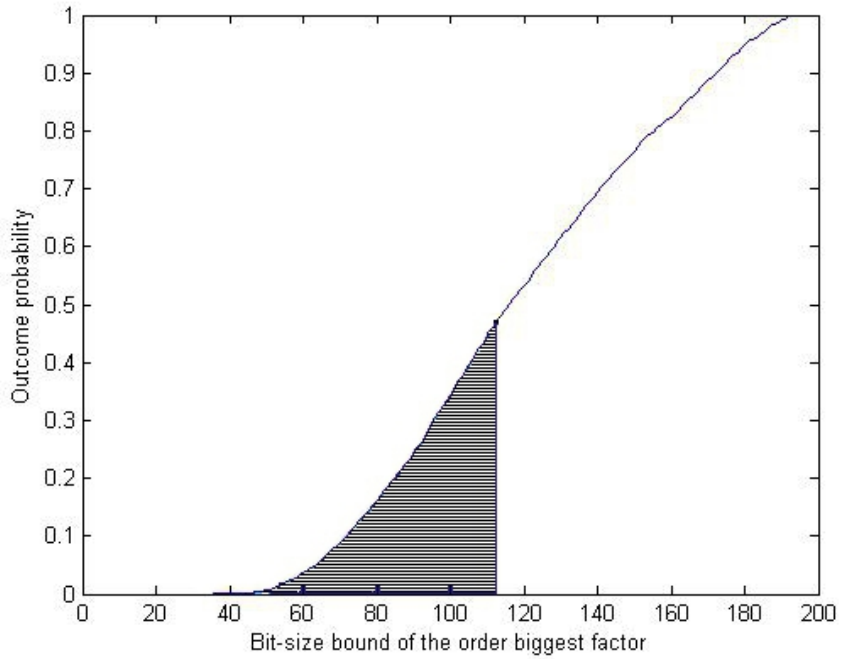
1. Send input point $P = (0, \sqrt{b}) \in \mathcal{E}(\mathbb{F}_p)$
2. $\widetilde{a} \leftarrow$ Fault a
3. Test: $y_p^2 = x_p^3 + \widetilde{a} \cdot x_p + b \bmod p$ ✓
4. $b = y_p^2 - x_p^3 - \widetilde{a} \cdot x_p \bmod p$
5. Test: $y_q^2 = x_q^3 + \widetilde{a} \cdot x_q + b \bmod p$ ✓
6. $Ord_{\widetilde{\mathcal{E}}}(P) \neq Ord_{\mathcal{E}}(P)$
7. $\widetilde{Q} = [d]P \Leftarrow$ **ECDL**



oberthur TECHNOLOGIES THE M COMPANY

Simulations

Faults producing a weak curve.



Probability that the biggest factor is smaller than ECDLP record of 112 bit is more than 45%.

oberthur TECHNOLOGIES THE M COMPANY

Overview

oberthur TECHNOLOGIES THE M COMPANY

Conclusion

Common Points

Common Points have never been remarked before.

PoC vs Checksums

The two countermeasures are NOT equivalent!

Curves

Parameter *b* must be a square.

- NIST: P-192, P-256, P-384.
- Secp: 192r1, 256r1, 384r1, 521r1.

oberthur TECHNOLOGIES THE M COMPANY

Questions?

Thank you

Feel free to ask any question