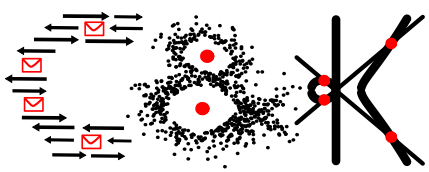
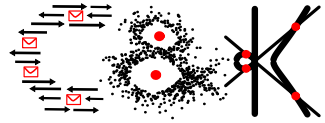
Tampering attacks in pairing-based cryptography

Johannes Blömer
University of Paderborn
September 22, 2014



UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Pairings



Definition 1

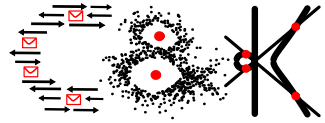
A pairing is a bilinear, non-degenerate, and efficiently computable map $e : \mathbb{G} \times \mathbb{G}' \to \mathbb{G}_T$, *where* $\mathbb{G}, \mathbb{G}', \mathbb{G}_T$ *are finite groups of the same size. Bilinearity:*

$$e(P + Q, R) = e(P, R) \cdot e(Q, R) \quad \text{for all } P, Q \in \mathbb{G}, R \in \mathbb{G}'$$
$$e(P, R + Q) = e(P, R) \cdot e(P, Q) \quad \text{for all } P \in \mathbb{G}, Q, R \in \mathbb{G}'.$$

Non-degeneracy: for all $P \in \mathbb{G} \setminus \{\mathcal{O}\}$ *there is a* $Q \in \mathbb{G}'$ *such that* $e(P, Q) \neq 1$.

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Pairings



Definition 1

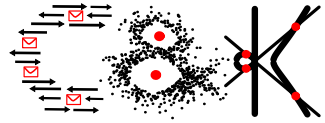
A pairing is a bilinear, non-degenerate, and efficiently computable map $e : \mathbb{G} \times \mathbb{G}' \to \mathbb{G}_T$, *where* $\mathbb{G}, \mathbb{G}', \mathbb{G}_T$ *are finite groups of the same size. Bilinearity:*

$$e(P + Q, R) = e(P, R) \cdot e(Q, R) \quad \text{for all } P, Q \in \mathbb{G}, R \in \mathbb{G}'$$
$$e(P, R + Q) = e(P, R) \cdot e(P, Q) \quad \text{for all } P \in \mathbb{G}, Q, R \in \mathbb{G}'.$$

Non-degeneracy: for all $P \in \mathbb{G} \setminus \{\mathcal{O}\}$ *there is a* $Q \in \mathbb{G}'$ *such that* $e(P, Q) \neq 1$.

- plus crypto assumptions

Pairings



Definition 1

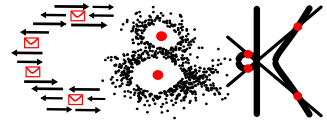
A pairing is a bilinear, non-degenerate, and efficiently computable map $e : \mathbb{G} \times \mathbb{G}' \to \mathbb{G}_T$, *where* $\mathbb{G}, \mathbb{G}', \mathbb{G}_T$ *are finite groups of the same size. Bilinearity:*

$$e(P + Q, R) = e(P, R) \cdot e(Q, R) \quad \text{for all } P, Q \in \mathbb{G}, R \in \mathbb{G}'$$
$$e(P, R + Q) = e(P, R) \cdot e(P, Q) \quad \text{for all } P \in \mathbb{G}, Q, R \in \mathbb{G}'.$$

Non-degeneracy: for all $P \in \mathbb{G} \setminus \{\mathcal{O}\}$ *there is a* $Q \in \mathbb{G}'$ *such that* $e(P, Q) \neq 1$.

- plus crypto assumptions
- $e(a \cdot P, b \cdot Q) = e(b \cdot P, a \cdot Q) = e(ab \cdot P, Q) = e(P, Q)^{ab}$
- can be used to combine and recombine shares of secrets or secrets and nonces

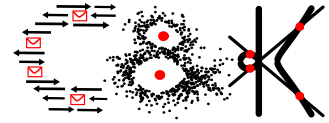
Pairings



Applications

- identity-based encryption
- attribute-based encryption
- group signatures
- key agreement
- anonymous credentials
- ...

Pairings



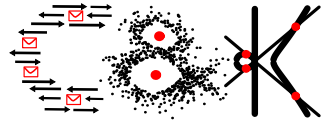
Applications

- identity-based encryption
- attribute-based encryption
- group signatures
- key agreement
- anonymous credentials
- ...

Attribute-based encryption

- encrypt data under attributes, not for individual users,
- users get rights,
- if rights and attributes match, data can be decrypted

Pairings

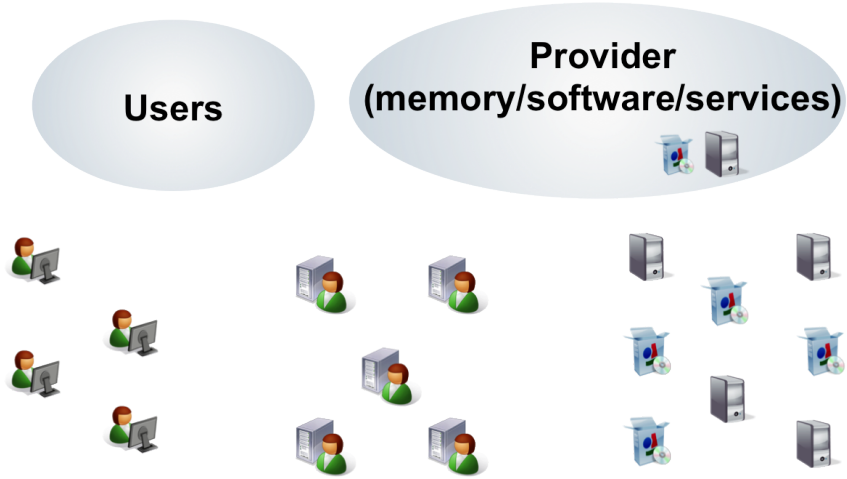


Applications

- identity-based encryption
- attribute-based encryption
- group signatures
- key agreement
- anonymous credentials
- ...

Attribute-based encryption

- encrypt data under attributes, not for individual users,
- users get rights,
- if rights and attributes match, data can be decrypted



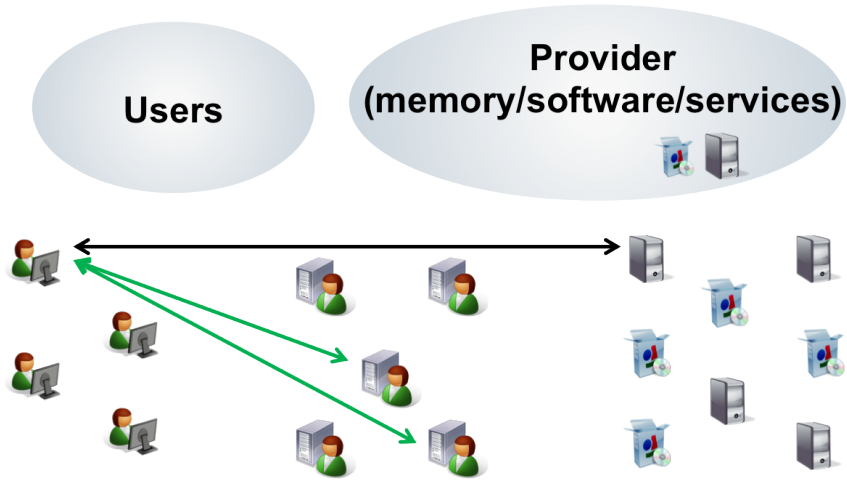
Pairings

Applications

- identity-based encryption
- attribute-based encryption
- group signatures
- key agreement
- anonymous credentials
- ...

Attribute-based encryption

- encrypt data under attributes, not for individual users,
- users get rights,
- if rights and attributes match, data can be decrypted



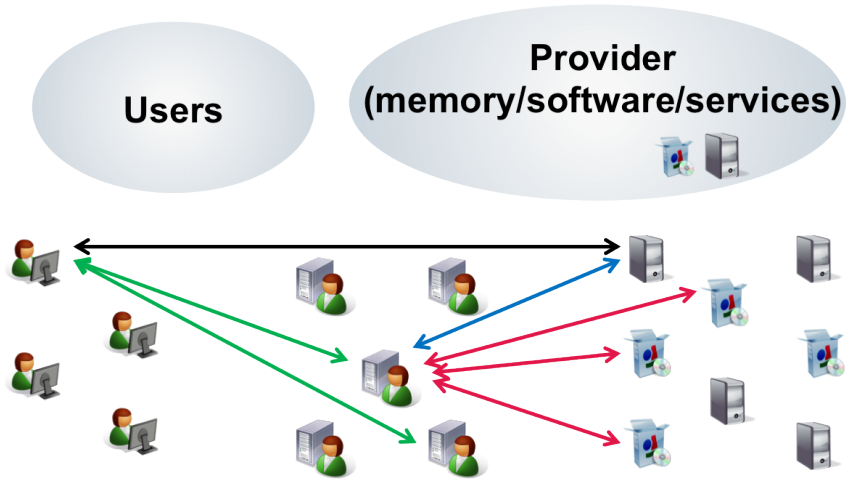
Pairings

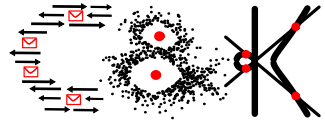
Applications

- identity-based encryption
- attribute-based encryption
- group signatures
- key agreement
- anonymous credentials
- ...

Attribute-based encryption

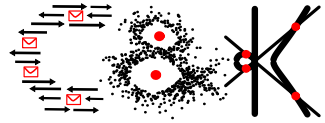
- encrypt data under attributes, not for individual users,
- users get rights,
- if rights and attributes match, data can be decrypted





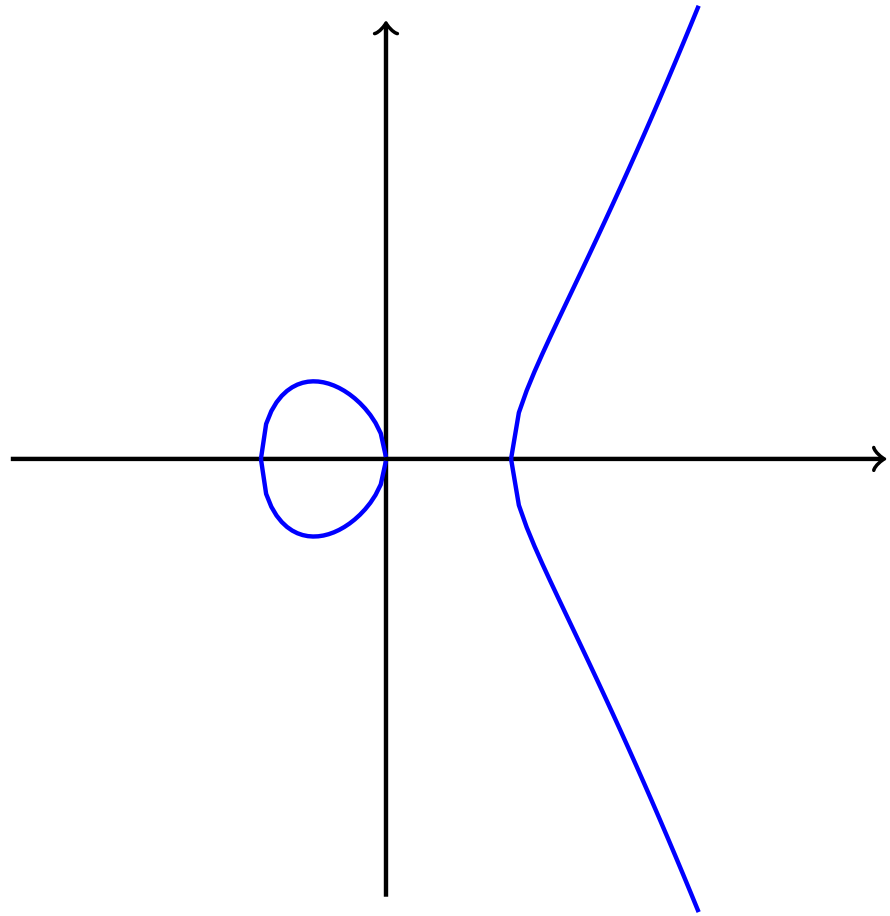
Elliptic curves

- $\mathbb{F}$ a field (finite or infinite), $\bar{\mathbb{F}}$ algebraic closure
- $a, b \in \mathbb{F}$
- $E := \{(x, y) \in \bar{\mathbb{F}}^2 : y^2 = x^3 + ax + b = 0\} \cup \{\mathcal{O}\}$ elliptic curve over $\mathbb{F}$
- $\mathcal{O}$ point at infinity
- elliptic curves have group structure using chord and tangent law

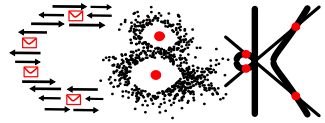


Elliptic curves

- $\mathbb{F}$ a field (finite or infinite), $\bar{\mathbb{F}}$ algebraic closure
- $a, b \in \mathbb{F}$
- $E := \{(x, y) \in \bar{\mathbb{F}}^2 : y^2 = x^3 + ax + b = 0\} \cup \{\mathcal{O}\}$ elliptic curve over $\mathbb{F}$
- $\mathcal{O}$ point at infinity
- elliptic curves have group structure using chord and tangent law

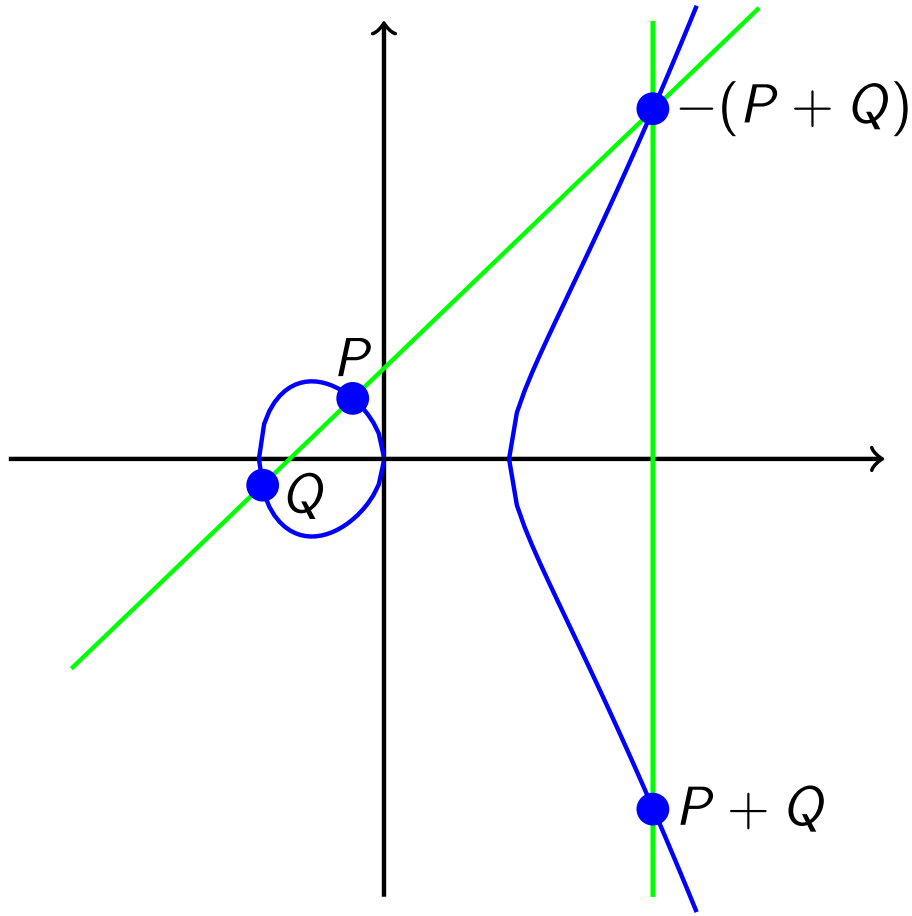


Elliptic curves



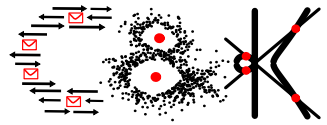
Elliptic curves

- $\mathbb{F}$ a field (finite or infinite), $\bar{\mathbb{F}}$ algebraic closure
- $a, b \in \mathbb{F}$
- $E := \{(x, y) \in \bar{\mathbb{F}}^2 : y^2 = x^3 + ax + b = 0\} \cup \{\mathcal{O}\}$ elliptic curve over $\mathbb{F}$
- $\mathcal{O}$ point at infinity
- elliptic curves have group structure using chord and tangent law



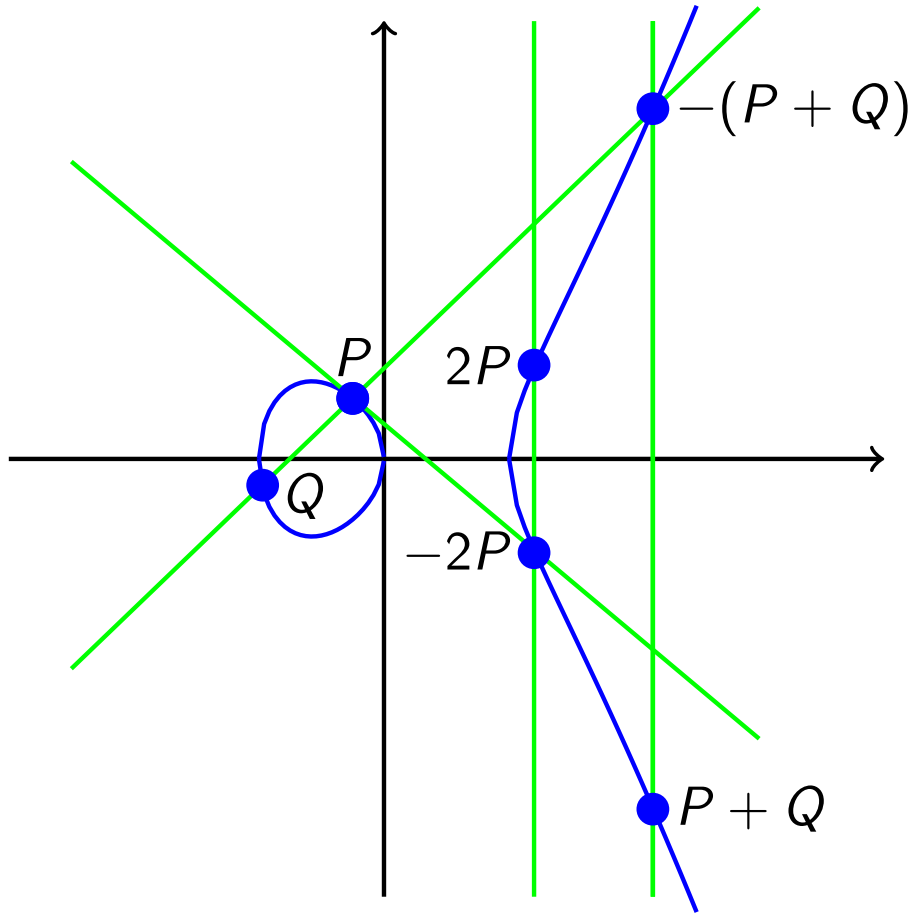
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Elliptic curves



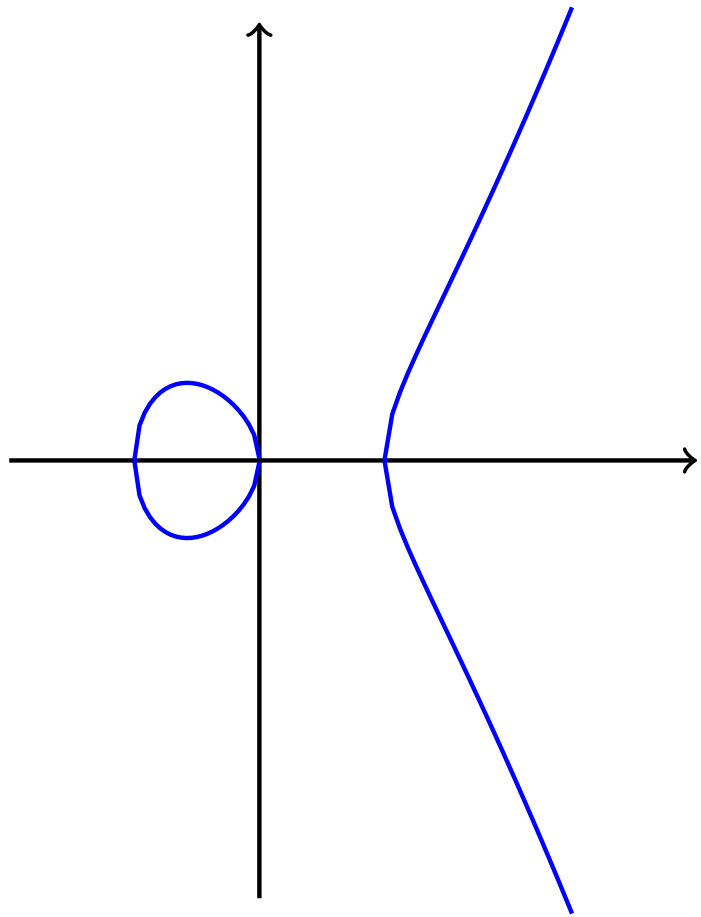
Elliptic curves

- $\mathbb{F}$ a field (finite or infinite), $\bar{\mathbb{F}}$ algebraic closure
- $a, b \in \mathbb{F}$
- $E := \{(x, y) \in \bar{\mathbb{F}}^2 : y^2 = x^3 + ax + b = 0\} \cup \{\mathcal{O}\}$ elliptic curve over $\mathbb{F}$
- $\mathcal{O}$ point at infinity
- elliptic curves have group structure using chord and tangent law

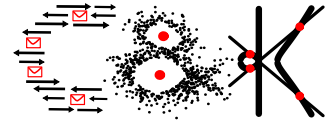


UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Torsion points and embedding degree

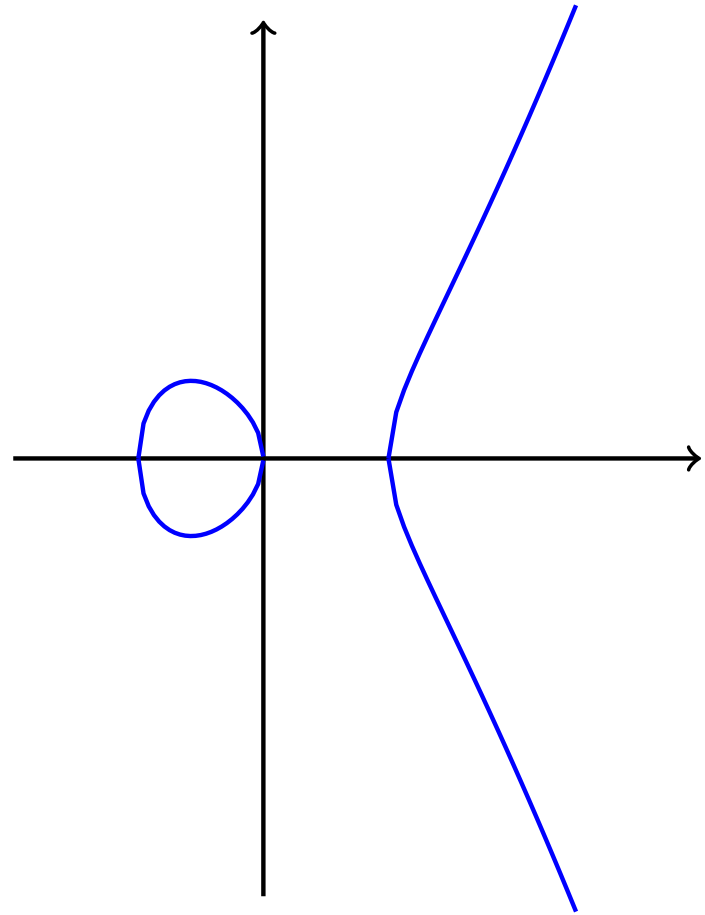


Torsion points and embedding degree



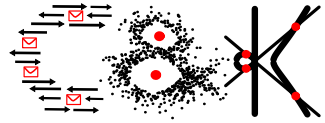
Torsion points on elliptic curves

- E elliptic curve, $P \in E, r \in \mathbb{N}$
- P torsion point of order r, iff $r \cdot P = \mathcal{O}$
- $E[r] :=$ set of points of order r
- $E[r]$ is subgroup of E



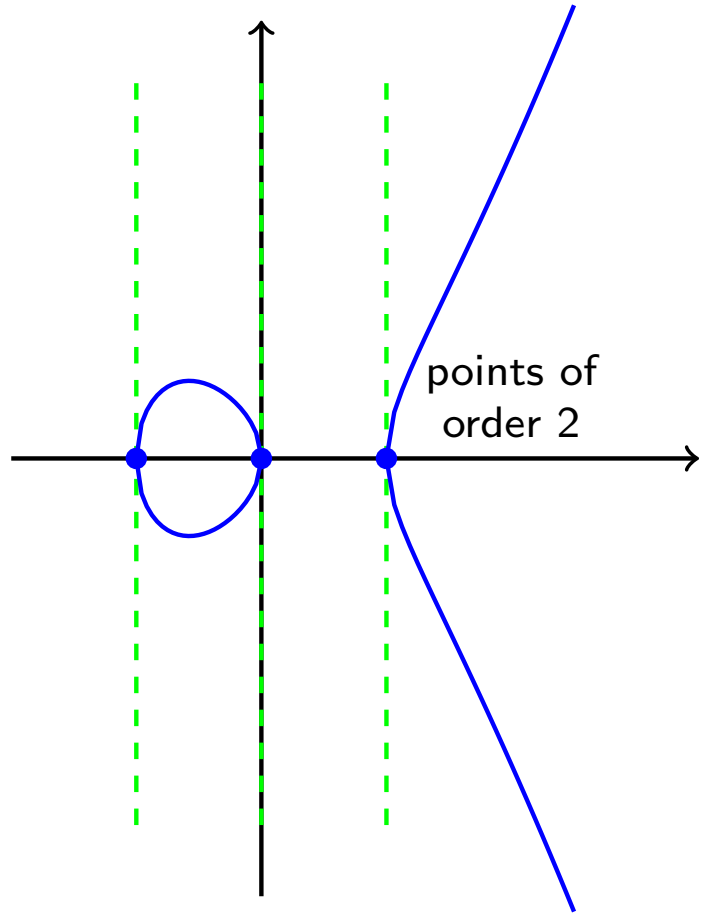
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Torsion points and embedding degree



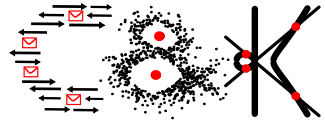
Torsion points on elliptic curves

- E elliptic curve, $P \in E, r \in \mathbb{N}$
- P torsion point of order r, iff $r \cdot P = \mathcal{O}$
- $E[r] :=$ set of points of order r
- $E[r]$ is subgroup of E



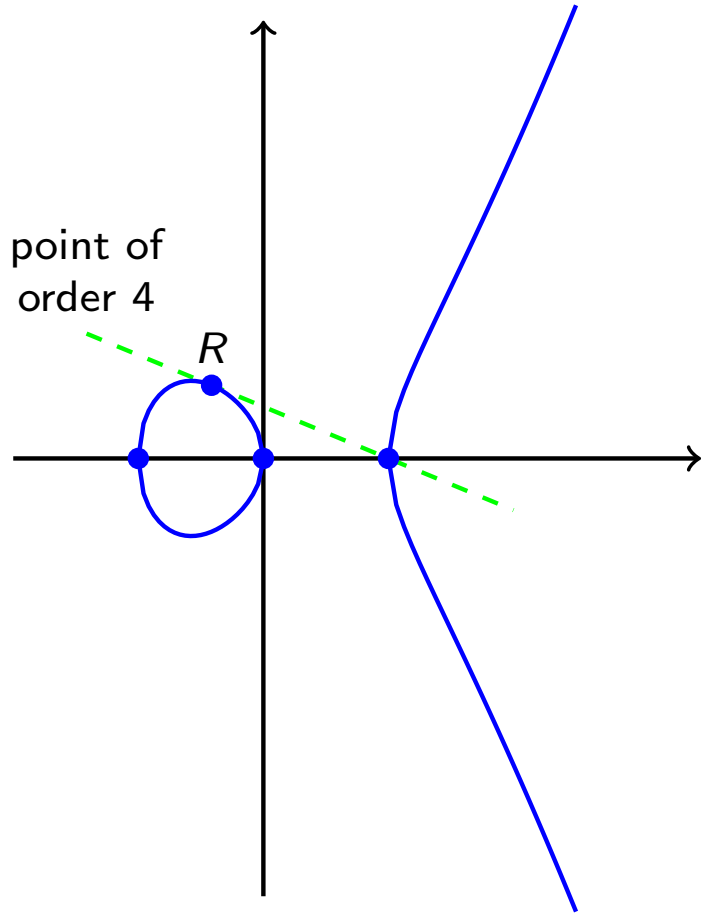
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Torsion points and embedding degree



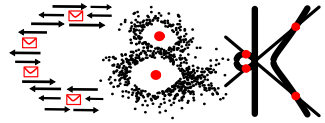
Torsion points on elliptic curves

- E elliptic curve, $P \in E, r \in \mathbb{N}$
- P torsion point of order r, iff $r \cdot P = \mathcal{O}$
- $E[r] :=$ set of points of order r
- $E[r]$ is subgroup of E



UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Torsion points and embedding degree

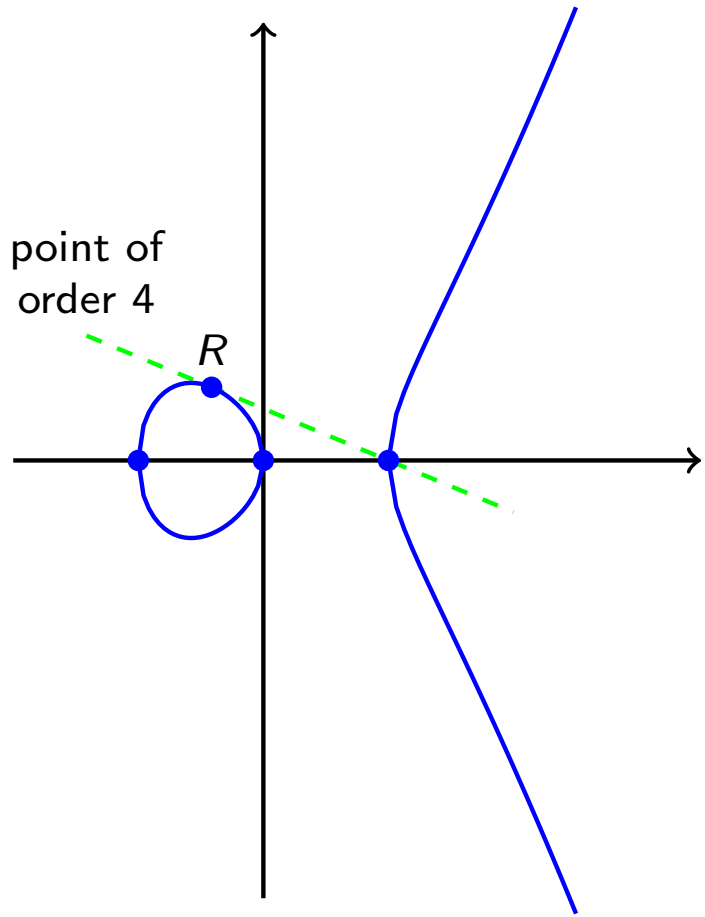


Torsion points on elliptic curves

- E elliptic curve, $P \in E, r \in \mathbb{N}$
- P torsion point of order r, iff $r \cdot P = \mathcal{O}$
- $E[r] :=$ set of points of order r
- $E[r]$ is subgroup of E

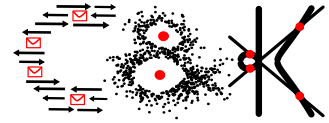
Embedding degree

- $\mathbb{F} = \mathbb{F}_q$ finite field, $r \in \mathbb{N}$
- smallest k s.th. $r \mid (q^k - 1)$ called embedding degree
- $E[r] \subset E(\mathbb{F}_{q^k}) := E \cap (\mathbb{F}_{q^k} \times \mathbb{F}_{q^k})$



UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Miller's algorithm



Miller Algorithm (MA)

---

input : $r \in \mathbb{N}, P, Q \in E, Q \neq P, \mathcal{O}, r = \sum_{j=0}^{t} r_j 2^j, r_j \in \{0,1\}$

$T \leftarrow P$;

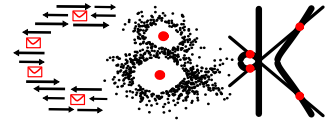
for $j = t-2 \ldots 0$ **do**

  $T \leftarrow 2T$;

  if $r_j = 1$ **then**

    $T \leftarrow T + P$;

Miller's algorithm



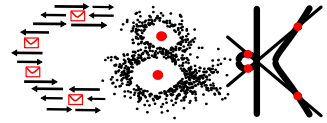
Miller Algorithm (MA)

input : $r \in \mathbb{N}, P, Q \in E, Q \neq P, \mathcal{O}, r = \sum_{j=0}^{t} r_j 2^j, r_j \in \{0,1\}$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1;$
for $j = t-2 \ldots 0$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q);$
  $T \leftarrow 2T;$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q);$
    $T \leftarrow T + P;$
return $f;$

$l_{U,V}$:= equation of line through U, V

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

The Weil pairing



$\mu_r := \{u \in \mathbb{F}_{q^k} : u^r = 1\}$ (set of r-th roots of unity)

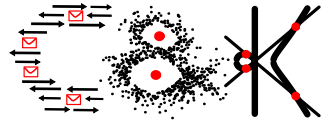
Definition 2 (Weil/Miller)

The Weil pairing w_r is the map defined by

$$w_r : E[r] \times E[r] \to \mu_r$$

$$(P, Q) \mapsto (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}.$$

The Weil pairing



$\mu_r := \{u \in \mathbb{F}_{q^k} : u^r = 1\}$ (set of r-th roots of unity)

Definition 2 (Weil/Miller)

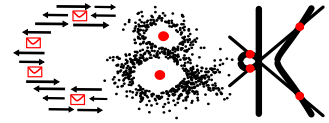
The Weil pairing w_r is the map defined by

$$w_r : E[r] \times E[r] \to \mu_r$$

$$(P, Q) \mapsto (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}.$$

- w_r is bilinear and non-degenerate,
- but rather inefficient, two invocations of MA

The reduced Tate pairing

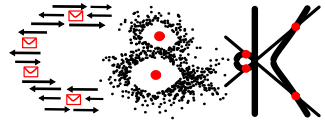


Definition 3

The reduced Tate pairing t_r is the map defined by

$$t_r : E[r] \times E\left(\mathbb{F}_{q^k}\right) / rE\left(\mathbb{F}_{q^k}\right) \to \mu_r$$
$$(P, Q) \mapsto f_{r,P}(Q)^{\left(q^k-1\right)/r}.$$

The reduced Tate pairing



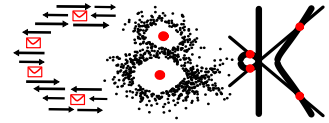
Definition 3

The reduced Tate pairing t_r is the map defined by

$$t_r : E[r] \times E\left(\mathbb{F}_{q^k}\right) / rE\left(\mathbb{F}_{q^k}\right) \to \mu_r$$
$$(P, Q) \mapsto f_{r,P}(Q)^{\left(q^k-1\right)/r}.$$

- t_r requires one MA invocation and one exponentiation, the *final exponentiation (FE)*
- more efficient to compute than w_r
- variants of t_r lead to pairings currently proposed for applications
- most variants have the structure MA + FE

Fault attacks on pairings

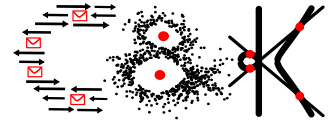


- most applications don't just compute a pairing - never mind

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1;$
for $j = t - 2 \ldots 0$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q);$
  $T \leftarrow 2T;$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q);$
    $T \leftarrow T + P;$
return $f^{(q^k-1)/r};$

Fault attacks on pairings

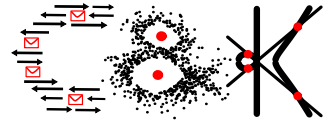


- most applications don't just compute a pairing - never mind
- secret is not the scalar r, rather it is P or Q

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1;$
for $j = t - 2 \ldots 0$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q);$
  $T \leftarrow 2T;$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q);$
    $T \leftarrow T + P;$
return $f^{(q^k-1)/r};$

Fault attacks on pairings

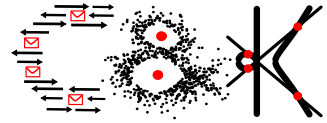


- most applications don't just compute a pairing - never mind
- secret is not the scalar r, rather it is P or Q
- both MA and FE individually are usually hard to invert

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1$;
for $j = t-2 \ldots 0$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
  $T \leftarrow 2T$;
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
    $T \leftarrow T + P$;
return $f^{(q^k-1)/r}$;

Fault attacks on pairings



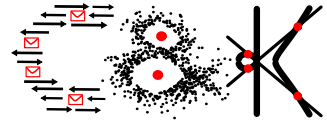
- most applications don't just compute a pairing - never mind
- secret is not the scalar r, rather it is P or Q
- both MA and FE individually are usually hard to invert
- FE many-to-one, need to find the "right" preimage

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1$;
for $j = t - 2 \ldots 0$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
  $T \leftarrow 2T$;
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
    $T \leftarrow T + P$;
return $f^{(q^k-1)/r}$;

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Fault attacks on pairings



- most applications don't just compute a pairing - never mind
- secret is not the scalar r, rather it is P or Q
- both MA and FE individually are usually hard to invert
- FE many-to-one, need to find the "right" preimage

MA + FE

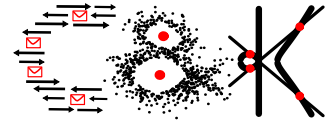
input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1$;
for $j = t-2 \ldots 0$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
  $T \leftarrow 2T$;
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
    $T \leftarrow T + P$;
return $f^{(q^k-1)/r}$;

$\Rightarrow$ game is different from standard elliptic curve cryptography (ECC)

- for practical evaluation see Marie's talk.

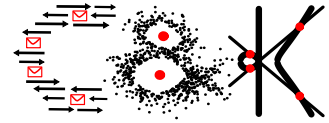
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Attacking a pairing - how to deal with FE



1. Ignore the problem.
2. Show that you can use correlated faults to induce faults in Miller's algorithm and skip the final exponentiation.
   $\rightarrow$ (see Peter's talk)
3. Assume that you can induce faults into Miller's algorithm and additional faults into the final exponentiation that facilitate the inversion problem for the exponentiation.
4. Use particular curves and pairings for which the inversion problem for the final exponentiation can be solved efficiently.

The strategies



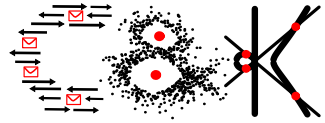
MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$

1 $T \leftarrow P, f \leftarrow 1$;
2 **for** $j = t - 2 \ldots 0$ **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
4 $\quad T \leftarrow 2T$;
5 $\quad$ **if** $r_j = 1$ **then**
6 $\quad\quad f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
7 $\quad\quad T \leftarrow T + P$;
8 **return** $f^{(q^k-1)/r}$;

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

The strategies



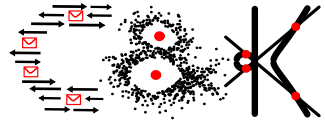
- attack operations in lines 3,4,6,7
  - lines 4 and 7 seem difficult

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$

1 $T \leftarrow P, f \leftarrow 1$;
2 **for** $j = t - 2 \ldots 0$ **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
4 $\quad T \leftarrow 2T$;
5 $\quad$ **if** $r_j = 1$ **then**
6 $\quad\quad f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
7 $\quad\quad T \leftarrow T + P$;
8 **return** $f^{(q^k-1)/r}$;

The strategies



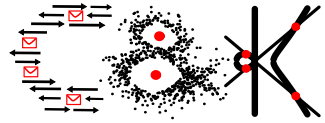
- attack operations in lines 3,4,6,7
  - lines 4 and 7 seem difficult
  - lines 3,6: attack by Wheelan, Scott and others

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$

1 $T \leftarrow P, f \leftarrow 1$;
2 **for** $j = t - 2 \ldots 0$ **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
4 $\quad T \leftarrow 2T$;
5 $\quad$ **if** $r_j = 1$ **then**
6 $\quad\quad f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
7 $\quad\quad T \leftarrow T + P$;
8 **return** $f^{(q^k-1)/r}$;

The strategies



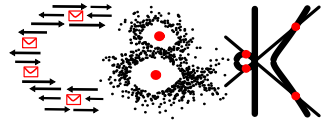
- attack operations in lines 3,4,6,7
  - lines 4 and 7 seem difficult
  - lines 3,6: attack by Wheelan, Scott and others
- attack loop in lines 2 - 7 (Page-Vercauteren)

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$

1 $T \leftarrow P, f \leftarrow 1$;
2 **for** $j = t - 2 \ldots 0$ **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
4 $\quad T \leftarrow 2T$;
5 $\quad$ **if** $r_j = 1$ **then**
6 $\quad\quad f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
7 $\quad\quad T \leftarrow T + P$;
8 **return** $f^{(q^k-1)/r}$;

The strategies



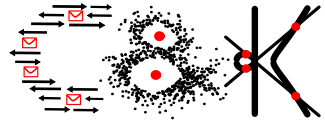
- attack operations in lines 3,4,6,7
  - lines 4 and 7 seem difficult
  - lines 3,6: attack by Wheelan, Scott and others
- attack loop in lines 2 - 7 (Page-Vercauteren)
  - leave the loop after completing a certain number of iterations

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$

1 $T \leftarrow P, f \leftarrow 1$;
2 **for** $j = t - 2 \ldots 0$ **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
4 $\quad T \leftarrow 2T$;
5 $\quad$ **if** $r_j = 1$ **then**
6 $\quad\quad f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
7 $\quad\quad T \leftarrow T + P$;
8 **return** $f^{(q^k-1)/r}$;

The strategies



- attack operations in lines 3,4,6,7
  - lines 4 and 7 seem difficult
  - lines 3,6: attack by Wheelan, Scott and others
- attack loop in lines 2 - 7 (Page-Vercauteren)
  - leave the loop after completing a certain number of iterations
  - leave the loop within an iteration and before executing the **if**-instruction in line 5

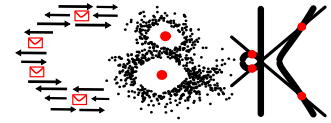
MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$

1 $T \leftarrow P, f \leftarrow 1$;
2 **for** $j = t-2 \ldots 0$ **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q)$;
4 $\quad T \leftarrow 2T$;
5 $\quad$ **if** $r_j = 1$ **then**
6 $\quad\quad f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q)$;
7 $\quad\quad T \leftarrow T + P$;
8 **return** $f^{(q^k-1)/r}$;

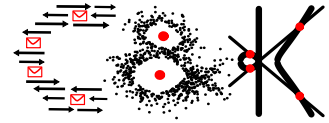
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Skipping iterations with two independent faults



- induce single fault in two independent runs of algorithm MA + FE

Skipping iterations with two independent faults

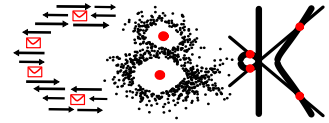


- induce single fault in two independent runs of algorithm MA + FE
- in first run leave **for**-loop after iteration s to obtain $f_s^{(q^k-1)/r}$

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1;$
for $j = t-2 \ldots s$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q);$
  $T \leftarrow 2T;$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q);$
    $T \leftarrow T + P;$
return $f^{(q^k-1)/r};$

Skipping iterations with two independent faults



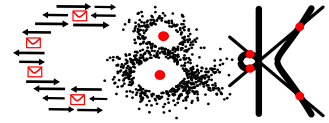
- induce single fault in two independent runs of algorithm MA + FE
- in first run leave **for**-loop after iteration s to obtain $f_s^{(q^k-1)/r}$
- in first run leave **for**-loop after iteration $s-1$ to obtain $f_{s-1}^{(q^k-1)/r}$

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1;$
for $j = t-2 \ldots s-1$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q);$
  $T \leftarrow 2T;$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q);$
    $T \leftarrow T + P;$
return $f^{(q^k-1)/r};$

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

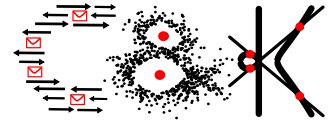
Skipping iterations with two independent faults - analysis



- P known, Q secret
- $\frac{f_{s-1}}{f_s^2} = \frac{l_{r'P,r'P}(Q) \cdot l_{2r'P,P}(Q)^{r_{s-1}}}{l_{2r'P,-2r'P}(Q) \cdot l_{r''P,-r''P}(Q)^{r_{s-1}}}$ low degree function in coordinates of Q

$\Rightarrow$ determine Q using computer algebra (system)

Skipping iterations with two independent faults - analysis

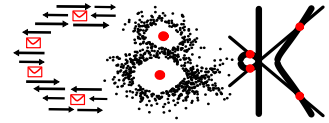


- P known, Q secret
- $\frac{f_{s-1}}{f_s^2} = \frac{l_{r'P,r'P}(Q) \cdot l_{2r'P,P}(Q)^{r_{s-1}}}{l_{2r'P,-2r'P}(Q) \cdot l_{r''P,-r''P}(Q)^{r_{s-1}}}$ low degree function in coordinates of Q

$\Rightarrow$ determine Q using computer algebra (system)

☹ only get $\left(f_{s-1}/f_s^2\right)^{(q^k-1)/r}$ (final exponentiation)

Skipping iterations with two independent faults - analysis



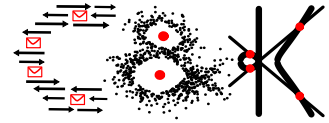
- P known, Q secret
- $\frac{f_{s-1}}{f_s^2} = \frac{l_{r'P,r'P}(Q) \cdot l_{2r'P,P}(Q)^{r_{s-1}}}{l_{2r'P,-2r'P}(Q) \cdot l_{r''P,-r''P}(Q)^{r_{s-1}}}$ low degree function in coordinates of Q

$\Rightarrow$ determine Q using computer algebra (system)

☹ only get $\left(f_{s-1}/f_s^2\right)^{(q^k-1)/r}$ (final exponentiation)

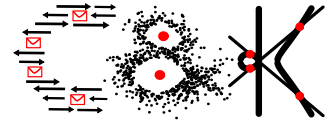
- similar analysis for other fault attacks

Final exponentiation



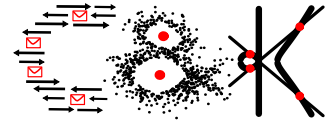
- $(q^k - 1)/r$ may be small, i.e. 4
- by choice of q, E, r

Final exponentiation



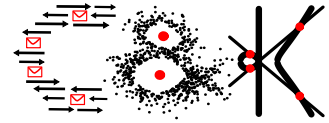
- $(q^k - 1)/r$ may be small, i.e. 4
- by choice of q, E, r
- $(q^k - 1)/r$ may be of special structure, that can be exploited
- due to optimizations of reduced Tate pairing

Final exponentiation



- $(q^k - 1)/r$ may be small, i.e. 4
- by choice of q, E, r
- $(q^k - 1)/r$ may be of special structure, that can be exploited
- due to optimizations of reduced Tate pairing
- final exponentiation can be skipped with correlated fault
- exponent can be simplified with correlated fault

Final exponentiation

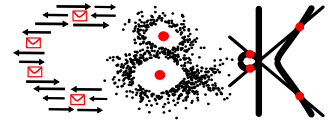


- $(q^k - 1)/r$ may be small, i.e. 4
- by choice of q, E, r
- $(q^k - 1)/r$ may be of special structure, that can be exploited
- due to optimizations of reduced Tate pairing
- final exponentiation can be skipped with correlated fault
- exponent can be simplified with correlated fault

$\Rightarrow$ final exponentiation should not be considered a countermeasure against fault attacks

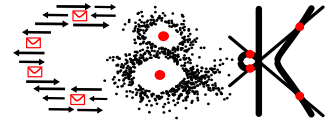
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Conclusion



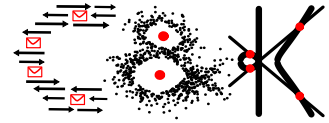
- fault attacks against pairings possible and realistic (see last two talks today)
- but more complex than in ECC, both in realization and in analysis
- combination of Miller algorithm and final exponentiation main difficulty

Conclusion



- fault attacks against pairings possible and realistic (see last two talks today)
- but more complex than in ECC, both in realization and in analysis
- combination of Miller algorithm and final exponentiation main difficulty
- timing and power analysis attacks also possible
- since points not scalars are the secrets need to attack arithmetic/elliptic curve operations

Conclusion

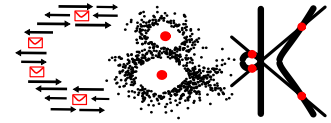


- fault attacks against pairings possible and realistic (see last two talks today)
- but more complex than in ECC, both in realization and in analysis
- combination of Miller algorithm and final exponentiation main difficulty
- timing and power analysis attacks also possible
- since points not scalars are the secrets need to attack arithmetic/elliptic curve operations

MA + FE

input : $r \in \mathbb{N}, P, Q \in E$
output: $f_{r,P}(Q)$
$T \leftarrow P, f \leftarrow 1;$
for $j = t - 2 \ldots s$ **do**
  $f \leftarrow f^2 \cdot l_{T,T}(Q) / l_{2T,-2T}(Q);$
  $T \leftarrow 2T;$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot l_{T,P}(Q) / l_{T+P,-(T+P)}(Q);$
    $T \leftarrow T + P;$
return $f^{(q^k-1)/r};$

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft



Thank you!

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft