Improved Side Channel Attacks on Pairing Based Cryptography

Peter Günther

joint work with

Johannes Blömer and Gennadij Liske

University of Paderborn

8. März 2013

Pairings as a building block. . .

. . . for various interesting primitives

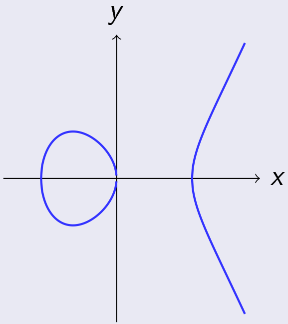
- Short signatures
- Identity based cryptography
- Attribute based encryption
- Anonymous group signatures
- Broadcast encryption
- Leak-resilient cryptography
- Noninteractive zero knowledge proofs
- . . .

Background

Foundations

- Finite field $\mathbb{F}_q$
- Degree k extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$
- Elliptic curve $E : y^2 = x^3 + ax + b$ as group with points defined over $\mathbb{F}_{q^k}$
- Large subgroups $\mathbb{G}_1, \mathbb{G}_2 \subseteq E(\mathbb{F}_{q^k})$, $\mathbb{G}_T \subseteq \mathbb{F}^*_{q^k}$ of order n
- Often $\mathbb{G}_1 \subseteq E(\mathbb{F}_{q^l})$ with $l < k$ possible

$E : y^2 = x^3 - x$



Background

The basic building block

Bilinear mapping:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

Interesting properties for application in cryptography

Bilinearity:

$$\begin{aligned} e(P_1 + Q_1, P_2) &= e(P_1, P_2) \cdot e(Q_1, P_2) \\ e(P_1, P_2 + Q_2) &= e(P_1, P_2) \cdot e(P_1, Q_2) \end{aligned}$$

Various hardness assumptions

- Fixed Argument Pairing Inversion
- Bilinear Diffie Hellman
- k-linear Decisional Diffie Hellman

Many variants

- Weil pairing
- Tate pairing
- Ate pairing
- Eta pairing

Computing the Pairing

Basic ingredient of $e(P, Q)$

- Rational function $f_{n,P}$ with zero of order n at point P and pole of order n at point $\mathcal{O}$ (neutral element/point at infinity)
- Evaluate $f_{n,P}$ at point Q.

Idea of Miller

- $f_{n,P}$ has degree n but ...
- ...there is an algorithm that evaluates $f_{n,P}$ at Q in time poly-logarithmic in n
- Based on elliptic curve double and add algorithm for computing nP
- Requires additional multiplicative correction terms

Observation

Pairings are not symmetric in their arguments.

Attacks on PBC: extending the toolbox

Our results

1. Tate pairing: extending passive attacks of Whelan/Scott (2006) and Mrabet (2009) w.r.t.
    - Secret argument P when $\mathbb{G}_1 = E(\mathbb{F}_q)$
    - Projective coordinates
    - Twists of degree 4 and 6
    - Diskussion of secret sharing as countermeasure
2. Eta pairing: generalizing fault attacks of Whelan/Scott (2007) to
    - A wider range of faults
    - Secret argument P

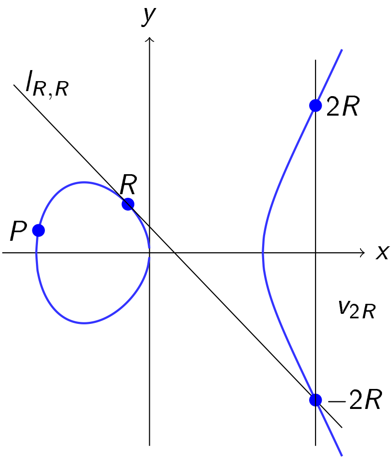
Miller Algorithm (Victor Miller 1986)

Extending the elliptic curve double and add algorithm

Input $P \in E$, $n = (n_{t-1} \dots n_0)$
Output nP

```
R ← O
for j ← t − 1, ..., 0 do
    R ← 2R
    if n_j = 1 then
        R ← R + P
    end if
end for
return R
```

Example: $E : y^2 = x^3 - x$



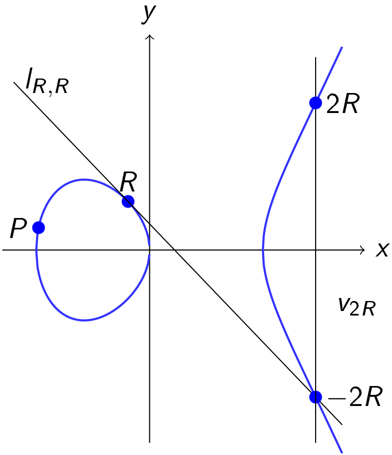
Miller Algorithm (Victor Miller 1986)

Extending the elliptic curve double and add algorithm

Input $P, Q \in E,\ n = (n_{t-1} \dots n_0)$
Output $f_{n,P}(Q)$

$f \leftarrow 1, R \leftarrow \mathcal{O}$
for $j \leftarrow t-1, \dots, 0$ **do**
  $f \leftarrow f^2 \cdot l_{R,R}(Q)/v_{2R}(Q)$
  $R \leftarrow 2R$
  if $n_j = 1$ **then**
    $f \leftarrow f \cdot l_{R,P}(Q)/v_{R+P}(Q)$
    $R \leftarrow R + P$
  end if
end for
return f

Example: $E : y^2 = x^3 - x$



Miller Algorithm (Victor Miller 1986)

Extending the elliptic curve double and add algorithm

Input $P, Q \in E,\ n = (n_{t-1} \dots n_0)$
Output $f_{n,P}(Q)$

$f \leftarrow 1, R \leftarrow \mathcal{O}$
for $j \leftarrow t-1, \dots, 0$ **do**
  $f \leftarrow f^2 \cdot l_{R,R}(Q)/v_{2R}(Q)$
  $R \leftarrow 2R$
  if $n_j = 1$ **then**
    $f \leftarrow f \cdot l_{R,P}(Q)/v_{R+P}(Q)$
    $R \leftarrow R + P$
  end if
end for
return f

- Secret is argument of function rather than exponent
  - High level program flow not dependent on secret
  - Results from ECC not applicable
- Many protocols allow secret to be either P or Q
- Pairing is not symmetric $\Rightarrow$ dedicated analysis for both cases
- Approach: dig into the arithmetic & exploit optimization

Miller Algorithm (Victor Miller 1986)

Extending the elliptic curve double and add algorithm

Input $P, Q \in E,\ n = (n_{t-1} \dots n_0)$
Output $f_{n,P}(Q)$

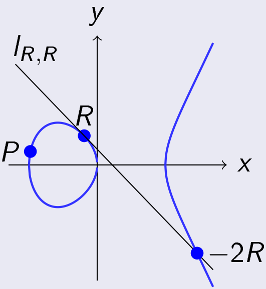
```
f ← 1, R ← O
for j ← t − 1, ..., 0 do
    f ← f² · l_{R,R}(Q)/v_{2R}(Q)
    R ← 2R
    if n_j = 1 then
        f ← f · l_{R,P}(Q)/v_{R+P}(Q)
        R ← R + P
    end if
end for
return f
```

- Secret is argument of function rather than exponent
  - High level program flow not dependent on secret
  - Results from ECC not applicable
- Many protocols allow secret to be either P or Q
- Pairing is not symmetric $\Rightarrow$ dedicated analysis for both cases
- Approach: dig into the arithmetic & exploit optimization

An example of our work: attacking the Tate pairing

Based on tangent through $R = (x_R, y_R)$ with slope $\lambda_{R,R}$

$$l_{R,R}(Q) = y_R - y_Q + \underline{\lambda_{R,R} \cdot (x_Q - x_R)}$$



Exploits a common optimization used almost everywhere

- Restrict $\mathbb{G}_1$ to $E(\mathbb{F}_q)$ (compared to $E(\mathbb{F}_{q^k})$)
- Saves a lot of expensive arithmetic in $\mathbb{F}_{q^k}$
- Possible, but this implies $\mathbb{G}_2 \not\subseteq E(\mathbb{F}_{q^d})$ for $d < k$

Analyzing the line function

Tool: correlation based power analysis of multiplication (e.g. CPA)

- Requirement: one operand is known by the attacker
- Result: recovery of the unknown operand

Application to line function

- Q secret $\Rightarrow \lambda_{R,R}$ known $\Rightarrow$ CPA $\Rightarrow$ recovery of x_Q (Whelan/Scott 06)

$$l_{R,R}(Q) = y_R - y_Q + \lambda_{R,R} \cdot (x_Q - x_R)$$

- P secret $\Rightarrow$ both operands unknown $\Rightarrow$ Problem!?

$$l_{R,R}(Q) = y_R - y_Q + \underline{\lambda_{R,R} \cdot (x_Q - x_R)}$$

- Dig even deeper into the arithmetic

The Setting of our Attack

$$l_{R,R}(Q) = y_R - y_Q + \underline{\lambda_{R,R} \cdot (x_Q - x_R)}$$

Representation of $\mathbb{G}_1$ and $\mathbb{G}_2$

- $P, R \in E(\mathbb{F}_q) \Rightarrow x_P, y_P, x_R, y_R, \lambda_{R,R} \in \mathbb{F}_q$
- $Q \in \mathbb{F}_{q^k} \Rightarrow x_Q, y_Q \in \mathbb{F}_{q^k} = \mathbb{F}_q(\alpha)$:

$$x_Q = \sum_{i=0}^{k-1} x_Q^{(i)} \alpha^i \text{ with } x_Q^{(i)} \in \mathbb{F}_q$$

Close-up of the representation

$$l_{R,R}(Q) = y_R - y_Q + \underline{\lambda_{R,R} \cdot (x_Q - x_R)}$$

A closer look at the extension field arithmetic ...

- ... shows how this is actually computed

$$\lambda_{R,R} \cdot (x_Q - x_R) = \lambda_{R,R} \cdot \left(\left(\sum_{i=0}^{k-1} x_Q^{(i)} \alpha^i \right) - x_R \right)$$

$$= \left(\lambda_{R,R} \cdot \left(x_Q^{(0)} - x_R \right) \right) \alpha^0 + \sum_{i=1}^{k-1} \left(\underline{\lambda_{R,R} \cdot x_Q^{(i)}} \right) \alpha^i$$

- $x_Q^{(i)}$ known $\Rightarrow$ CPA $\Rightarrow$ Recovery of $\lambda_{R,R}$ $\Rightarrow$ R $\Rightarrow$ P

Ongoing work and open problems

- Practical implementations of the attacks
- Practical evaluation of countermeasures
- Main open question: how vulnerable is pairing based cryptography to side channel attacks?