Hardware Operators for Pairing-Based Cryptography
— Part I: Because size matters —

Jean-Luc Beuchat
Laboratory of Cryptography and Information Security
University of Tsukuba, Japan
jeanluc.beuchat@gmail.com

Joint work with:

Nicolas Brisebarre
Arénaire, LIP, ÉNS Lyon, France

Jérémie Detrey
CACAO, LORIA, Nancy, France

Nicolas Estibals
CACAO, LORIA, Nancy, France

Eiji Okamoto
LCIS, University of Tsukuba, Japan

Francisco Rodríguez-Henríquez
CSD, IPN, Mexico City, Mexico
Outline of the talk

- Pairing-based cryptography
- Pairings over elliptic curves
- Finite-field arithmetic
- Implementation results
- Concluding thoughts
Outline of the talk

- Pairing-based cryptography
- Pairings over elliptic curves
- Finite-field arithmetic
- Implementation results
- Concluding thoughts
Elliptic curves

- \( E \) defined by a Weierstraß equation of the form
  \[ y^2 = x^3 + Ax + B \]
Elliptic curves

- $E$ defined by a Weierstraß equation of the form $y^2 = x^3 + Ax + B$

- $E(K)$ set of rational points over a field $K$
Elliptic curves

- $E$ defined by a Weierstraß equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field $K$
- Additive group law over $E(K)$
Elliptic curves

- $E$ defined by a Weierstraß equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field $K$
- Additive group law over $E(K)$
- Many applications in cryptography since 1985
  - EC-based Diffie-Hellman key exchange
  - EC-based Digital Signature Algorithm
  - ...
- Interest: smaller keys than usual cryptosystems (RSA, DSA, ElGamal, ...)
Elliptic curves

- $E$ defined by a Weierstraß equation of the form $y^2 = x^3 + Ax + B$
- $E(K)$ set of rational points over a field $K$
- Additive group law over $E(K)$
- Many applications in cryptography since 1985
  - EC-based Diffie-Hellman key exchange
  - EC-based Digital Signature Algorithm
  - ...
- Interest: smaller keys than usual cryptosystems (RSA, DSA, ElGamal, ...)
- But there’s more: bilinear pairings
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$

- $P$, a generator of the group: $\mathbb{G}_1 = \langle P \rangle$
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$
- $P$, a generator of the group: $\mathbb{G}_1 = \langle P \rangle$
- Scalar multiplication: for any integer $k$, we have $kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}$
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$

- $P$, a generator of the group: $\mathbb{G}_1 = \langle P \rangle$

- **Scalar multiplication**: for any integer $k$, we have $kP = P + P + \cdots + P$ ($k$ times)
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$

- $P$, a generator of the group: $\mathbb{G}_1 = \langle P \rangle$

- Scalar multiplication: for any integer $k$, we have $kP = P + P + \cdots + P$ ($k$ times)
Group cryptography

- \((\mathbb{G}_1, +)\), an additively-written cyclic group of prime order \(\#\mathbb{G}_1 = \ell\)

- \(P\), a generator of the group: \(\mathbb{G}_1 = \langle P \rangle\)

- **Scalar multiplication:** for any integer \(k\), we have \(kP = P + P + \cdots + P\) (\(k\) times)

- **Discrete logarithm:** given \(Q \in \mathbb{G}_1\), compute \(k\) such that \(Q = kP\)
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$

- $P$, a generator of the group: $\mathbb{G}_1 = \langle P \rangle$

- Scalar multiplication: for any integer $k$, we have $kP = P + P + \cdots + P$ ($k$ times)

- Discrete logarithm: given $Q \in \mathbb{G}_1$, compute $k$ such that $Q = kP$
Group cryptography

- \((\mathbb{G}_1, +)\), an additively-written cyclic group of prime order \(\#\mathbb{G}_1 = \ell\)
- \(P\), a generator of the group: \(\mathbb{G}_1 = \langle P \rangle\)
- Scalar multiplication: for any integer \(k\), we have \(kP = P + P + \cdots + P\) \(k\) times

Discrete logarithm: given \(Q \in \mathbb{G}_1\), compute \(k\) such that \(Q = kP\)
Group cryptography

- $(\mathbb{G}_1, +)$, an additively-written cyclic group of prime order $\#\mathbb{G}_1 = \ell$

- $P$, a generator of the group: $\mathbb{G}_1 = \langle P \rangle$

- Scalar multiplication: for any integer $k$, we have $kP = P + P + \cdots + P$

- Discrete logarithm: given $Q \in \mathbb{G}_1$, compute $k$ such that $Q = kP$

- We assume that the discrete logarithm problem (DLP) in $\mathbb{G}_1$ is hard
Bilinear pairings

- \((G_2, \times)\), a multiplicatively-written cyclic group of order \(\#G_2 = \#G_1 = \ell\)
Bilinear pairings

- $(\mathbb{G}_2, \times)$, a multiplicatively-written cyclic group of order $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$

- A bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2)$ is a map

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$$

that satisfies the following conditions:

- **non-degeneracy**: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalently $\hat{e}(P, P)$ generates $\mathbb{G}_2$)

- **bilinearity**:

$$\hat{e}(Q_1 + Q_2, R) = \hat{e}(Q_1, R) \cdot \hat{e}(Q_2, R)$$

$$\hat{e}(Q, R_1 + R_2) = \hat{e}(Q, R_1) \cdot \hat{e}(Q, R_2)$$

- **computability**: $\hat{e}$ can be efficiently computed
Bilinear pairings

- \((G_2, \times)\), a multiplicatively-written cyclic group of order \(\#G_2 = \#G_1 = \ell\)

- A bilinear pairing on \((G_1, G_2)\) is a map

\[
\hat{e} : G_1 \times G_1 \to G_2
\]

that satisfies the following conditions:

- **non-degeneracy**: \(\hat{e}(P, P) \neq 1_{G_2}\) (equivalently \(\hat{e}(P, P)\) generates \(G_2\))
- **bilinearity**:

\[
\hat{e}(Q_1 + Q_2, R) = \hat{e}(Q_1, R) \cdot \hat{e}(Q_2, R) \quad \hat{e}(Q, R_1 + R_2) = \hat{e}(Q, R_1) \cdot \hat{e}(Q, R_2)
\]
- **computability**: \(\hat{e}\) can be efficiently computed

- **Immediate property**: for any two integers \(k_1\) and \(k_2\)

\[
\hat{e}(k_1 Q, k_2 R) = \hat{e}(Q, R)^{k_1 k_2}
\]
Bilinear pairings

- \((G_2, \times)\), a multiplicatively-written cyclic group of order \(\#G_2 = \#G_1 = \ell\)

- A bilinear pairing on \((G_1, G_2)\) is a map

\[ \hat{e} : G_1 \times G_1 \rightarrow G_2 \]

that satisfies the following conditions:

- **non-degeneracy**: \(\hat{e}(P, P) \neq 1_{G_2}\) (equivalently \(\hat{e}(P, P)\) generates \(G_2\))
- **bilinearity**:

\[ \hat{e}(Q_1 + Q_2, R) = \hat{e}(Q_1, R) \cdot \hat{e}(Q_2, R) \quad \hat{e}(Q, R_1 + R_2) = \hat{e}(Q, R_1) \cdot \hat{e}(Q, R_2) \]
- **computability**: \(\hat{e}\) can be efficiently computed

- **Immediate property**: for any two integers \(k_1\) and \(k_2\)

\[ \hat{e}(k_1 Q, k_2 R) = \hat{e}(Q, R)^{k_1 k_2} \]
**Bilinear pairings**

- $(\mathbb{G}_2, \times)$, a multiplicatively-written cyclic group of order $\#\mathbb{G}_2 = \#\mathbb{G}_1 = \ell$

- A bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2)$ is a map
  $$
  \hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2
  $$
  that satisfies the following conditions:
  - **non-degeneracy:** $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ (equivalently $\hat{e}(P, P)$ generates $\mathbb{G}_2$)
  - **bilinearity:**
    $$
    \hat{e}(Q_1 + Q_2, R) = \hat{e}(Q_1, R) \cdot \hat{e}(Q_2, R) \quad \hat{e}(Q, R_1 + R_2) = \hat{e}(Q, R_1) \cdot \hat{e}(Q, R_2)
    $$
  - **computability:** $\hat{e}$ can be efficiently computed

- **Immediate property:** for any two integers $k_1$ and $k_2$
  $$
  \hat{e}(k_1 Q, k_2 R) = \hat{e}(Q, R)^{k_1 k_2}
  $$

**Diagram:**
- $k_1 Q$
- $k_2 R$
- $\hat{e}$
- $\hat{e}(Q, R)^{k_1 k_2}$
Pairings in cryptography

- At first, used to attack supersingular elliptic curves
    \[ \text{DLP}_{G_1} \]
    \[ kP \]
Pairings in cryptography

» At first, used to attack supersingular elliptic curves
  

\[
\begin{align*}
\text{DLP}_{G_1} & <_P \text{ DLP}_{G_2} \\
 kP & \rightarrow \hat{e}(kP, P) = \hat{e}(P, P)^k
\end{align*}
\]
Pairings in cryptography

- At first, used to attack supersingular elliptic curves
    \[
    \text{DLP}_{G_1} <_P \text{ DLP}_{G_2}
    \]
    \[
    kP \longrightarrow \hat{e}(kP, P) = \hat{e}(P, P)^k
    \]
  - for cryptographic applications, we will also require the DLP in $G_2$ to be hard
Pairings in cryptography

- At first, used to attack supersingular elliptic curves
    \[ \text{DLP}_{G_1} \prec_{P} \text{DLP}_{G_2} \]
    \[ kP \longrightarrow \hat{e}(kP, P) = \hat{e}(P, P)^k \]
  - for cryptographic applications, we will also require the DLP in \( G_2 \) to be hard

- One-round three-party key agreement (Joux, 2000)

- Identity-based encryption
  - Boneh-Franklin, 2001
  - Sakai-Kasahara, 2001

- Short digital signatures
  - Boneh-Lynn-Shacham, 2001
  - Zang-Safavi-Naini-Susilo, 2004

- ...
Short signature (Boneh, Lynn & Shacham, 2001)
Short signature (Boneh, Lynn & Shacham, 2001)

PKI

$P$

$aP$

Alice

Bob

$e$
Short signature (Boneh, Lynn & Shacham, 2001)

PKI

$P$  $aP$

Alice

Message digest

Bob
Short signature (Boneh, Lynn & Shacham, 2001)

PKI

$P \quad aP$

Alice  $a$

Signature:

$aD$

Bob
Short signature (Boneh, Lynn & Shacham, 2001)
Short signature (Boneh, Lynn & Shacham, 2001)

PKI

\[ P \quad aP \]

Alice \( a \)

Message digest

Signature: \( aD \)
Short signature (Boneh, Lynn & Shacham, 2001)

Alice

Bob

Message digest

Signature:
Short signature (Boneh, Lynn & Shacham, 2001)

PKI

Alice

Bob

Message digest

Signature:
Short signature (Boneh, Lynn & Shacham, 2001)

PKI

Alice

Bob

Message digest

Signature: aD

Jean-Luc Beuchat – Hardware Operators for Pairing-Based Cryptography – Part I: Because size matters
Short signature (Boneh, Lynn & Shacham, 2001)

Alice

Bob

PKI

$P$
$aP$

$\hat{e}(D, aP)$

$\hat{e}(aD, P)$

Message digest

Signature: $aD$

Jean-Luc Beuchat – Hardware Operators for Pairing-Based Cryptography – Part I: Because size matters
Outline of the talk

- Pairing-based cryptography
- Pairings over elliptic curves
- Finite-field arithmetic
- Implementation results
- Concluding thoughts
Pairings over elliptic curves

We first define

- \( \mathbb{F}_q \), a finite field, with \( q = 2^m, 3^m \) or \( p \)
- \( E \), an elliptic curve defined over \( \mathbb{F}_q \)
- \( \ell \), a large prime factor of \( \#E(\mathbb{F}_q) \)
Pairings over elliptic curves

We first define

- \( \mathbb{F}_q \), a finite field, with \( q = 2^m, 3^m \) or \( p \)
- \( E \), an elliptic curve defined over \( \mathbb{F}_q \)
- \( \ell \), a large prime factor of \( \#E(\mathbb{F}_q) \)

\[ G_1 = E(\mathbb{F}_q)[\ell], \] the \( \mathbb{F}_q \)-rational \( \ell \)-torsion of \( E \):

\[ G_1 = \{ P \in E(\mathbb{F}_q) \mid \ell P = \mathcal{O} \} \]
Pairings over elliptic curves

- We first define
  - \( \mathbb{F}_q \), a finite field, with \( q = 2^m, 3^m \) or \( p \)
  - \( E \), an elliptic curve defined over \( \mathbb{F}_q \)
  - \( \ell \), a large prime factor of \( \#E(\mathbb{F}_q) \)

- \( G_1 = E(\mathbb{F}_q)[\ell] \), the \( \mathbb{F}_q \)-rational \( \ell \)-torsion of \( E \):
  \[
  G_1 = \{ P \in E(\mathbb{F}_q) \mid \ell P = O \}
  \]

- \( G_2 = \mu_\ell \), the group of \( \ell \)-th roots of unity in \( \mathbb{F}_{q^k}^\times \):
  \[
  G_2 = \{ U \in \mathbb{F}_{q^k}^\times \mid U^\ell = 1 \}.
  \]
Pairings over elliptic curves

We first define

- $\mathbb{F}_q$, a finite field, with $q = 2^m$, $3^m$ or $p$
- $E$, an elliptic curve defined over $\mathbb{F}_q$
- $\ell$, a large prime factor of $\#E(\mathbb{F}_q)$

$G_1 = E(\mathbb{F}_q)[\ell]$, the $\mathbb{F}_q$-rational $\ell$-torsion of $E$:

$$G_1 = \{P \in E(\mathbb{F}_q) \mid \ell P = \mathcal{O}\}$$

$G_2 = \mu_\ell$, the group of $\ell$-th roots of unity in $\mathbb{F}_{q^k}^\times$:

$$G_2 = \{U \in \mathbb{F}_{q^k}^\times \mid U^\ell = 1\}$$

$k$ is the embedding degree, the smallest integer such that $\mu_\ell \subseteq \mathbb{F}_{q^k}^\times$
- usually large for ordinary elliptic curves
- bounded in the case of supersingular elliptic curves
  (4 in characteristic 2; 6 in characteristic 3; and 2 in characteristic $> 3$)
Pairings over elliptic curves

We first define

- $\mathbb{F}_q$, a finite field, with $q = 2^m, 3^m$ or $p$
- $E$, an elliptic curve defined over $\mathbb{F}_q$
- $\ell$, a large prime factor of $\#E(\mathbb{F}_q)$

$G_1 = E(\mathbb{F}_q)[\ell]$, the $\mathbb{F}_q$-rational $\ell$-torsion of $E$:

$G_1 = \{ P \in E(\mathbb{F}_q) \mid \ell P = O \}$

$G_2 = \mu_\ell$, the group of $\ell$-th roots of unity in $\mathbb{F}_{q^k}^\times$:

$G_2 = \{ U \in \mathbb{F}_{q^k}^\times \mid U^\ell = 1 \}$

$k$ is the embedding degree, the smallest integer such that $\mu_\ell \subseteq \mathbb{F}_{q^k}^\times$

- usually large for ordinary elliptic curves
- bounded in the case of supersingular elliptic curves
  (4 in characteristic 2; 6 in characteristic 3; and 2 in characteristic $> 3$)
The Tate pairing

\[ E \]

\[ \hat{e} \]
The Tate pairing

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \]
\[ (P, Q) \]
The Tate pairing

\[ P = (x_P, y_P) \]

\[ Q = (x_Q, y_Q) \]

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \rightarrow \mu_{\ell} \subseteq \mathbb{F}_q^* \]

\[ \hat{e}(P, Q) \]
The Tate pairing

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mu_\ell \subseteq \mathbb{F}_{q^k} \]

\[ \hat{e}(P, Q) \]

Computation via Miller's iterative algorithm:

- \( m/2 \) iterations over \( \mathbb{F}_{2m} \) and \( \mathbb{F}_{3m} \) (\( \eta_T \) pairing)
- \( \log_2 p \) iterations over \( \mathbb{F}_p \)
Security considerations

\[ aP \]
Security considerations

\[ aP \xrightarrow{dlog_{G_1}} a \]
Security considerations

- Discrete logarithm problem should be hard in $G_1$
Security considerations

- Discrete logarithm problem should be hard in $G_1$
Security considerations

- Discrete logarithm problem should be hard in $\mathbb{G}_1$
Security considerations

- Discrete logarithm problem should be hard in $\mathbb{G}_1$
Security considerations

- Discrete logarithm problem should be hard in $\mathbb{G}_1$
Security considerations

- Discrete logarithm problem should be hard in $G_1$

- Discrete logarithm problem should be hard in $G_2$
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \]
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \]

- Discrete logarithm in \( G_1 = E(\mathbb{F}_q)[\ell] \) (Pollard’s \( \rho \)):

\[ \sqrt{\ell} \approx \sqrt{q} \]

- Discrete logarithm in \( G_2 = \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \) (FFS or NFS):

\[ \exp \left( c \cdot (\ln q^k)^{\frac{1}{3}} \cdot (\ln \ln q^k)^{\frac{2}{3}} \right) \]
Security considerations

\[ \hat{e} : E(F_q)[\ell] \times E(F_q)[\ell] \to \mu_\ell \subseteq F_{q^k}^\times \]

- Discrete logarithm in \( G_1 = E(F_q)[\ell] \) (Pollard’s \( \rho \)):

\[ \sqrt{\ell} \approx \sqrt{q} = \exp \left( \frac{1}{2} \cdot (\ln q) \right) \]

- Discrete logarithm in \( G_2 = \mu_\ell \subseteq F_{q^k}^\times \) (FFS or NFS):

\[ \exp \left( c \cdot (\ln q^k)^{\frac{1}{3}} \cdot (\ln \ln q^k)^{\frac{2}{3}} \right) \]
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \]

- Discrete logarithm in \( G_1 = E(\mathbb{F}_q)[\ell] \) (Pollard’s \( \rho \)):

\[ \sqrt{\ell} \approx \sqrt{q} = \exp \left( \frac{1}{2} \cdot (\ln q) \right) \]

- Discrete logarithm in \( G_2 = \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \) (FFS or NFS):

\[ \exp \left( c \cdot (\ln q^k)^\frac{1}{3} \cdot (\ln \ln q^k)^\frac{2}{3} \right) \]

- The discrete logarithm problem is usually easier in \( G_2 \) than in \( G_1 \)

  - current security: \( \sim 2^{80} \), equivalent to 80-bit symmetric encryption or RSA-1024
  - recommended security: \( \sim 2^{128} \) (AES-128, RSA-3072)
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \]

- The embedding degree \( k \) depends on the field characteristic \( q \).
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)\mathbb{[}l\mathbb{]} \times E(\mathbb{F}_q)\mathbb{[}l\mathbb{]} \to \mu_l \subseteq \mathbb{F}_{q^k} \]

> The embedding degree \( k \) depends on the field characteristic \( q \)

<table>
<thead>
<tr>
<th>Base field ((\mathbb{F}_q))</th>
<th>( \mathbb{F}_{2m} )</th>
<th>( \mathbb{F}_{3m} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Embedding degree ((k))</strong></td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \]

- The embedding degree \( k \) depends on the field characteristic \( q \)

<table>
<thead>
<tr>
<th>Base field ((\mathbb{F}_q))</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding degree ((k))</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Lower security ((\sim 2^{64}))</td>
<td>( m = 239 )</td>
<td>( m = 97 )</td>
<td>(</td>
</tr>
<tr>
<td>Medium security ((\sim 2^{80}))</td>
<td>( m = 373 )</td>
<td>( m = 163 )</td>
<td>(</td>
</tr>
<tr>
<td>Higher security ((\sim 2^{128}))</td>
<td>( m = 1103 )</td>
<td>( m = 503 )</td>
<td>(</td>
</tr>
</tbody>
</table>
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mu_\ell \subseteq \mathbb{F}_q^\times \]

- The embedding degree \( k \) depends on the field characteristic \( q \)

<table>
<thead>
<tr>
<th>Base field (( \mathbb{F}_q ))</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding degree (( k ))</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Lower security (( \sim 2^{64} ))</td>
<td>( m = 239 )</td>
<td>( m = 97 )</td>
<td>(</td>
</tr>
<tr>
<td>Medium security (( \sim 2^{80} ))</td>
<td>( m = 373 )</td>
<td>( m = 163 )</td>
<td>(</td>
</tr>
<tr>
<td>Higher security (( \sim 2^{128} ))</td>
<td>( m = 1103 )</td>
<td>( m = 503 )</td>
<td>(</td>
</tr>
</tbody>
</table>

- \( \mathbb{F}_{2^m} \): simpler finite field arithmetic

Jean-Luc Beuchat – Hardware Operators for Pairing-Based Cryptography – Part I: Because size matters
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mu_\ell \subseteq \mathbb{F}_q^\times \]

- The embedding degree \( k \) depends on the field characteristic \( q \)

<table>
<thead>
<tr>
<th>Base field (( \mathbb{F}_q ))</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding degree (( k ))</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Lower security (( \sim 2^{64} ))</td>
<td>( m = 239 )</td>
<td>( m = 97 )</td>
<td>(</td>
</tr>
<tr>
<td>Medium security (( \sim 2^{80} ))</td>
<td>( m = 373 )</td>
<td>( m = 163 )</td>
<td>(</td>
</tr>
<tr>
<td>Higher security (( \sim 2^{128} ))</td>
<td>( m = 1103 )</td>
<td>( m = 503 )</td>
<td>(</td>
</tr>
</tbody>
</table>

- \( \mathbb{F}_{2^m} \): simpler finite field arithmetic

- \( \mathbb{F}_{3^m} \): smaller field extension
Security considerations

\[ \hat{e} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mu_\ell \subseteq \mathbb{F}_{q^k} \]

- The embedding degree \( k \) depends on the field characteristic \( q \)

<table>
<thead>
<tr>
<th>Base field (( \mathbb{F}_q ))</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding degree (( k ))</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Lower security (( \sim 2^{64} ))</td>
<td>( m = 239 )</td>
<td>( m = 97 )</td>
<td>(</td>
</tr>
<tr>
<td>Medium security (( \sim 2^{80} ))</td>
<td>( m = 373 )</td>
<td>( m = 163 )</td>
<td>(</td>
</tr>
<tr>
<td>Higher security (( \sim 2^{128} ))</td>
<td>( m = 1103 )</td>
<td>( m = 503 )</td>
<td>(</td>
</tr>
</tbody>
</table>

- \( \mathbb{F}_{2^m} \): simpler finite field arithmetic
- \( \mathbb{F}_{3^m} \): smaller field extension
- \( \mathbb{F}_p \): prohibitive field sizes
Security considerations

\[ \hat{e}: E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mu_\ell \subseteq \mathbb{F}_{q^k}^\times \]

- The embedding degree \( k \) depends on the field characteristic \( q \)

<table>
<thead>
<tr>
<th>Base field (( \mathbb{F}_q ))</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding degree (( k ))</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Lower security (( \sim 2^{64} ))</td>
<td>( m = 239 )</td>
<td>( m = 97 )</td>
<td>(</td>
</tr>
<tr>
<td>Medium security (( \sim 2^{80} ))</td>
<td>( m = 373 )</td>
<td>( m = 163 )</td>
<td>(</td>
</tr>
<tr>
<td>Higher security (( \sim 2^{128} ))</td>
<td>( m = 1103 )</td>
<td>( m = 503 )</td>
<td>(</td>
</tr>
</tbody>
</table>

- \( \mathbb{F}_{2^m} \): simpler finite field arithmetic
- \( \mathbb{F}_{3^m} \): smaller field extension
- \( \mathbb{F}_p \): prohibitive field sizes
Computation of the Tate pairing

\[ \hat{e} : E(\mathbb{F}_p^m)[\ell] \times E(\mathbb{F}_p^m)[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}_p^{km} \]
Computation of the Tate pairing

$$\hat{e} : E(\mathbb{F}_{p^m})[\ell] \times E(\mathbb{F}_{p^m})[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}^\times_{p^{km}}$$

► Arithmetic over $\mathbb{F}_{p^m}$:

- polynomial basis: $\mathbb{F}_{p^m} \cong \mathbb{F}_p[x]/(f(x))$
- $f(x)$, degree-$m$ polynomial irreducible over $\mathbb{F}_p$
Computation of the Tate pairing

\[ \hat{e} : E(\mathbb{F}_{p^m})[\ell] \times E(\mathbb{F}_{p^m})[\ell] \rightarrow \mu_\ell \subseteq \mathbb{F}_{p^{km}}^{\times} \]

- **Arithmetic over** \( \mathbb{F}_{p^m} \):
  - polynomial basis: \( \mathbb{F}_{p^m} \cong \mathbb{F}_p[x]/(f(x)) \)
  - \( f(x) \), degree-\( m \) polynomial irreducible over \( \mathbb{F}_p \)

- **Arithmetic over** \( \mathbb{F}_{p^{km}}^{\times} \):
  - tower-field representation
  - only arithmetic over the underlying field \( \mathbb{F}_{p^m} \)
Computation of the Tate pairing

\[ \hat{e} : E(F_{p^m})[\ell] \times E(F_{p^m})[\ell] \rightarrow \mu_\ell \subseteq F_{p^{km}} \]

► Arithmetic over \( F_{p^m} \):
  - polynomial basis: \( F_{p^m} \cong F_p[x]/(f(x)) \)
  - \( f(x) \), degree-\( m \) polynomial irreducible over \( F_p \)

► Arithmetic over \( F_{p^{km}} \):
  - tower-field representation
  - only arithmetic over the underlying field \( F_{p^m} \)

► Operations over \( F_{p^m} \):

<table>
<thead>
<tr>
<th>Base field ( (F_{p^m}) )</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{2^{313}} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_{3^{127}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( +/− )</td>
<td>27 ( \left\lfloor \frac{m}{2} \right\rfloor ) + 75</td>
<td>4287</td>
<td>119 ( \left\lfloor \frac{m}{4} \right\rfloor ) + 260</td>
<td>3949</td>
</tr>
<tr>
<td>( \times )</td>
<td>7 ( \left\lfloor \frac{m}{2} \right\rfloor ) + 29</td>
<td>1121</td>
<td>25 ( \left\lfloor \frac{m}{4} \right\rfloor ) + 93</td>
<td>868</td>
</tr>
<tr>
<td>( a^p )</td>
<td>6( m ) + 9</td>
<td>1887</td>
<td>17 ( \left\lfloor \frac{m}{2} \right\rfloor ) + 8</td>
<td>1079</td>
</tr>
<tr>
<td>( a^{-1} )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Computation of the Tate pairing

\[ \hat{e} : E(\mathbb{F}_{p^m})[\ell] \times E(\mathbb{F}_{p^m})[\ell] \to \mu_\ell \subseteq \mathbb{F}_{p^{km}} \]

- Arithmetic over \( \mathbb{F}_{p^m} \):
  - polynomial basis: \( \mathbb{F}_{p^m} \cong \mathbb{F}_p[x]/(f(x)) \)
  - \( f(x) \), degree-\( m \) polynomial irreducible over \( \mathbb{F}_p \)

- Arithmetic over \( \mathbb{F}_{p^{km}} \):
  - tower-field representation
  - only arithmetic over the underlying field \( \mathbb{F}_{p^m} \)

- Operations over \( \mathbb{F}_{p^m} \):

<table>
<thead>
<tr>
<th>Base field (( \mathbb{F}_{p^m} ))</th>
<th>( \mathbb{F}_{2^m} )</th>
<th>( \mathbb{F}_{2^{313}} )</th>
<th>( \mathbb{F}_{3^m} )</th>
<th>( \mathbb{F}_{3^{127}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(+/-)</td>
<td>( 27 \lceil \frac{m}{2} \rceil + 75 )</td>
<td>4287</td>
<td>119 ( \lceil \frac{m}{4} \rceil ) + 260</td>
<td>3949</td>
</tr>
<tr>
<td>( \times )</td>
<td>( 7 \lceil \frac{m}{2} \rceil + 29 )</td>
<td>1121</td>
<td>25 ( \lceil \frac{m}{4} \rceil ) + 93</td>
<td>868</td>
</tr>
<tr>
<td>( a^p )</td>
<td>( 6m + 9 )</td>
<td>1887</td>
<td>17 ( \lceil \frac{m}{2} \rceil ) + 8</td>
<td>1079</td>
</tr>
<tr>
<td>( a^{-1} )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Software** not well suited to small characteristic: need for hardware acceleration
Outline of the talk

- Pairing-based cryptography
- Pairings over elliptic curves
- Finite-field arithmetic
- Implementation results
- Concluding thoughts
Outline of the talk

▶ Pairing-based cryptography
▶ Pairings over elliptic curves
▶ **Finite-field arithmetic (only in characteristic 3)**
▶ Implementation results
▶ Concluding thoughts
Arithmetic over $\mathbb{F}_{3^m}$

- $f \in \mathbb{F}_3[x]$: degree-$m$ irreducible polynomial over $\mathbb{F}_3$

$$f = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + f_0$$
Arithmetic over $\mathbb{F}_{3^m}$

- $f \in \mathbb{F}_3[x]$: degree-$m$ irreducible polynomial over $\mathbb{F}_3$
  
  \[ f = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + f_0 \]

- $\mathbb{F}_{3^m} \cong \mathbb{F}_3[x]/(f)$

- $a \in \mathbb{F}_{3^m}$:
  
  \[ a = a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \]

- Each element of $\mathbb{F}_3$ stored using two bits
Addition over $\mathbb{F}_{3^m}$

$r = a + b = (a_{m-1} + b_{m-1})x^{m-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$
Addition over $\mathbb{F}_{3^m}$

\[ r = a + b = (a_{m-1} + b_{m-1})x^{m-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0) \]

- coefficient-wise additions over $\mathbb{F}_3$: \( r_i = (a_i + b_i) \mod 3 \)
Addition over $\mathbb{F}_{3^m}$

\[ r = a + b = (a_{m-1} + b_{m-1})x^{m-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0) \]

- coefficient-wise additions over $\mathbb{F}_3$: $r_i = (a_i + b_i) \mod 3$
- addition over $\mathbb{F}_3$: small look-up tables
Addition, subtraction and accumulation over $\mathbb{F}_{3^m}$

- **sign selection**: multiplication by 1 or 2
  $$-a \equiv 2a \pmod{3}$$

- **feedback loop** for accumulation
Multiplication over $\mathbb{F}_{3^m}$

- **Parallel-serial multiplication**
  - multiplicand loaded in a parallel register
  - multiplier loaded in a shift register

- Most significant coefficients first (Horner scheme)

- $D$ coefficients processed at each clock cycle: $\left\lceil \frac{m}{D} \right\rceil$ cycles per multiplication
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{cccc}
  x^{m-1} & \ldots & x^2 & x \\
  a & & & \\
\end{array}
\]

\[
\begin{array}{cccc}
  \times & \bullet & \bullet & \bullet \\
  b & & & \\
\end{array}
\]

\[
\begin{array}{cccc}
  \bullet & \bullet & \bullet & \bullet \\
  & & & \\
\end{array}
\]

\[
\begin{array}{cccc}
  \bullet & \bullet & \bullet & \bullet \\
  & & & \\
\end{array}
\]
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

$$x^{m-1} \ldots x^2 x 1$$

\[ \begin{array}{cccc}
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\end{array} \]
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{cccccc}
  x^{m-1} & \ldots & x^2 & x & 1 \\
  \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & a \\
  \times & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & b \\
  \hline
  \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & b_{m-1} \cdot a \\
  \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & b_{m-2} \cdot a \\
  \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & b_{m-3} \cdot a
\end{array}
\]
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{cccccc}
x^{m-1} & \ldots & x^2 & x & 1 \\
\times & & & & \\
\hline \\
& & & b_{m-1} \cdot a \cdot x^2 & \\
& & b_{m-2} \cdot a \cdot x & \\
& b_{m-3} \cdot a & \\
\end{array}
\]
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{cccccc}
  & x^{m-1} & \cdots & x^2 & x & 1 \\
\times & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\hline \\
  & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
  & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
  & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
  & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\end{array}
\]

$a$

$b$

$b_{m-1} \cdot a \cdot x^2$

$b_{m-2} \cdot a \cdot x$

$b_{m-3} \cdot a$
Example for $D = 3$ (3 coefficients per iteration):

\[ x^{m-1} \quad \ldots \quad x^2 \quad x^1 \]

\[ \times \]

\[ \begin{array}{cccc}
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\end{array} \]

\[
\begin{array}{cccc}
a & b & (b_{m-1} \cdot a \cdot x^2) \mod f \\
b & \cdot & (b_{m-2} \cdot a \cdot x) \mod f \\
\cdot & \cdot & b_{m-3} \cdot a \\
\end{array}
\]
Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{ccccccc}
  x^{m-1} & \cdots & x^2 & x & 1 \\
  \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
  \times & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
  \hline
  \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
  + & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
  + & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
  \hline
  \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{array}
\]

$a$

$b$

$(b_{m-1} \cdot a \cdot x^2) \mod f$

$(b_{m-2} \cdot a \cdot x) \mod f$

$b_{m-3} \cdot a$

$r$ (partial sum)
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{c}
\begin{array}{cccc}
 x^{m-1} & \ldots & x^2 & x^1 \\
 a & b & (b_{m-1} \cdot a \cdot x^2) \mod f & (b_{m-2} \cdot a \cdot x) \mod f \\
 \times & & & b_{m-3} \cdot a \\
 + & & & r \text{ (partial sum)}
\end{array}
\end{array}
\]
Example for $D = 3$ (3 coefficients per iteration):

$$
\begin{array}{cccc}
  x^{m-1} & \ldots & x^2 & x & 1 \\
  a & & & & \\
  \times & & & & \\
  b & & & & \\
  \hline
  (b_{m-1} \cdot a \cdot x^2) \mod f \\
  (b_{m-2} \cdot a \cdot x) \mod f \\
  b_{m-3} \cdot a \\
  \hline
  r \quad \text{(partial sum)}
\end{array}
$$
Example for $D = 3$ (3 coefficients per iteration):

\[
x^{m-1} \quad \ldots \quad x^2 \quad x^1
\]

\[
\begin{align*}
\times & \quad a \\
\times & \quad b \\
\hline
\end{align*}
\]

\[
\begin{align*}
(b_{m-1} \cdot a \cdot x^2) \mod f & \\
(b_{m-2} \cdot a \cdot x) \mod f & \\
(b_{m-3} \cdot a) & \\
\hline
r & \text{(partial sum)} \\
(b_{m-4} \cdot a) & \\
(b_{m-5} \cdot a) & \\
(b_{m-6} \cdot a) & \\
\end{align*}
\]
Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{c}
\times \quad x^{m-1} \quad \ldots \quad x^2 \quad x \quad 1 \\
\times \\
\hline \\
\end{array}
\]

\[
\begin{array}{c}
a \\
b \\
(b_{m-1} \cdot a \cdot x^2) \mod f \\
(b_{m-2} \cdot a \cdot x) \mod f \\
b_{m-3} \cdot a \\
r \cdot x^3 \\
(b_{m-4} \cdot a \cdot x^2) \\
(b_{m-5} \cdot a \cdot x) \\
b_{m-6} \cdot a
\end{array}
\]
**Multiplication over \( \mathbb{F}_{3^m} \)**

Example for \( D = 3 \) (3 coefficients per iteration):

\[
\begin{array}{cccc}
   x^{m-1} & \ldots & x^2 & x & 1 \\
\hline
   a \\
   b \\
\end{array}
\]

\[
\begin{array}{cccc}
   \cdot \\
\hline
   (b_{m-1} \cdot a \cdot x^2) \mod f \\
   (b_{m-2} \cdot a \cdot x) \mod f \\
   b_{m-3} \cdot a \\
\end{array}
\]

\[
\begin{array}{cccc}
   \cdot \cdot \\
\hline
   r \cdot x^3 \\
   b_{m-4} \cdot a \cdot x^2 \\
   b_{m-5} \cdot a \cdot x \\
   b_{m-6} \cdot a \\
\end{array}
\]
Example for $D = 3$ (3 coefficients per iteration):

\[
x^{m-1} \quad \ldots \quad x^2 \quad x \quad 1
\]

\[
\begin{array}{cccccc}
\times & & & & & \\
& & & & & \\
+ & & & & & \\
+ & & & & & \\
\end{array}
\]

\[
\begin{array}{cccccc}
\text{a} & & & & & \\
\text{b} & & & & & \\
(b_{m-1} \cdot a \cdot x^2) \mod f & & & & & \\
(b_{m-2} \cdot a \cdot x) \mod f & & & & & \\
b_{m-3} \cdot a & & & & & \\
(r \cdot x^3) \mod f & & & & & \\
(b_{m-4} \cdot a \cdot x^2) \mod f & & & & & \\
(b_{m-5} \cdot a \cdot x) \mod f & & & & & \\
b_{m-6} \cdot a & & & & & \\
\end{array}
\]
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

\[
\begin{array}{cccc}
  x^{m-1} & \ldots & x^2 & x^1 \\
  a & b & & \\
  \times & & & \\
  \hline
  & (b_{m-1} \cdot a \cdot x^2) \mod f & (b_{m-2} \cdot a \cdot x) \mod f & b_{m-3} \cdot a \\
  + & & & \\
  + & & & \\
  + & & & \\
  + & & & \\
  \hline
  & (r \cdot x^3) \mod f & (b_{m-4} \cdot a \cdot x^2) \mod f & (b_{m-5} \cdot a \cdot x) \mod f & b_{m-6} \cdot a \\
  \hline
  & & & & r \text{ (partial sum)}
\end{array}
\]
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):

$$x^{m-1} \quad \ldots \quad x^2 \quad x^1$$

$$\times \quad a \quad b$$

$$\frac{b_{m-1} \cdot a \cdot x^2 \mod f}{+ \quad b_{m-2} \cdot a \cdot x \mod f} \quad b_{m-3} \cdot a$$

$$\frac{r \cdot x^3 \mod f}{+ \quad b_{m-4} \cdot a \cdot x^2 \mod f} \quad b_{m-5} \cdot a \quad b_{m-6} \cdot a$$

$$r \quad \text{(partial sum)}$$
Example for $D = 3$ (3 coefficients per iteration):

$\begin{array}{cccc}
& x^{m-1} & \ldots & x^2 & x & 1 \\
\times & & & & & \\
\hline
& a & & & & \\
& b & & & & \\
\hline
+ & & & & & \\
+ & & & & & \\
\hline
& (b_{m-1} \cdot a \cdot x^2) \mod f & & & & \\
+ & (b_{m-2} \cdot a \cdot x) \mod f & & & & \\
+ & b_{m-3} \cdot a & & & & \\
\hline
& (r_\cdot x^3) \mod f & & & & \\
+ & (b_{m-4} \cdot a \cdot x^2) \mod f & & & & \\
+ & (b_{m-5} \cdot a \cdot x) \mod f & & & & \\
+ & b_{m-6} \cdot a & & & & \\
\hline
& r & & & & (\text{partial sum})
\end{array}$
Example for $D = 3$ (3 coefficients per iteration):

$$
\begin{array}{rcccc}
\times & x^{m-1} & \ldots & x^2 & x & 1 \\
\times & a \\
\times & b \\
\hline
+ & (b_{m-1} \cdot a \cdot x^2) \mod f & (b_{m-2} \cdot a \cdot x) \mod f & b_{m-3} \cdot a \\
+ & (r \cdot x^3) \mod f & (b_{m-4} \cdot a \cdot x^2) \mod f & (b_{m-5} \cdot a \cdot x) \mod f & b_{m-6} \cdot a \\
+ & \ldots \\
\hline
r & \text{partial sum} \\
\end{array}
$$
Multiplication over $\mathbb{F}_3^m$

- Computing the partial products $b_j \cdot a$:
  - coefficient-wise multiplication over $\mathbb{F}_3$: $(b_j \cdot a_i) \mod 3$
  - multiplications over $\mathbb{F}_3$: small look-up tables
Multiplication over $\mathbb{F}_{3^m}$

- Computing the partial products $b_j \cdot a$:
  - coefficient-wise multiplication over $\mathbb{F}_3$: $(b_j \cdot a_i) \mod 3$
  - multiplications over $\mathbb{F}_3$: small look-up tables

- Multiplication by $x^j$: simple shift (only wires)
Multiplication over $\mathbb{F}_{3^m}$

- Computing the partial products $b_j \cdot a_i$:
  - coefficient-wise multiplication over $\mathbb{F}_3$: $(b_j \cdot a_i) \mod 3$
  - multiplications over $\mathbb{F}_3$: small look-up tables

- Multiplication by $x^j$: simple shift (only wires)

- Modulo $f$ reduction:
  - $f = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + f_0$ gives
    \[ x^m \equiv (-f_{m-1})x^{m-1} + \cdots + (-f_1)x + (-f_0) \pmod{f} \]
  - highest degree of polynomial to reduce: $m + D - 1$
  - if $f$ is carefully selected (e.g. a trinomial or pentanomial),
    only a few multiplications and additions over $\mathbb{F}_3$
Multiplication over $\mathbb{F}_{3^m}$

- Computing the partial products $b_j \cdot a$:
  - coefficient-wise multiplication over $\mathbb{F}_3$: $(b_j \cdot a_i) \mod 3$
  - multiplications over $\mathbb{F}_3$: small look-up tables

- Multiplication by $x^j$: simple shift (only wires)

- Modulo $f$ reduction:
  - $f = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + f_0$ gives
    \[
    x^m \equiv (-f_{m-1})x^{m-1} + \cdots + (-f_1)x + (-f_0) \pmod{f}
    \]
  - highest degree of polynomial to reduce: $m + D - 1$
  - if $f$ is carefully selected (e.g. a trinomial or pentanomial), only a few multiplications and additions over $\mathbb{F}_3$
  - example for $m = 97$: $f = x^{97} + x^{12} + 2$
Multiplication over $\mathbb{F}_{3^m}$

Example for $D = 3$ (3 coefficients per iteration):
Frobenius map over $\mathbb{F}_{3^m}$: cubing

Since $\binom{3}{1} = \binom{3}{2} = 3$:

$$a^3 \equiv a_{m-1}x^{3(m-1)} + \cdots + a_1x^3 + a_0 \pmod{3}$$

Degree-$(3m - 3)$ polynomial: requires a modulo $f$ reduction
Frobenius map over $\mathbb{F}_{3^m}$: cubing

- Since $\binom{3}{1} = \binom{3}{2} = 3$:

$$a^3 \equiv a_{m-1}x^{3(m-1)} + \cdots + a_1x^3 + a_0 \pmod{3}$$

- Degree-$(3m - 3)$ polynomial: requires a modulo $f$ reduction

- Symbolic computation of the reduction:
  
  each coefficient of the result is a linear combination of the $a_i$’s

$$a^3 \mod f = \sum_{j=0}^{n-1} w_j \cdot \mu_j$$

with $w_j \in \mathbb{F}_3$, $\mu_j \in \mathbb{F}_{3^m}$, and $\mu_{j,i} \in \{0\} \cup \{a_{m-1}, \ldots, a_1, a_0\}$
Frobenius map over $\mathbb{F}_{3^m}$

Example for $m = 97$ and $f = x^{97} + x^{12} + 2$:

$$a^3 \mod f = \left(a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0\right) \times 1$$
$$+ \left(0 + 0 + a_{88}x^{94} + \cdots + 0 + 0 + a_{89}\right) \times 1$$
$$+ \left(0 + 0 + a_{92}x^{94} + \cdots + 0 + 0 + a_{93}\right) \times 1$$
$$+ \left(0 + a_{60}x^{95} + 0 + \cdots + 0 + a_{61}x + 0\right) \times 2$$
Example for $m = 97$ and $f = x^{97} + x^{12} + 2$:

$$a^3 \mod f = \left( a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0 \right) \times 1$$

$$+ \left( 0 + 0 + a_{88}x^{94} + \cdots + 0 + 0 + a_{89} \right) \times 1$$

$$+ \left( 0 + 0 + a_{92}x^{94} + \cdots + 0 + 0 + a_{93} \right) \times 1$$

$$+ \left( 0 + a_{60}x^{95} + 0 + \cdots + 0 + a_{61}x + 0 \right) \times 2$$

$$= \left( a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0 \right) \times 1$$

$$+ \left( 0 + a_{60}x^{95} + a_{88}x^{94} + \cdots + 0 + a_{61}x + a_{89} \right) \times 1$$

$$+ \left( 0 + a_{60}x^{95} + a_{92}x^{94} + \cdots + 0 + a_{61}x + a_{93} \right) \times 1$$
Example for $m = 97$ and $f = x^{97} + x^{12} + 2$:

$$a^3 \mod f = (a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0) \times 1$$

$$+ (0 + 0 + a_{88}x^{94} + \cdots + 0 + 0 + a_{89}) \times 1$$

$$+ (0 + 0 + a_{92}x^{94} + \cdots + 0 + 0 + a_{93}) \times 1$$

$$+ (0 + a_{60}x^{95} + 0 + \cdots + 0 + a_{61}x + 0) \times 2$$

$$= (a_{32}x^{96} + a_{64}x^{95} + a_{96}x^{94} + \cdots + a_{33}x^2 + a_{65}x + a_0) \times 1$$

$$+ (0 + a_{60}x^{95} + a_{88}x^{94} + \cdots + 0 + a_{61}x + a_{89}) \times 1$$

$$+ (0 + a_{60}x^{95} + a_{92}x^{94} + \cdots + 0 + a_{61}x + a_{93}) \times 1$$

Required hardware:

- only wires to compute the $\mu_j$’s
- multiplications over $\mathbb{F}_3$ for the weights $w_j$
- multi-operand addition over $\mathbb{F}_{3^m}$
Frobenius map over $\mathbb{F}_{3^m}$

- feedback loop for successive cubings
- sign selection for computing either $a^3$ or $-a^3$
Inversion over $\mathbb{F}_{3^m}$

- Extended Euclidean Algorithm?
Inversion over $\mathbb{F}_{3^m}$

- Extended Euclidean Algorithm?
  - fast computation
  - ... but need for additional hardware
Inversion over $\mathbb{F}_{3^m}$

- Extended Euclidean Algorithm?
  
  - fast computation
  - ... but need for additional hardware

- Our solution: Fermat’s little theorem

$$a^{-1} = a^{3^m-2} \quad \text{on } \mathbb{F}_{3^m} \ (a \neq 0)$$
Inversion over $\mathbb{F}_{3^m}$

- Extended Euclidean Algorithm?
  - fast computation
  - ... but need for additional hardware

- Our solution: Fermat’s little theorem

\[
a^{-1} = a^{3^m-2} \quad \text{on } \mathbb{F}_{3^m} \ (a \neq 0)
\]

- algorithm by Itoh and Tsujii
- requires only multiplications and cubings over $\mathbb{F}_{3^m}$
Inversion over $\mathbb{F}_{3^m}$

- **Extended Euclidean Algorithm?**
  - *fast* computation
  - *... but need for additional hardware*

- **Our solution: Fermat’s little theorem**

\[
a^{-1} = a^{3^m-2} \quad \text{on } \mathbb{F}_{3^m} \ (a \neq 0)
\]

- algorithm by Itoh and Tsujii
- requires only *multiplications* and *cubings* over $\mathbb{F}_{3^m}$
- only *one inversion* for the full pairing: delay overhead is negligible ($< 1\%$)
The full processing element
The full processing element

- For the Tate pairing:
  limited parallelism between additions, multiplications and Frobenius maps

- Can we share hardware resources between the three operators?
What can we share?

▶ Input and output registers

▶ Partial product generators:
  • sign selection for the addition / subtraction
  • partial products for the multiplication
  • multiplication by the $w_j$’s for the Frobenius map

▶ Multi-operand addition tree

▶ Feedback loops for accumulation
Our unified operator
Our unified operator

[Diagram of the unified operator with various components and operations labeled, including select, load, cubing, multiplication, multiplication accumulate, and enable.]
Our unified operator
Outline of the talk

- Pairing-based cryptography
- Pairings over elliptic curves
- Finite-field arithmetic
- Implementation results
- Concluding thoughts
Experimental setup

- Full coprocessor for computation of the Tate pairing
- Architecture based on our unified operator
- Prototyped on a Xilinx Virtex-II Pro 20 FPGA (mid-range model)
- Post place-and-route results: area, computation time, AT product
Coproces sor area (characteristic 2)

Area usage [%]

Equivalent symmetric key size [bits]

\[ D = 7 \]
\[ D = 15 \]
\[ D = 31 \]
Coprocessor area (characteristic 3)

![Graph showing the relationship between area usage and equivalent symmetric key size for different characteristic values.]

Area usage [%]

Equivalent symmetric key size [bits]
Coprocessor area

Area usage [%]

Equivalent symmetric key size [bits]

Characteristic 2

Characteristic 3

D = 3
D = 7
D = 15
D = 31
Calculation time (characteristic 2)

Equivalent symmetric key size [bits]

Calc. time [$\mu$s]

- $D = 7$
- $D = 15$
- $D = 31$
Calculation time (characteristic 3)

Calc. time [$\mu$s]

Equivalent symmetric key size [bits]

$D = 3$

$D = 7$

$D = 15$
Calculation time

Calc. time [µs]

Characteristic 2
Characteristic 3

Equivalent symmetric key size [bits]

D = 3
D = 7
D = 15
D = 31
D = 7
D = 15
Comparison with published results

AT product

Results from the literature

Equivalent symmetric key size [bits]
Comparison with published results

![Graph showing comparison between different operators and AT product vs. equivalent symmetric key size.](Image)

- **Results from the literature**
- **Unified operator, char. 2 \((D = 15)\)**
- **Unified operator, char. 3 \((D = 7)\)**
Comparison with published results

Equivalent symmetric key size [bits]

AT product

- Results from the literature
- Unified operator, char. 2 ($D = 15$)
- Unified operator, char. 3 ($D = 7$)
- Parallel operator, char. 2
- Parallel operator, char. 3
Comparison with published results

AT product

Equivalent symmetric key size [bits]

Results from the literature
Unified operator, char. 2 ($D = 15$)
Unified operator, char. 3 ($D = 7$)
Parallel operator, char. 2
Parallel operator, char. 3

AES-128?
Outline of the talk

- Pairing-based cryptography
- Pairings over elliptic curves
- Finite-field arithmetic
- Implementation results
- Concluding thoughts
Concluding thoughts

- **Characteristic 3** performs slightly better than **characteristic 2**
  
  - at least on our **unified architecture**
  - good overall performances vouch for **stronger confidence** in this observation
Concluding thoughts

- **Characteristic 3** performs slightly better than **characteristic 2**
  - at least on our **unified architecture**
  - good overall performances vouch for **stronger confidence** in this observation
  - not true anymore on **parallel architectures**: the battle is not over!
Concluding thoughts

- **Characteristic 3** performs slightly better than **characteristic 2**
  - at least on our **unified architecture**
  - good overall performances vouch for **stronger confidence** in this observation
  - not true anymore on **parallel architectures**: the battle is not over!

- **Unified operator**
  - small but also **competitively fast**
  - parameter $D$ to explore the **area-time tradeoff**
  - high scalability: support for **larger extension degrees** and **higher levels of security**
  - automatic **VHDL generation**: ultra-fast development
Concluding thoughts

- **Characteristic 3** performs slightly better than characteristic 2
  - at least on our unified architecture
  - good overall performances vouch for stronger confidence in this observation
  - not true anymore on parallel architectures: the battle is not over!

- **Unified operator**
  - small but also competitively fast
  - parameter $D$ to explore the area-time tradeoff
  - high scalability: support for larger extension degrees and higher levels of security
  - automatic VHDL generation: ultra-fast development

- **Perspectives**
  - parallel architectures (work in progress with N. Cortez-Duarte and N. Estibals)
  - hyperelliptic curves (work in progress with G. Hanrot on genus 2)
  - Ate pairing
  - pairings on Edwards curves
Concluding thoughts

- **Characteristic 3** performs slightly better than **characteristic 2**
  - at least on our **unified architecture**
  - good overall performances vouch for **stronger confidence** in this observation
  - not true anymore on **parallel architectures**: the battle is not over!

- **Unified operator**
  - small but also **competitively fast**
  - parameter $D$ to explore the **area-time tradeoff**
  - high scalability: support for larger extension degrees and **higher levels of security**
  - automatic **VHDL generation**: ultra-fast development

- **Perspectives**
  - parallel architectures (work in progress with N. Cortez-Duarte and N. Estibals)
  - hyperelliptic curves (work in progress with G. Hanrot on genus 2)
  - Ate pairing
  - pairings on **Edwards curves**
  - **AES-128-equivalent security!**
With thanks to our sponsor
Thank you for your attention

Questions?