

Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions

Robert Granger, Michael Scott

`{rgranger,mike}@computing.dcu.ie`
Claude Shannon Institute
Dublin City University
Ireland

CSI Workshop 2010, May 17-18th

Outline

- 1 Motivation and Results
- 2 Method
- 3 Applications

Statement of Problem

Consider \mathbb{F}_{q^n} :

Statement of Problem

Consider \mathbb{F}_{q^n} :

- Given $\alpha \in \mathbb{F}_{q^n}^\times$, what is the fastest way to compute α^2 ?

Statement of Problem

Consider \mathbb{F}_{q^n} :

- Given $\alpha \in \mathbb{F}_{q^n}^\times$, what is the fastest way to compute α^2 ?
- What if α belongs to a proper subgroup of $\mathbb{F}_{q^n}^\times$?

Statement of Problem

Group decomposition of $\mathbb{F}_{q^n}^\times$

The identity $|\mathbb{F}_{q^n}^\times| = q^n - 1 = \prod_{d|n} \Phi_d(q)$, with $\Phi_d(\cdot)$ the d -th cyclotomic polynomial \implies

- $\Phi_d(q) | (q^d - 1)$ and so subgroup of this order embeds into $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$

Statement of Problem

Group decomposition of $\mathbb{F}_{q^n}^\times$

The identity $|\mathbb{F}_{q^n}^\times| = q^n - 1 = \prod_{d|n} \Phi_d(q)$, with $\Phi_d(\cdot)$ the d -th cyclotomic polynomial \implies

- $\Phi_d(q) | (q^d - 1)$ and so subgroup of this order embeds into $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$

Definition

The **Cyclotomic Subgroup** (w.r.t. $\mathbb{F}_{q^n}/\mathbb{F}_q$) of $\mathbb{F}_{q^n}^\times$ is

$$G_{\Phi_n(q)} = \{\alpha \in \mathbb{F}_{q^n} \mid \alpha^{\Phi_n(q)} = 1\}$$

Statement of Problem

Group decomposition of $\mathbb{F}_{q^n}^\times$

The identity $|\mathbb{F}_{q^n}^\times| = q^n - 1 = \prod_{d|n} \Phi_d(q)$, with $\Phi_d(\cdot)$ the d -th cyclotomic polynomial \implies

- $\Phi_d(q) | (q^d - 1)$ and so subgroup of this order embeds into $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$

Definition

The **Cyclotomic Subgroup** (w.r.t. $\mathbb{F}_{q^n}/\mathbb{F}_q$) of $\mathbb{F}_{q^n}^\times$ is

$$G_{\Phi_n(q)} = \{\alpha \in \mathbb{F}_{q^n} \mid \alpha^{\Phi_n(q)} = 1\}$$

- **Question:** Can one square elements of $G_{\Phi_n(q)}$ faster than one can square elements of \mathbb{F}_{q^n} ?

Motivation

Pairing-based Cryptography (PBC)

- PBC requires an efficiently computable, non-degenerate bilinear pairing

$$e_r : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

- *Security* necessitates hard DLP in each of \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_T
- *Efficiency* necessitates fast arithmetic in \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_T

Motivation

PBC - Security

- Instantiations of pairings typically have the form

$$e_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \rightarrow \mu_r \in \mathbb{F}_{p^k}^\times$$

- Matching DLP security in \mathbb{G}_1 and \mathbb{G}_T [KM05]:

| | | | | |
|----------------|------|------|-----------------|-------|
| security level | 80 | 128 | 192 | 256 |
| b_r | 160 | 256 | 384 | 512 |
| b_{p^k} | 1024 | 3072 | 8192 | 15360 |
| b_{p^k}/b_r | 6.4 | 12 | $21\frac{1}{3}$ | 30 |

- $\implies k \approx 6, 12, 18, 24, 30, 36$ depending on $\rho = \log p / \log r$

Motivation

PBC - Efficiency

- $2 \mid k \implies$ can use quadratic twist for \mathbb{G}_2
- $4 \mid k \implies$ can use quartic twist for \mathbb{G}_2
- $6 \mid k \implies$ can use sextic twist for \mathbb{G}_2

Motivation

PBC - Efficiency

- $2 \mid k \implies$ can use quadratic twist for \mathbb{G}_2
- $2 \mid k \implies$ can compress pairings by factor of 2

- $4 \mid k \implies$ can use quartic twist for \mathbb{G}_2
- $4 \mid k \implies$ can compress pairings by factor of 2

- $6 \mid k \implies$ can use sextic twist for \mathbb{G}_2
- $6 \mid k \implies$ can compress pairings by factor of 3

Motivation

PBC - Efficiency

- $2 \mid k \implies$ can use quadratic twist for \mathbb{G}_2
- $2 \mid k \implies$ can compress pairings by factor of 2
- $2 \mid k \implies$ can square fast in \mathbb{G}_T

- $4 \mid k \implies$ can use quartic twist for \mathbb{G}_2
- $4 \mid k \implies$ can compress pairings by factor of 2
- $4 \mid k \implies$ can square fast in \mathbb{G}_T

- $6 \mid k \implies$ can use sextic twist for \mathbb{G}_2
- $6 \mid k \implies$ can compress pairings by factor of 3
- $6 \mid k \implies$ can square very fast in \mathbb{G}_T (this work)

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in G_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in G_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

- We present a method to compute α^2 twice as fast as that for squaring general elements of \mathbb{F}_{q^6}

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in G_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

- We present a method to compute α^2 twice as fast as that for squaring general elements of \mathbb{F}_{q^6}
- For $q = p, p^2, p^3, p^4$ this is between 2/3-rds and 3/4's the cost of previous best method [SL03]

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in G_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

- We present a method to compute α^2 twice as fast as that for squaring general elements of \mathbb{F}_{q^6}
- For $q = p, p^2, p^3, p^4$ this is between 2/3-rds and 3/4's the cost of previous best method [SL03]

Result applies to:

- 'Final-powering' in pairing computations

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in \mathbf{G}_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

- We present a method to compute α^2 twice as fast as that for squaring general elements of \mathbb{F}_{q^6}
- For $q = p, p^2, p^3, p^4$ this is between 2/3-rds and 3/4's the cost of previous best method [SL03]

Result applies to:

- 'Final-powering' in pairing computations
- Post-pairing arithmetic

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in \mathbf{G}_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

- We present a method to compute α^2 twice as fast as that for squaring general elements of \mathbb{F}_{q^6}
- For $q = p, p^2, p^3, p^4$ this is between 2/3-rds and 3/4's the cost of previous best method [SL03]

Result applies to:

- 'Final-powering' in pairing computations
- Post-pairing arithmetic
- Torus-Based Cryptography

Main Result

For $q \equiv 1 \pmod{6}$, let $\alpha \in \mathbf{G}_{\Phi_6(q)} \subset \mathbb{F}_{q^6}^\times$:

- We present a method to compute α^2 twice as fast as that for squaring general elements of \mathbb{F}_{q^6}
- For $q = p, p^2, p^3, p^4$ this is between 2/3-rds and 3/4's the cost of previous best method [SL03]

Result applies to:

- 'Final-powering' in pairing computations
- Post-pairing arithmetic
- Torus-Based Cryptography
- Fields in IEEE 'Draft Standard for Identity-Based Public Key Cryptography using Pairings' (P1363.3/D1)

Pairing-Friendly Fields

Simplification of PBC Treatment

Koblitz and Menezes introduced the following [KM05]:

- Let $p \equiv 1 \pmod{12}$ and $k = 2^a 3^b$ for $a \geq 1$ and $b \geq 0$.
Then \mathbb{F}_{p^k} is known as a Pairing-Friendly Field (PFF)

Pairing-Friendly Fields

Simplification of PBC Treatment

Koblitz and Menezes introduced the following [KM05]:

- Let $p \equiv 1 \pmod{12}$ and $k = 2^a 3^b$ for $a \geq 1$ and $b \geq 0$.
Then \mathbb{F}_{p^k} is known as a Pairing-Friendly Field (PFF)
- We restrict to \mathbb{F}_{p^k} with $k = 2^a 3^b$ with $a, b \geq 1$, so that $6 \mid k$.
Then:

$$\Phi_{2^a 3^b}(x) = x^{2 \cdot 2^{a-1} 3^{b-1}} - x^{2^{a-1} 3^{b-1}} + 1$$

Pairing-Friendly Fields

Simplification of PBC Treatment

Koblitz and Menezes introduced the following [KM05]:

- Let $p \equiv 1 \pmod{12}$ and $k = 2^a 3^b$ for $a \geq 1$ and $b \geq 0$. Then \mathbb{F}_{p^k} is known as a Pairing-Friendly Field (PFF)
- We restrict to \mathbb{F}_{p^k} with $k = 2^a 3^b$ with $a, b \geq 1$, so that $6 \mid k$. Then:

$$\Phi_{2^a 3^b}(x) = x^{2 \cdot 2^{a-1} 3^{b-1}} - x^{2^{a-1} 3^{b-1}} + 1$$

- Note that $\Phi_{2^a 3^b}(x) = \Phi_6(x^{2^{a-1} 3^{b-1}})$ and hence

$$G_{\Phi_k(p)} = G_{\Phi_6(p^{k/6})}$$

Pairing-Friendly Fields

Simplification of PBC Treatment

Koblitz and Menezes introduced the following [KM05]:

- Let $p \equiv 1 \pmod{12}$ and $k = 2^a 3^b$ for $a \geq 1$ and $b \geq 0$. Then \mathbb{F}_{p^k} is known as a Pairing-Friendly Field (PFF)
- We restrict to \mathbb{F}_{p^k} with $k = 2^a 3^b$ with $a, b \geq 1$, so that $6 \mid k$. Then:

$$\Phi_{2^a 3^b}(x) = x^{2 \cdot 2^{a-1} 3^{b-1}} - x^{2^{a-1} 3^{b-1}} + 1$$

- Note that $\Phi_{2^a 3^b}(x) = \Phi_6(x^{2^{a-1} 3^{b-1}})$ and hence

$$G_{\Phi_k(p)} = G_{\Phi_6(p^{k/6})}$$

- So we need only consider $G_{\Phi_6(q)}$ with $q = p^{k/6}$

Weil Restriction of Scalars

- The condition $\alpha^{\Phi_k(\rho)} = 1$ defines a variety V over \mathbb{F}_{p^k}

Weil Restriction of Scalars

- The condition $\alpha^{\Phi_k(\rho)} = 1$ defines a variety V over \mathbb{F}_{p^k}
- For $d \mid k$ one can consider the same equation over \mathbb{F}_{p^d}

Weil Restriction of Scalars

- The condition $\alpha^{\Phi_k(\rho)} = 1$ defines a variety V over \mathbb{F}_{p^k}
- For $d \mid k$ one can consider the same equation over \mathbb{F}_{p^d}
- We write $\text{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V$ for the Weil restriction of scalars of V from \mathbb{F}_{p^k} to \mathbb{F}_{p^d}

Weil Restriction of Scalars

- The condition $\alpha^{\Phi_k(\rho)} = 1$ defines a variety V over \mathbb{F}_{p^k}
- For $d \mid k$ one can consider the same equation over \mathbb{F}_{p^d}
- We write $\text{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V$ for the Weil restriction of scalars of V from \mathbb{F}_{p^k} to \mathbb{F}_{p^d}
- $\text{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V$ is a variety defined over \mathbb{F}_{p^d} and we have an isomorphism

$$\eta : (\text{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V)(\mathbb{F}_{p^d}) \rightarrow V(\mathbb{F}_{p^k})$$

Weil Restriction of Scalars

In previous work

- Stam-Lenstra restrict $G_{\Phi_2(\rho)}$ from \mathbb{F}_{p^2} to \mathbb{F}_p [SL03]
- Stam-Lenstra restrict $G_{\Phi_6(\rho)}$ from \mathbb{F}_{p^6} to \mathbb{F}_p [SL03]
- G.-Page-Smart restrict $G_{\Phi_k(\rho)}$ from \mathbb{F}_{p^k} to \mathbb{F}_p [GPS06]

Fast squaring in $\text{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q} G_{\Phi_2(q)}$ - [SL03]

- Let $\mathbb{F}_{q^2} = \mathbb{F}_q[x]/(x^2 - i)$ with i a quadratic non-residue in \mathbb{F}_q , and consider the square of a generic element $\alpha = a + bx$:

$$\begin{aligned}\alpha^2 &= (a + xb)^2 = a^2 + 2abx + b^2x^2 = a^2 + ib^2 + 2abx \\ &= (a + ib)(a + b) - ab(1 + i) + 2abx\end{aligned}$$

- If $\alpha \in G_{\Phi_2(q)}$, we have $\alpha^{q+1} = 1$, or $\alpha^q \cdot \alpha = 1$. Observe that since i is a quadratic non-residue:

$$\begin{aligned}\alpha^q &= (a + xb)^q = a + bx^q = a + bx^{2(q-1)/2} \cdot x \\ &= a + bi^{(q-1)/2} \cdot x = a - bx\end{aligned}$$

Fast squaring in $\text{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q} G_{\Phi_2}(q)$ - [SL03]

- Hence variety defined by single \mathbb{F}_q equation:

$$(a + xb)(a - xb) = 1, \text{ or } a^2 - x^2b^2 = 1, \text{ or } a^2 - ib^2 = 1$$

- Substituting from this equation into the squaring formula, one obtains

$$\alpha^2 = (a + xb)^2 = 2a^2 - 1 + [(a + b)^2 - a^2 - (a^2 - 1)/i]x$$

- Main cost of computing this is just two \mathbb{F}_q -squarings.
- Observe that if i is 'small' (for example if $i = -1$ for $p \equiv 3 \pmod{4}$) when $\mathbb{F}_q = \mathbb{F}_p$, then the above simplifies

Where to next?

- First [SL03] result equivalently considers $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}} G_{\Phi_2(q^3)}$
- Since $\Phi_6(q) \mid \Phi_2(q^3)$, this method applies to $G_{\Phi_6(q)}$, but has some redundancy
- Second [SL03] result restricts $G_{\Phi_6(q)}$ from \mathbb{F}_{q^6} to \mathbb{F}_q , but for $q \equiv 2$ or $5 \pmod{9}$, so can't be used with sextic twists
- [GPS06] restrict from \mathbb{F}_{q^k} to \mathbb{F}_q , but complicated and slower than from \mathbb{F}_{q^6} to \mathbb{F}_{q^3}

Where to next?

- First [SL03] result equivalently considers $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}} G_{\Phi_2(q^3)}$
- Since $\Phi_6(q) \mid \Phi_2(q^3)$, this method applies to $G_{\Phi_6(q)}$, but has some redundancy
- Second [SL03] result restricts $G_{\Phi_6(q)}$ from \mathbb{F}_{q^6} to \mathbb{F}_q , but for $q \equiv 2$ or $5 \pmod{9}$, so can't be used with sextic twists
- [GPS06] restrict from \mathbb{F}_{q^k} to \mathbb{F}_q , but complicated and slower than from \mathbb{F}_{q^6} to \mathbb{F}_{q^3}

Obvious next step is to restrict from \mathbb{F}_{q^6} to \mathbb{F}_{q^2} ...

Fast squaring in $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$

- Let $\mathbb{F}_{q^6} = \mathbb{F}_q[z]/(z^6 - i)$, with $i \in \mathbb{F}_q$ a sextic non-residue
- Standard representation for an element of $\mathbb{F}_{q^6}/\mathbb{F}_q$ is

$$\alpha = \alpha_0 + \alpha_1 z + \alpha_2 z^2 + \alpha_3 z^3 + \alpha_4 z^4 + \alpha_5 z^5$$

- In order to make the subfield structure explicit, we write elements of \mathbb{F}_{q^6} in two possible ways:
 - As a compositum of \mathbb{F}_{q^2} and \mathbb{F}_{q^3}
 - As a cubic extension of a quadratic extension of \mathbb{F}_q

Fast squaring in $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$ \mathbb{F}_{q^6} as a compositum

- Let $\mathbb{F}_{q^2} = \mathbb{F}_q[y]/(y^2 - i)$ and $\mathbb{F}_{q^3} = \mathbb{F}_q[x]/(x^3 - i)$ and hence $y = z^3$, $x = z^2$
- $\alpha = (a_0 + a_1 y) + (b_0 + b_1 y)x + (c_0 + c_1 y)x^2 = a + bx + cx^2$
- We thus have

$$\mathbb{F}_{q^6} = \mathbb{F}_q(z) = \mathbb{F}_{q^3}(y) = \mathbb{F}_{q^2}(x)$$

- Viewing α in the latter form its square is $(a + bx + cx^2)^2$

$$= a^2 + 2abx + (2ac + b^2)x^2 + 2bcx^3 + c^2x^4$$

$$= (a^2 + 2ibc) + (2ab + ic^2)x + (2ac + b^2)x^2$$

$$= A + Bx + Cx^2$$

Fast squaring in $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$ \mathbb{F}_{q^6} as a compositum

- As $\alpha \in G_{\Phi_6}$ we have $\alpha^{q^2-q+1} = 1$
- To restrict to \mathbb{F}_{q^2} , compute Frobenius action on basis:

$$y^q = y^{2(q-1)/2} \cdot y = i^{(q-1)/2} \cdot y = -y,$$

hence $a^q = (a_0 + a_1 y)^q = a_0 - a_1 y$, which for simplicity we write as \bar{a} , and similarly for \bar{b} , \bar{c} ;

- Let ω is a primitive cube root of unity in \mathbb{F}_q . Then

$$x^q = x^{3(q-1)/3} \cdot x = i^{(q-1)/3} \cdot x = \omega x$$

- Applying the Frobenius again gives $x^{q^2} = \omega^2 x$

Fast squaring in $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$

\mathbb{F}_{q^6} as a compositum

- Rewriting $\alpha^{q^2-q+1} = 1$ as $\alpha^{q^2} \cdot \alpha = \alpha^q$ gives:

$$(a + b\omega^2x + c\omega^4x^2)(a + bx + cx^2) = \bar{a} + \bar{b}\omega x + \bar{c}\omega^2x^2,$$

- Upon expanding, reducing modulo $x^3 - i$, and modulo $\Phi_3(\omega) = \omega^2 + \omega + 1$, this becomes

$$(a^2 - \bar{a} - bci) + \omega(ic^2 - \bar{b} - ab)x + \omega^2(b^2 - \bar{c} - ac)x^2 = 0$$

- This equation defines the variety $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$, as each \mathbb{F}_{q^2} coefficient of x^i equals zero.

Fast squaring in $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$ \mathbb{F}_{q^6} as a compositum

- Solving for bc , ab , ac , one obtains:

$$bc = (a^2 - \bar{a})/i$$

$$ab = ic^2 - \bar{b}$$

$$ac = b^2 - \bar{c}$$

- Substituting these into the original squaring formula gives

$$A = a^2 + 2ibc = a^2 + 2i(a^2 - \bar{a})/i = 3a^2 - 2\bar{a}$$

$$B = ic^2 + 2ab = ic^2 + 2(ic^2 - \bar{b}) = 3ic^2 - 2\bar{b}$$

$$C = b^2 + 2ac = b^2 + 2(b^2 - \bar{c}) = 3b^2 - 2\bar{c}$$

Fast squaring in $\text{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6}(q)$

\mathbb{F}_{q^6} as a tower extension

- Let $\mathbb{F}_{q^2} = \mathbb{F}_q[y]/(y^2 - i)$ and $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[x]/(x^3 - \sqrt{i})$ and hence $y = z^3$, $x = z$
- $\alpha = (a_0 + a_1 y) + (b_0 + b_1 y)x + (c_0 + c_1 y)x^2 = a + bx + cx^2$
- Similar argument with a primitive sixth root of unity gives:

$$A = 3a^2 - 2\bar{a}$$

$$B = 3\sqrt{i}c^2 + 2\bar{b}$$

$$C = 3b^2 - 2\bar{c}$$

Comparison with Prior Work

Operation counts for squaring in Weil restrictions of $G_{\Phi_k}(q)$:

| k | \mathbb{F}_{q^k} | $\text{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_{q^{k/2}}} G_{\Phi_2}(q^{k/2})$ [SL03] | $\text{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_{q^{k/3}}} G_{\Phi_6}(q^{k/6})$ (Present result) | $\text{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_q} G_{\Phi_6}(q^{k/6})$ [GPS06] |
|-----|--------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 6 | $12m$ | $2S_3 = 4m + 6s$ | $3S_2 = 6m$ | $3m + 6s$ |
| 12 | $36m$ | $2S_6 = 24m$ | $3S_4 = 18m$ | $18m + 12s$ |
| 18 | $72m$ | $2S_9 = 24m + 30s$ | $3S_6 = 36m$ | |
| 24 | $108m$ | $2S_{12} = 72m$ | $3S_8 = 54m$ | $84m + 24s$ |

Barreto-Naehrig Curves [BN05]

- These are elliptic curves $E/\mathbb{F}_p : y^2 = x^3 + b$ with embedding degree 12 for which

$$p(t) = 36t^4 + 36t^3 + 24t^2 + 6t + 1$$

$$r(t) = 36t^4 + 36t^3 + 18t^2 + 6t + 1$$

$$tr(t) = 6t^2 + 1$$

- Odd $t \implies p \equiv 3 \pmod{4}$ and so $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2 + 1)$
- $p^2 \equiv 1 \pmod{6}$ hence apply our construction for $\mathbb{F}_{p^{12}}/\mathbb{F}_{p^2}$
- For ‘final powering’ using Scott et al.’s method [SBCPK09]: [SL03] costs $5971m$, our method costs $4856m$

Torus-Based Cryptography (TBC)

- TBC is cryptography based in $T_k(\mathbb{F}_q) \cong G_{\Phi_k(q)}$
- Uses rationality of algebraic torus to compress elements - best factor is 3 for $6 \mid k$
- For $\alpha = (a_0 + a_1x + a_2x^2) + (b_0 + b_1x + b_2x^2)y = a + by$ using compositum representation and $p \equiv 1 \pmod{6}$ let

$$c = -(a + 1)/b = c_0 + c_1x + c_2x^2$$

- Then (c_0, c_1) represents α with inverse

$$\begin{aligned} \psi : \mathbb{A}^2(\mathbb{F}_q) &\rightarrow T_6(\mathbb{F}_q) \setminus \{1\} : \\ (c_0, c_1 \neq 0) &\mapsto \frac{3ic_0c_1 + 3ic_1^2x + (3c_0^2 + i)x^2 - 3ic_1y}{3ic_0c_1 + 3ic_1^2x + (3c_0^2 + i)x^2 + 3ic_1y} \end{aligned}$$

Other Considerations

- Weil restriction framework applies to any k and $d \mid k$ - for PBC extension degrees our squaring method is best

Other Considerations

- Weil restriction framework applies to any k and $d \mid k$ - for PBC extension degrees our squaring method is best
- Higher powerings?
 - Possible eg., $\alpha^{\Phi_3(q)} = 1$ aids in cubing but slower than squaring
 - Degree of $\alpha^{\Phi_k(q)} = 1$ when expanded is ≤ 2 only for $k = 2^a 3^b$ for $a \geq 1, b \geq 0$
 - Hence fields with these extension degrees ideally suited to our squaring method

Summary

Our method:

- Provides the fastest available squaring in $G_{\Phi_6(q)}$ and for PBC fields
- Is conceptually easy and permits generalisation
- Is highly applicable - only requires $q \equiv 1 \pmod{6}$ so applies to 3/4's finite fields
- Ideal for TBC - allows fast maximal compression (assuming $p \equiv 1 \pmod{6}$) and fastest squaring
- Applies to fields in IEEE P1363.3/D1 and so gives a compelling argument for their adoption