Cyclotomic Subgroups in Cryptography

ECC '05

Martijn Stam

Department of Computer Science, University of Bristol

20 September 2005

Outline

Outline

DLP-based Cryptosystems

- Let g generate cyclic group G_q of order q.
  Discrete Logarithm Problem (DLP):
  Given $A \in \mathrm{G}_q$, determine $0 \leq a < q$ s.t. $g^a = A$.

DLP-based Cryptosystems

- Let g generate cyclic group G_q of order q.
  Discrete Logarithm Problem (DLP):
  Given $A \in G_q$, determine $0 \leq a < q$ s.t. $g^a = A$.
- Most common choices for G_q
  Finite Fields Subgroup $G_q \subseteq \mathbb{F}_{p^n}^*$ of a finite field.
  Elliptic Curves Subgroup $G_q \subseteq E(\mathbb{F}_{p^n})$ of an elliptic curve.

DLP-based Cryptosystems

- Let g generate cyclic group G_q of order q.
  Discrete Logarithm Problem (DLP):
  Given $A \in \mathrm{G}_q$, determine $0 \leq a < q$ s.t. $g^a = A$.
- Most common choices for G_q
  Finite Fields Subgroup $\mathrm{G}_q \subseteq \mathbb{F}_{p^n}^*$ of a finite field.
  Elliptic Curves Subgroup $\mathrm{G}_q \subseteq E(\mathbb{F}_{p^n})$ of an elliptic curve.
- Pairing provides the connection. A bilinear map

$$e : E(\mathbb{F}_{p^n}) \times E(\mathbb{F}_{p^n}) \to \mathbb{F}_{p^{kn}}^*$$

preserving lots of structure.

Outline

Structure of Finite Fields

Some Notation

- Euler totient function $\phi(n)$
  The number of integers f with $0 < f \leq n$ coprime to n.

Structure of Finite Fields

Some Notation

- Euler totient function $\phi(n)$
  The number of integers f with $0 < f \leq n$ coprime to n.
- Cyclotomic Polynomials.
  $\Phi_d(p)$ is the d-th cyclotomic polynomial.

d	$\Phi_d(p)$
1	$p-1$
2	$p+1$
3	p^2+p+1
4	p^2+1
5	$p^4+p^3+p^2+p+1$
6	p^2-p+1

Finite Field Representation

- The multiplicative group $\mathbb{F}_{p^n}^*$ is cyclic and has cardinality $p^n - 1$, where

$$p^n - 1 = \prod_{d|n} \Phi_d(p)$$

Finite Field Representation

- The multiplicative group $\mathbb{F}_{p^n}^*$ is cyclic and has cardinality $p^n - 1$, where

$$p^n - 1 = \prod_{d|n} \Phi_d(p)$$

- Let $T_d(\mathbb{F}_{p^e}) \subset \mathbb{F}_{p^n}^*$ with $de|n$ be subgroup of order $\Phi_d(p^e)$.

Finite Field Representation

- The multiplicative group $\mathbb{F}_{p^6}^*$ is cyclic and has cardinality $p^6 - 1$, where

$$p^6 - 1 = \prod_{d|6} \Phi_d(p)$$

- Let $T_d(\mathbb{F}_{p^e}) \subset \mathbb{F}_{p^6}^*$ with $de|6$ be subgroup of order $\Phi_d(p^e)$.

Finite Field Representation

- The multiplicative group $\mathbb{F}_{p^6}^*$ is cyclic and has cardinality $p^6 - 1$, where

$$p^6 - 1 = \underbrace{(p-1)}_{T_1(\mathbb{F}_p)} \; \underbrace{(p+1)}_{T_2(\mathbb{F}_p)} \; \underbrace{(p^2+p+1)}_{T_3(\mathbb{F}_p)} \; \underbrace{(p^2-p+1)}_{T_6(\mathbb{F}_p)}$$

- For $de|6$, let $T_d(\mathbb{F}_{p^e}) \subset \mathbb{F}_{p^6}^*$ be subgroup of order $\Phi_d(p^e)$.

Finite Field Representation

- The multiplicative group $\mathbb{F}_{p^6}^*$ is cyclic and has cardinality $p^6 - 1$, where

$$p^6 - 1 = \underbrace{(p-1)\quad(p+1)}_{T_1(\mathbb{F}_{p^2})}\quad(p^2+p+1)\quad(p^2-p+1)$$

- For $de|6$, let $T_d(\mathbb{F}_{p^e}) \subset \mathbb{F}_{p^6}^*$ be subgroup of order $\Phi_d(p^e)$.
- Combinations are also possible.

Finite Field Representation

- The multiplicative group $\mathbb{F}_{p^6}^*$ is cyclic and has cardinality $p^6 - 1$, where

$$p^6 - 1 = \quad (p-1) \quad (p+1) \quad \underbrace{(p^2+p+1) \quad (p^2-p+1)}_{T_2(\mathbb{F}_{p^3})}$$

- For $de|6$, let $T_d(\mathbb{F}_{p^e}) \subset \mathbb{F}_{p^6}^*$ be subgroup of order $\Phi_d(p^e)$.
- Combinations are also possible.

Outline

Security

Attacking the DLP

Index Calculus in Full Field: DLP in $\mathbb{F}_{p^n}$ is assumed to be as hard as $n \log_2 p$ bit prime DLP:

$$n \log_2 p > 1024$$

Pohlig-Hellman: Necessity: prevent working in a subfield of $\mathbb{F}_{p^n}$, work in subgroup of prime order in the cyclotomic subgroup.

$$\mathrm{G}_q \subseteq T_n(\mathbb{F}_p) \subseteq \mathbb{F}_{p^n}^*$$

Pollard ρ: Attacks G_q without using structure in $O(\sqrt{q})$.

$$\log_2 q > 160$$

Security
Attacking the DLP

Index Calculus in Full Field: DLP in $\mathbb{F}_{p^n}$ is assumed to be as hard as $n \log_2 p$ bit prime DLP:

$$n \log_2 p > 1024$$

Pohlig-Hellman: Necessity: prevent working in a subfield of $\mathbb{F}_{p^n}$, work in subgroup of prime order in the cyclotomic subgroup.

$$\mathrm{G}_q \subseteq T_n(\mathbb{F}_p) \subseteq \mathbb{F}_{p^n}^*$$

Pollard ρ: Attacks G_q without using structure in $O(\sqrt{q})$.

$$\log_2 q > 160$$

Index Calculus in Torus: (Granger and Vercauteren, Crypto'05) Exponential in p, but for some parameters beats Pollard ρ.

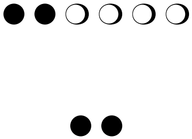
Compression

- Standard way of representing $\mathbb{F}_{p^6}^*$ with 6 elts in $\mathbb{F}_p$.

Compression

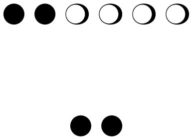
- Standard way of representing $\mathbb{F}_{p^6}^*$ with 6 elts in $\mathbb{F}_p$.
- However, $T_6(\mathbb{F}_p) \subset \mathbb{F}_{p^6}^*$ is considerably smaller.

Compression



- Standard way of representing $\mathbb{F}_{p^6}^*$ with 6 elts in $\mathbb{F}_p$.
- However, $T_6(\mathbb{F}_p) \subset \mathbb{F}_{p^6}^*$ is considerably smaller.
- Can't we represent using only 2 elts in $\mathbb{F}_p$?

Compression



- Standard way of representing $\mathbb{F}_{p^6}^*$ with 6 elts in $\mathbb{F}_p$.
- However, $T_6(\mathbb{F}_p) \subset \mathbb{F}_{p^6}^*$ is considerably smaller.
- Can't we represent using only 2 elts in $\mathbb{F}_p$?
- More general: Represent $T_n(\mathbb{F}_p)$ with $\mathbb{A}^{\phi(n)}(\mathbb{F}_p)$ giving compression factor $n/\phi(n)$.

Efficiency

Single exponentiation

Compute $A = g^a$, given $g \in G_q$ and $a \in \mathbb{Z}_q$.

Double exponentiation

Compute $g^a h^b$, given $g, h \in G_q$ and $a, b \in \mathbb{Z}_q$.

Compression and Decompression

Outline

LUC

Smith and Skinner

$$\mathbb{F}^*_{p^2} \xrightarrow{\supset} \mathbb{G}_{p+1}$$

LUC

Smith and Skinner

Let $\mathrm{Tr} : \mathbb{F}_{p^2} \to \mathbb{F}_p, \mathrm{Tr}(g) = g^p + g$.

$$\mathbb{F}_{p^2}^* \xrightarrow{\supset} G_{p+1}/\sigma \xrightarrow{\mathrm{Tr}} \mathbb{F}_p$$

LUC

Smith and Skinner

Let $\mathrm{Tr}\ : \mathbb{F}_{p^2} \to \mathbb{F}_p, \mathrm{Tr}\,(g) = g^p + g$.

$$\mathbb{F}_{p^2}^* \xleftarrow{\ \supset\ } \mathsf{G}_{p+1}/\sigma \xleftarrow{\ \mathrm{Tr}^{-1}\ } \mathbb{F}_p$$

$$\mathbb{F}_{p^2}^* \xrightarrow{\ \supset\ } \mathsf{G}_{p+1}/\sigma \xrightarrow{\ \mathrm{Tr}\ } \mathbb{F}_p$$

LUC

Smith and Skinner

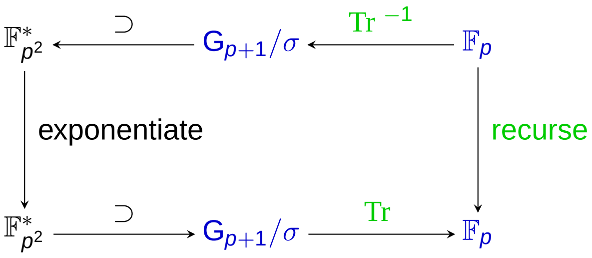
Let $\mathrm{Tr} : \mathbb{F}_{p^2} \to \mathbb{F}_p$, $\mathrm{Tr}(g) = g^p + g$.

$$
\begin{array}{ccccc}
\mathbb{F}_{p^2}^* & \xleftarrow{\supset} & \mathsf{G}_{p+1}/\sigma & \xleftarrow{\mathrm{Tr}^{-1}} & \mathbb{F}_p \\
\downarrow \text{exponentiate} & & & & \\
\mathbb{F}_{p^2}^* & \xrightarrow{\supset} & \mathsf{G}_{p+1}/\sigma & \xrightarrow{\mathrm{Tr}} & \mathbb{F}_p
\end{array}
$$

LUC

Smith and Skinner

Let $\mathrm{Tr} : \mathbb{F}_{p^2} \to \mathbb{F}_p, \mathrm{Tr}(g) = g^p + g$.



Let $g \in \mathrm{G}_{p+1}$ and $v_a = \mathrm{Tr}(g^a)$ then

$$v_{a+b} = v_a v_b - v_{a-b}$$

LUC

Smith and Skinner

Let $\mathrm{Tr} : \mathbb{F}_{p^2} \to \mathbb{F}_p, \mathrm{Tr}(g) = g^p + g$.

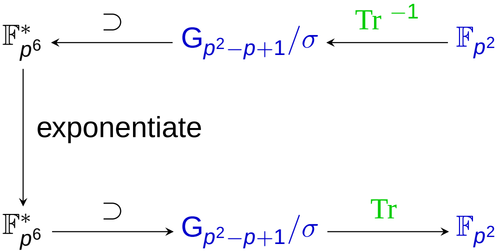
$$
\begin{array}{ccccc}
\mathbb{F}_{p^2}^* & \xleftarrow{\supset} & G_{p+1}/\sigma & \xleftarrow{\mathrm{Tr}^{-1}} & \mathbb{F}_p \\
\downarrow \text{exponentiate} & & & & \downarrow \text{recurse} \\
\mathbb{F}_{p^2}^* & \xrightarrow{\supset} & G_{p+1}/\sigma & \xrightarrow{\mathrm{Tr}} & \mathbb{F}_p
\end{array}
$$

- **Pro** Gives factor 2 compression
- **Pro** Faster than field exponentiation.
- **Con** Conjugacy problems (σ)

XTR

Lenstra and Verheul (Crypto 2000)

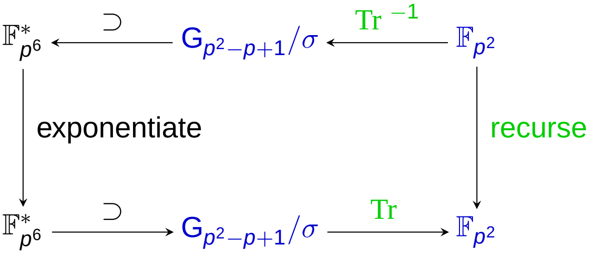
Let $\mathrm{Tr} : \mathbb{F}_{p^6} \to \mathbb{F}_{p^2}, \mathrm{Tr}(g) = g^{p^4} + g^{p^2} + g.$



XTR

Lenstra and Verheul (Crypto 2000)

Let $\mathrm{Tr} : \mathbb{F}_{p^6} \to \mathbb{F}_{p^2}, \mathrm{Tr}(g) = g^{p^4} + g^{p^2} + g$.



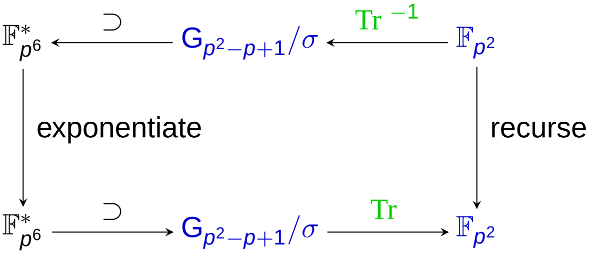
Let $g \in \mathrm{G}_{p^2-p+1}$ and $c_a = \mathrm{Tr}(g^a)$ then

$$c_{a+b} = c_a c_b - c_b^p c_{a-b} + c_{a-2b}$$

XTR

Lenstra and Verheul (Crypto 2000)

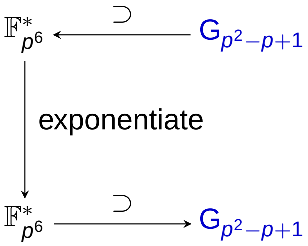
Let $\mathrm{Tr}: \mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$, $\mathrm{Tr}(g) = g^{p^4} + g^{p^2} + g$.



- **Pro** Gives factor 3 compression
- **Pro** Three times faster than field exponentiation
- **Con** Conjugacy problems (σ)

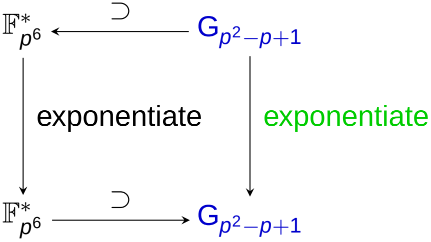
HEX

Stam and Lenstra (2002)



HEX

Stam and Lenstra (2002)



Pro Three times faster than field exponentiation

Con No compression.

Outline

The Algebraic Torus

- The algebraic torus $T_n(\mathbb{F}_{p^e})$ is defined as

$$T_n(\mathbb{F}_{p^e}) = \bigcap_{d|n, d\neq n} \mathrm{Ker}\,[N_{\mathbb{F}_{p^{ne}}/\mathbb{F}_{p^{de}}}]$$

- $T_n(\mathbb{F}_p)$ is the subgroup of $\mathbb{F}^*_{p^n}$ of cardinality $\Phi_n(p)$.

The Algebraic Torus

- The algebraic torus $T_n(\mathbb{F}_{p^e})$ is defined as

$$T_n(\mathbb{F}_{p^e}) = \bigcap_{d|n, d \neq n} \mathrm{Ker}\, [N_{\mathbb{F}_{p^{ne}}/\mathbb{F}_{p^{de}}}]$$

- $T_n(\mathbb{F}_p)$ is the subgroup of $\mathbb{F}_{p^n}^*$ of cardinality $\Phi_n(p)$.
- Rationality of torus implies efficient almost bijection with $\mathbb{A}^{\phi(n)}(\mathbb{F}_p)$.

The Algebraic Torus

- The algebraic torus $T_n(\mathbb{F}_{p^e})$ is defined as

$$T_n(\mathbb{F}_{p^e}) = \bigcap_{d|n, d \neq n} \text{Ker}\,[N_{\mathbb{F}_{p^{ne}}/\mathbb{F}_{p^{de}}}]$$

- $T_n(\mathbb{F}_p)$ is the subgroup of $\mathbb{F}_{p^n}^*$ of cardinality $\Phi_n(p)$.
- Rationality of torus implies efficient almost bijection with $\mathbb{A}^{\phi(n)}(\mathbb{F}_p)$.
- Algebraic torus known to be rational for n the product of two prime powers. So 6 yes, but 30 unknown.

The Quotient Group for $T_2(\mathbb{F}_p) = \mathrm{G}_{p+1}$

Rubin and Silverberg

$$\mathrm{Pow} : \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \to \mathrm{G}_{p+1}, \mathrm{Pow}(g) = g^{p-1}$$

$$\begin{array}{ccccc}
\mathbb{F}_{p^2}^* & \xleftarrow{\supset} & \mathrm{G}_{p+1} & \xleftarrow{\mathrm{Pow}} & \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \\
\downarrow \text{exponentiate} & & & & \downarrow \text{exponentiate} \\
\mathbb{F}_{p^2}^* & \xrightarrow{\supset} & \mathrm{G}_{p+1} & \xrightarrow{\mathrm{Pow}^{-1}} & \mathbb{F}_{p^2}^*/\mathbb{F}_p^*
\end{array}$$

The Quotient Group for $T_2(\mathbb{F}_p) = \mathsf{G}_{p+1}$

Rubin and Silverberg

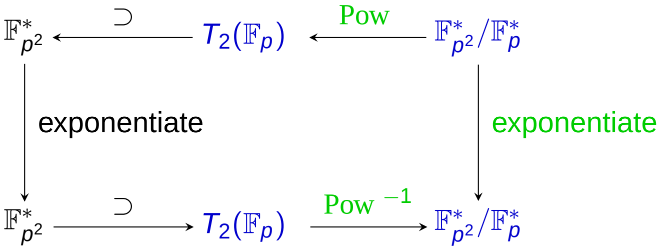
$$\text{Pow} : \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \to \mathsf{G}_{p+1}, \text{Pow}(g) = g^{p-1}$$

$$\begin{array}{ccccc}
\mathbb{F}_{p^2}^* & \xleftarrow{\supset} & T_2(\mathbb{F}_p) & \xleftarrow{\text{Pow}} & \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \\
\downarrow \text{exponentiate} & & & & \downarrow \text{exponentiate} \\
\mathbb{F}_{p^2}^* & \xrightarrow{\supset} & T_2(\mathbb{F}_p) & \xrightarrow{\text{Pow}^{-1}} & \mathbb{F}_{p^2}^*/\mathbb{F}_p^*
\end{array}$$

The Quotient Group for $T_2(\mathbb{F}_p) = \mathsf{G}_{p+1}$

Rubin and Silverberg

$$\mathrm{Pow} : \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \rightarrow \mathsf{G}_{p+1}, \mathrm{Pow}(g) = g^{p-1}$$



- **Pro** Gives factor 2 compression
- **Pro** Full Functionality
- **Pro** Fast mixed coordinate style exponentiaton

CEILIDH

Rubin and Silverberg (Crypto'03)

Compression map $\mathrm{Zip} : T_6(\mathbb{F}_p)\backslash\{1, a\} \to \mathbb{A}^2(\mathbb{F}_p)\backslash T_2(\mathbb{F}_p)$

$$
\begin{array}{ccccc}
\mathbb{F}_{p^6}^* & \xleftarrow{\ \supset\ } & T_6(\mathbb{F}_p) & \xleftarrow{\ \mathrm{Zip}^{-1}\ } & \mathbb{A}^2(\mathbb{F}_p) \\
\Big\downarrow \text{exponentiate} & & & & \\
\mathbb{F}_{p^6}^* & \xrightarrow{\ \text{represents}\ } & T_6(\mathbb{F}_p) & \xrightarrow{\ \mathrm{Zip}\ } & \mathbb{A}^2(\mathbb{F}_p)
\end{array}
$$

Pro Gives factor 2 compression

Pro Full Functionality

Con Seems slow to implement

KYLIE

Granger et al. (ANTS 2004)

The T_2 compression is a substage of CEILIDH.

$$
\begin{array}{ccccc}
G_{p^2-p+1} & \xleftarrow{\mathrm{Pow}} & \mathbb{F}^*_{p^6}/\mathbb{F}^*_{p^3} & \xleftarrow{\frac{1}{2}\mathrm{Zip}^{-1}} & \mathbb{A}^2(\mathbb{F}_p) \\
\downarrow \text{exponentiate} & & \downarrow \text{exponentiate} & & \\
G_{p^2-p+1} & \xrightarrow{\mathrm{Pow}^{-1}} & \mathbb{F}^*_{p^6}/\mathbb{F}^*_{p^3} & \xrightarrow{\frac{1}{2}\mathrm{Zip}} & \mathbb{A}^2(\mathbb{F}_p)
\end{array}
$$

- Pro Gives factor 2 compression
- Pro Full Functionality
- Pro Almost as fast as XTR

Outline

Adding Affinity

Usage by chaining

Given a map

$$f : T_n(\mathbb{F}_p) \longrightarrow \mathbb{A}^{\phi(n)}(\mathbb{F}_p)$$

Adding Affinity

Usage by chaining

Given a map

$$f : T_n(\mathbb{F}_p) \times \mathbb{A}^m(\mathbb{F}_p) \longrightarrow \mathbb{A}^{\phi(n)+m}(\mathbb{F}_p)$$

we can create maps for simultaneous compression

$$f_i : (T_n(\mathbb{F}_p))^i \times \mathbb{A}^m(\mathbb{F}_p) \longrightarrow \mathbb{A}^{i\phi(n)+m}(\mathbb{F}_p)$$

1. $(g_1,$ ●●●●●$) \longrightarrow$ ●●●●●●●

Adding Affinity

Usage by chaining

Given a map

$$f : T_n(\mathbb{F}_p) \times \mathbb{A}^m(\mathbb{F}_p) \longrightarrow \mathbb{A}^{\phi(n)+m}(\mathbb{F}_p)$$

we can create maps for simultaneous compression

$$f_i : (T_n(\mathbb{F}_p))^i \times \mathbb{A}^m(\mathbb{F}_p) \longrightarrow \mathbb{A}^{i\phi(n)+m}(\mathbb{F}_p)$$

1. $(g_1,$ ●●●●●$)$ $\longrightarrow$ ●●●●●●●
2. $(g_2,$ ●●●●●$)$ $\longrightarrow$ ●●●●●●●

Adding Affinity

Usage by chaining

Given a map

$$f : T_n(\mathbb{F}_p) \times \mathbb{A}^m(\mathbb{F}_p) \rightarrow \mathbb{A}^{\phi(n)+m}(\mathbb{F}_p)$$

we can create maps for simultaneous compression

$$f_i : (T_n(\mathbb{F}_p))^i \times \mathbb{A}^m(\mathbb{F}_p) \rightarrow \mathbb{A}^{i\phi(n)+m}(\mathbb{F}_p)$$

1. $(g_1,$ ●●●●●$)$ $\rightarrow$ ●●●●●●●
2. $(g_2,$ ●●●●●$)$ $\rightarrow$ ●●●●●●●
3. $(g_3,$ ●●●●●$)$ $\rightarrow$ ●●●●●●●

$$T_{30}(\mathbb{F}_p) \times \mathbb{A}^2(\mathbb{F}_p) \longrightarrow \mathbb{A}^{10}(\mathbb{F}_p)$$

Van Dijk et al. (Eurocrypt 2005)

Based on equality $\Phi_{30}(p)\Phi_6(p) = \Phi_6(p^5)$

$$T_{30}(\mathbb{F}_p) \times \mathbb{A}^2(\mathbb{F}_p) \xleftarrow{\text{Zip}} T_{30}(\mathbb{F}_p) \times T_6(\mathbb{F}_p) \xleftarrow{\text{unCRT}} T_6(\mathbb{F}_{p^5}) \xleftarrow{\text{Zip}^{-1}} \mathbb{A}^2(\mathbb{F}_{p^5})$$

$$\Big\downarrow \text{exponentiate}$$

$$T_{30}(\mathbb{F}_p) \times \mathbb{A}^2(\mathbb{F}_p) \xrightarrow{\text{Zip}^{-1}} T_{30}(\mathbb{F}_p) \times T_6(\mathbb{F}_p) \xrightarrow{\text{CRT}} T_6(\mathbb{F}_{p^5}) \xrightarrow{\text{Zip}} \mathbb{A}^2(\mathbb{F}_{p^5})$$

- **Pro** Beats Van Dijk and Woodruff (Crypto 2004).
- **Pro** Beats XTR/CEILIDH-compression $\geq$ 2 points.
- **Con** T_{30} susceptible to Rob-Fré attack.

Outline

Pairings

Let $E(\mathbb{F}_{p^m})[q] \subseteq E(\mathbb{F}_{p^m})$ and let $q | p^{km-1}$

- The pairing is a map

$$e_q : E(\mathbb{F}_{p^m})[q] \times E(\mathbb{F}_{p^{km}})[q] \rightarrow \mathbb{F}^*_{p^{km}} / (\mathbb{F}^*_{p^{km}})^q$$

Pairings

Let $E(\mathbb{F}_{p^m})[q] \subseteq E(\mathbb{F}_{p^m})$ and let $q | p^{km-1}$

- The pairing is a map

$$e_q : E(\mathbb{F}_{p^m})[q] \times E(\mathbb{F}_{p^{km}})[q] \longrightarrow \mathbb{F}^*_{p^{km}} / (\mathbb{F}^*_{p^{km}})^q$$

- Easy observation of e_q's range

$$\mathbb{F}^*_{p^{km}} / (\mathbb{F}^*_{p^{km}})^q \simeq \mathrm{G}_q \subseteq T_k(\mathbb{F}_{p^m}) \subseteq \mathbb{F}^*_{p^{km}}$$

Pairings

Let $E(\mathbb{F}_{p^m})[q] \subseteq E(\mathbb{F}_{p^m})$ and let $q | p^{km-1}$

- The pairing is a map

$$e_q : E(\mathbb{F}_{p^m})[q] \times E(\mathbb{F}_{p^{km}})[q] \to \mathbb{F}^*_{p^{km}}/(\mathbb{F}^*_{p^{km}})^q$$

- Easy observation of e_q's range

$$\mathbb{F}^*_{p^{km}}/(\mathbb{F}^*_{p^{km}})^q \simeq \mathrm{G}_q \subseteq T_k(\mathbb{F}_{p^m}) \subseteq \mathbb{F}^*_{p^{km}}$$

- Properties of the pairing

non-degeneracy $\forall P \neq \mathcal{O}_E \quad \exists Q \in E(\mathbb{F}_{p^{km}})[q]$:

$$e_q(P,Q) \neq 1 \in \mathbb{F}^*_{p^{km}}/(\mathbb{F}^*_{p^{km}})^q$$

bilinearity $e_q([n]P,Q) = e_q(P,[n]Q) = e_q(P,Q)^n$

computability Let $q|r|p^{km-1}$. Then

$$e_q(P,Q)^{(p^{km}-1)/q} = e_r(P,Q)^{(p^{km}-1)/r}.$$

Pairings

Let $E(\mathbb{F}_{3^m})[q] \subseteq E(\mathbb{F}_{3^m})$ and let $q | 3^{6m-1}$

- The pairing is a map

$$e_q : E(\mathbb{F}_{3^m})[q] \times E(\mathbb{F}_{3^{6m}})[q] \to \mathbb{F}^*_{3^{6m}} / (\mathbb{F}^*_{3^{6m}})^q$$

- Easy observation of e_q's range

$$\mathbb{F}^*_{3^{6m}} / (\mathbb{F}^*_{3^{6m}})^q \simeq \mathsf{G}_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$

- Properties of the pairing

non-degeneracy $\forall P \neq \mathcal{O}_E \quad \exists Q \in E(\mathbb{F}_{3^{6m}})[q]$:
$e_q(P, Q) \neq 1 \in \mathbb{F}^*_{3^{6m}} / (\mathbb{F}^*_{3^{6m}})^q$

bilinearity $e_q([n]P, Q) = e_q(P, [n]Q) = e_q(P, Q)^n$

computability Let $q | r | 3^{6m-1}$. Then
$e_q(P, Q)^{(3^{6m}-1)/q} = e_r(P, Q)^{(3^{6m}-1)/r}$.

Pairings

Exponentiation after the Pairing

$$E(\mathbb{F}_{3^m})[q] \times E(\mathbb{F}_{3^{6m}})[q]$$

$$\downarrow e_q$$

$$\mathbb{F}^*_{3^{6m}} / (\mathbb{F}^*_{3^{6m}})^q$$

$$\downarrow \mathrm{Pow}$$

$$\mathrm{G}_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$

$$\downarrow \text{exponentiate}$$

$$\mathrm{G}_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$

Trace-based:

2004: Scott and Baretto's ternary ladder takes 12.

Pairings

Exponentiation after the Pairing

$$E(\mathbb{F}_{3^m})[q] \times E(\mathbb{F}_{3^{6m}})[q]$$

$$\downarrow e_q$$

$$\mathbb{F}^*_{3^{6m}}/(\mathbb{F}^*_{3^{6m}})^q$$

$$\downarrow \text{Pow}$$

$$\mathsf{G}_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$

$$\downarrow \text{exponentiate}$$

$$\mathsf{G}_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$

Trace-based:

2001: Stam and Lenstra's Euclidean method takes only 10.3.

2004: Scott and Baretto's ternary ladder takes 12.

Pairings

Exponentiation after the Pairing

$$E(\mathbb{F}_{3^m})[q] \times E(\mathbb{F}_{3^{6m}})[q]$$
$$\downarrow e_q$$
$$\mathbb{F}^*_{3^{6m}} / (\mathbb{F}^*_{3^{6m}})^q$$
$$\downarrow \text{Pow}$$
$$G_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$
$$\downarrow \text{exponentiate}$$
$$G_q \subseteq T_6(\mathbb{F}_{3^m}) \subseteq \mathbb{F}^*_{3^{6m}}$$

Trace-based:

2001: Stam and Lenstra's Euclidean method takes only 10.3.

2004: Scott and Baretto's ternary ladder takes 12.

Torus-based: (Granger et al., 2005) Depending on the bag of tricks, between 4.5 and 9.

Pairings
Actual Computation

Algorithm 1: The *Duursma-Lee* Algorithm

input : Two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in $E(\mathbb{F}_{p^m})[q]$
output: $e_{3^{3m}+1}(P, Q) \in \mathbb{F}^*_{3^{6m}} / \mathbb{F}^*_{3^{3m}}$

$f \leftarrow 1$
for $i = 1$ **to** m **do**
  $x_1 \leftarrow x_1^3, y_1 \leftarrow y_1^3$
  $\mu \leftarrow x_1 + x_2 + b, \lambda \leftarrow -y_1 y_2 \sigma - \mu^2$
  $g \leftarrow \lambda - \mu\rho - \rho^2, f \leftarrow f \cdot g$
  $x_2 \leftarrow x_2^{1/3}, y_2 \leftarrow y_2^{1/3}$
end
return f

- Using traces does not work.
- Using naive implementation takes 20M.
- Exploiting sparsity takes 15M, with loop unrolling 14M.

Conclusion

- For large characteristic, trace-based systems have a slight efficiency edge.
- However, torus-based gives wider range of functionality.
- Adding affinity gives better compression for T_{30} than CEILIDH.
- For small characteristic, torus-based systems have the edge.
- Using traces inside the pairing evaluation seems doomed.