Compact Diffie-Hellman key exchange with efficient endomorphisms

Benjamin Smith

Team **GRACE**

INRIA Saclay–Île-de-France

Laboratoire d'Informatique de l'École polytechnique (LIX)

YACC 2014, Porquerolles
June 12, 2014

For the next hour,

q is a power of a prime $p > 3$

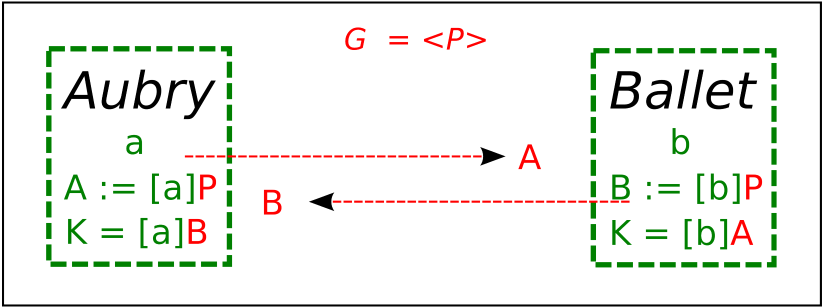
Everything is defined over $\mathbb{F}_q$

(unless otherwise noted)

All abelian varieties are ordinary

(not supersingular)

Diffie–Hellman Key Exchange



Original scheme: $G \subset \mathbb{F}_q^\times$

Compute $P \mapsto [m]P := P^m$ via chain of squares & mults

To break CDHP $(P, [a]P, [b]P) \mapsto [ab]P$:
subexponential solution using index calculus
Recent developments $\implies$ *q must be prime*

q prime: solve CHDP with Number Field Sieve variant

$\implies$ *key sizes and computational costs scale like RSA*

128-bit security ($\equiv$ basic AES): need 3000-bit q

$\implies$ $\mathbb{F}_q^\times$ is slow and inefficient

Elliptic curves: $By^2 = x(x^2 + Ax + 1)$.

Compute $P \mapsto [m]P$ via chain of doubles & adds

$$x(P \oplus Q) := BF_{\oplus}(P,Q)^2 - (x(P) + x(Q) + A)$$

$$y(P \oplus Q) := (2x(P) + x(Q) + A)F_{\oplus}(P,Q) - BF_{\oplus}(P,Q)^3 - y(P)$$

where $F_{\oplus}(P,Q) := (y(Q) - y(P))/(x(Q) - x(P))$, while

$$x([2]P) := BF_2(P)^2 - (2x(P) + A)$$

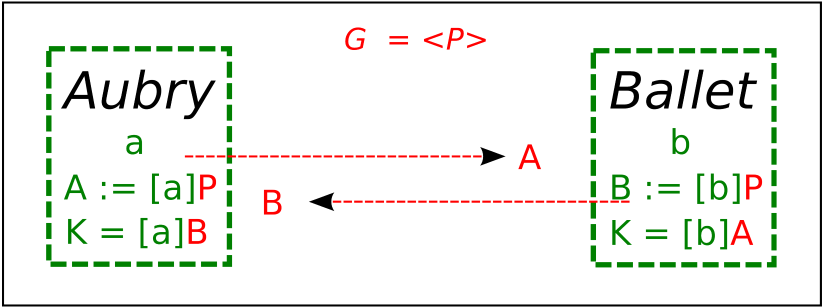
$$y([2]P) := (3x(P) + A)F_2(P) - BF_2(P)^3 - y(P)$$

where $F_2(P) := (3x(P)^2 + 2Ax(P) + 1)/(2By(P))$.

Exponential CDHP (Pollard ρ) $\implies$ shorter keys & chains

eg. 128-bit security ($\simeq$ AES): 256-bit q (vs 3k-bit for $\mathbb{G}_m$)

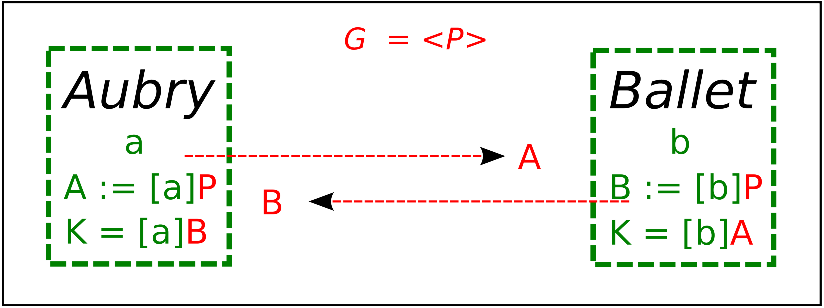
Look again:



Focus: scalar multiplication $P \mapsto [m]P$,
not group law $\oplus$.

In fact: we don't care if $\mathcal{G}$ is not a group!

Modern Diffie–Hellman



- $\mathcal{G}$ is a large set (with no proper group operation!)
- $[a], [b] \in$ large set of *easy* *commuting maps* $\mathcal{G} \to \mathcal{G}$ with a *hard* CHDP (given $P, [a]P, [b]P$, find $[ab]P$)

Montgomery's observation

If P and Q are points on $\mathcal{E} : By^2 = x(x^2 + Ax + 1)$, then

$$x(P \oplus Q)x(P \ominus Q) = \frac{(x(P)x(Q) - 1)^2}{(x(P) - x(Q))^2}$$

$$\text{and} \quad x([2]P) = \frac{(x(P) - 1)^2}{4x(P)(x(P)^2 + Ax(P) + 1)} .$$

Notice: B and y are gone!

Use *differential* addition chains, where
$P \oplus Q$ only appears if $P \ominus Q$ appeared previously

$\implies$ compute $[m]_* : x(P) \mapsto x([m]P)$ using *only* x-coord

Montgomery arithmetic

$$[m]_* : x =: X_1/Z_1 \longmapsto X_m/Z_m \quad \text{for any } m \in \mathbb{Z}$$

where we compute $(X_m : Z_m)$ using a differential chain based on

- Pseudo-addition (6M + 4A) where $r \neq s$:

$$X_{r+s} = Z_{r-s}\left[(X_r - Z_r)(X_s + Z_s) + (X_r + Z_r)(Z_s - Z_s)\right]^2$$
$$Z_{r+s} = X_{r-s}\left[(X_r - Z_r)(X_s + Z_s) - (X_r + Z_r)(Z_s - Z_s)\right]^2$$

- Pseudo-doubling (5M + 4A):

$$X_{2r} = (X_r + Z_r)^2(X_r - Z_r)^2$$
$$Z_{2r} = (4X_rZ_r)\left[(X_r - Z_r)^2 + \frac{A+2}{4} \cdot (4X_rZ_r)\right]$$

where $4X_rZ_r = (X_r + Z_r)^2 - (X_r - Z_r)^2$.

If $\omega = x(P)$ for P in $\mathcal{E}(\overline{\mathbb{F}}_q)$, then $[m]_*(\omega) = x([m]P)$.

Quadratic twist of $\mathcal{E} : By^2 = x(x^2 + Ax + 1)$:
any $\mathcal{E}' : B'y^2 = x(x^2 + Ax + 1)$ where B'/B is not a square in $\mathbb{F}_q$.

The maps $[m]_*$ depend on A but not B (or B')
$\implies$ $[m]_*$ is identical for $\mathcal{E}$ and $\mathcal{E}'$.

For every $\omega \in \mathbb{F}_q$, either

- $\omega = x(P)$ for some $P \in \mathcal{E}(\mathbb{F}_q)$ and $[m]_*(\omega) = x([m]P)$, or
- $\omega = x(P')$ for some $P' \in \mathcal{E}'(\mathbb{F}_q)$ and $[m]_*(\omega) = x([m]P')$.

Conclusion:

$[a]_* : \mathbb{F}_q \to \mathbb{F}_q$ and $[b]_* : \mathbb{F}_q \to \mathbb{F}_q$
commute for all a, b in $\mathbb{Z}$.

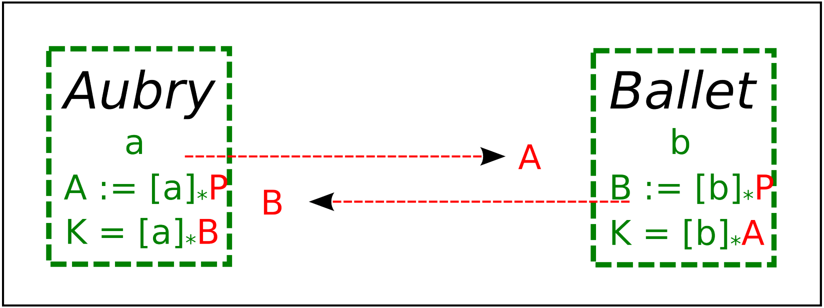
If $\omega = x(P)$, then $[m]_*(\omega) = x([m]P)$.

Given $\omega, [a]_*(\omega), [b]_*(\omega)$, find $[ab]_*(\omega)$ *(pseudo-CDHP)*:

- lift to $\mathcal{E}(\mathbb{F}_q)$ if $\omega = x(P)$ for some P in $\mathcal{E}(\mathbb{F}_q)$
- lift to $\mathcal{E}'(\mathbb{F}_q)$ if $\omega = x(P')$ for some P' in $\mathcal{E}'(\mathbb{F}_q)$.

Hence, both $\mathcal{E}(\mathbb{F}_q)$ and $\mathcal{E}'(\mathbb{F}_q)$ must be secure.

State-of-the-Art Diffie–Hellman



- $\mathcal{G} = \mathbb{F}_q$ (not viewed as a group!)
- secret $[a]_*$, $[b]_*$ from random a, b in $O(q)$
  and twist-secure $\mathcal{E} : By^2 = x(x^2 + Ax + 1)$ over $\mathbb{F}_q$
- Example: Bernstein's `Curve25519` software.

The challenge:
Go faster.

Endomorphisms

Suppose $\mathcal{E}/\mathbb{F}_q$ is an elliptic curve, $\mathcal{E}'$ its quadratic twist.

Endomorphisms: algebraic maps $\phi : \mathcal{E} \to \mathcal{E}$ such that $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$ for all P, Q in $\mathcal{E}$.

Examples: $[m]$ for m in $\mathbb{Z}$, Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$.

General form: $\phi : (x, y) \mapsto (\phi_*(x), y \cdot \mu \frac{d\phi_*}{dx}(x))$ for some ϕ_* in $\mathbb{F}_q(x)$, μ in $\mathbb{F}_q$.

- The endomorphisms form a (quadratic imaginary) ring, $\mathrm{End}(\mathcal{E})$
- $\mathbb{Z}[\pi] \subseteq \mathrm{End}(\mathcal{E})$
- $\mathrm{End}(\mathcal{E}) \cong \mathrm{End}(\mathcal{E}')$
- If $\phi \in \mathrm{End}(\mathcal{E})$, then the corresponding $\phi' \in \mathrm{End}(\mathcal{E}')$ satisfies $\phi_* = \phi'_*$

Suppose $\phi \in \mathrm{End}(\mathcal{E})$ is efficient and defined $/\mathbb{F}_q$

("efficient" = compute $P \mapsto \phi(P)$ in $O(1)$ $\mathbb{F}_q$-operations)

Suppose $\mathcal{G} \cong \mathbb{Z}/N\mathbb{Z}$ and $\mathcal{G}' \cong \mathbb{Z}/N'\mathbb{Z}$

are large subgroups of $\mathcal{E}(\mathbb{F}_q)$ and $\mathcal{E}'(\mathbb{F}_q)$, respectively.

$$\implies \phi(\mathcal{G}) \subseteq \mathcal{G} \text{ and } \phi'(\mathcal{G}) \subseteq \mathcal{G}'$$

$$\implies \begin{cases} \phi(P) = [\lambda]P \ \forall P \in \mathcal{G} & \text{for some } \lambda \bmod N \\ \phi'(P') = [\lambda']P' \ \forall P' \in \mathcal{G}' & \text{for some } \lambda' \bmod N' \end{cases}$$

$$\implies \phi_*(\omega) = \phi'_*(\omega) = \begin{cases} [\lambda]_*(\omega) & \text{if } \omega \in x(\mathcal{E}(\mathbb{F}_q)) \\ [\lambda']_*(\omega) & \text{if } \omega \in x(\mathcal{E}'(\mathbb{F}_q)) \end{cases}$$

Scalar decompositions on $\mathcal{E}$

Suppose ϕ has eigenvalue λ on $\mathcal{G} \subseteq \mathcal{E}(\mathbb{F}_q)$.

To compute $[m]P$ for P in $\mathcal{G}$:

- Compute m_0 and m_1 st $m \equiv m_0 + m_1\lambda \pmod{N}$ [easy]
- Compute $[m]P = [m_0]P \oplus [m_1]\phi(P)$ using (simultaneous) multiexponentiation: *chain length* $\sim \max(\log_2 |m_i|)$.
- If $|\lambda| \geq \sqrt{N}$, then $\max(\log_2 |m_i|) = \frac{1}{2}\log_2 N + \epsilon$.

Converse: sample (m_0, m_1) from $O(\sqrt{N})^2$,
$\implies [m_0]P \oplus [m_1]\phi(P) \approx$ random element of $\mathcal{G}$

Efficient ϕ? $\deg \phi = \deg_{\mathrm{sep}} \phi \cdot \deg_{\mathrm{insep}} \phi$.

- $\deg_{\mathrm{insep}} \longleftrightarrow$ contribution of p-th powering (virtually free)
- $\deg_{\mathrm{sep}} \longleftrightarrow$ complexity of defining polynomials $\longleftrightarrow$ efficiency

Scalar decompositions on the x-line

We want to compute $x([m_0]P \oplus [m_1]\phi(P))$ from $x(P)$.

2-dim. differential addition chains: can compute $x([m_0]P \oplus [m_1]Q)$ from $x(P)$, $x(Q)$, $x(P \ominus Q)$

So: we need $x(P)$, $x(\phi(P))$, $x(P \ominus \phi(P))$

Naïve: start with $P \in \mathcal{E}(\mathbb{F}_q)$; compute $\phi(P)$ and $P \ominus \phi(P)$; then launch chain on x-coords.

Better: $1 - \phi$ is an endomorphism; compute $(1 - \phi)_*$. Use $x(P \ominus \phi(P)) = (1 - \phi)_*(x(P))$.

D–H with x-line endomorphisms

Public parameters: $\omega \in \mathbb{F}_q$, twist-secure $\mathcal{E}/\mathbb{F}_q$ with efficient ϕ

1. Aubry randomly samples $\cancel{a \in O(q)}$ $a_0, a_1 \in O(\sqrt{q})$; computes & publishes $\cancel{A = [a]_*(\omega)}$ $A = ([a_0] \oplus [a_1]\phi)_*(\omega)$ *using differential addition chain on* $\omega, \phi_*(\omega), (1-\phi)_*(\omega)$
2. Ballet randomly samples $\cancel{b \in O(q)}$ $b_0, b_1 \in O(\sqrt{q})$; computes & publishes $\cancel{B = [b]_*(\omega)}$ $B = ([b_0] \oplus [b_1]\phi)_*(\omega)$ *using differential addition chain on* $\omega, \phi_*(\omega), (1-\phi)_*(\omega)$
3. Aubry computes secret $\cancel{K = [a]_*(B)}$ $K = ([a_0] \oplus [a_1]\phi)_*(B)$ *using differential addition chain on* $B, \phi_*(B), (1-\phi)_*(B)$
4. Ballet computes secret $\cancel{K = [b]_*(A)}$ $K = ([b_0] \oplus [b_1]\phi)_*(A)$ *using differential addition chain on* $A, \phi_*(A), (1-\phi)_*(A)$

GLV (Gallant–Lambert–Vanstone, CRYPTO 2001)

Fast endomorphisms from CM curves with tiny CM discriminants.

Fast because $\deg_{\mathrm{sep}}(\phi) = \text{tiny}$ and $\deg_{\mathrm{insep}}(\phi) = 1$. Example:

$$\mathcal{E} : y^2 = x(x^2 + 1)$$

$$\phi : (x, y) \longmapsto (-x, \sqrt{-1}y).$$

Applying GLV endomorphisms to the x-line:

$$\phi_* : x \longmapsto -x \qquad \text{[fast]}$$

$$(1 - \phi)_* : x \longmapsto \frac{\sqrt{-1}}{2}(x + 1/x) \qquad \text{[fast]}$$

Disadvantage (major): GLV curves are impossibly rare

$\implies$ generally no secure curves $/\mathbb{F}_p$ for efficient p.

GLS (Galbraith–Lin–Scott, EUROCRYPT 2009)

Fast endomorphisms from twists of subfield curves over $\mathbb{F}_{p^2}$:
the fast endomorphism is a twisted sub-Frobenius.
Example: take any A_0 in $\mathbb{F}_p$, $p \equiv 3 \pmod 4$

$$\mathcal{E} : y^2 = x(x^2 + A_0\sqrt{-1}x + 1)$$

$$\phi : (x, y) \mapsto (-x^p, iy^p)$$

- Fast because $\deg_{\mathrm{sep}}(\phi) = 1$, and $\deg_{\mathrm{sep}}(\phi) = p$
- Advantage: $O(p)$ GLS curves over any $\mathbb{F}_{p^2}$:
  $\implies$ can find secure curves over fast $\mathbb{F}_{p^2}$
- Disadvantage: GLS curves are catastrophically twist-insecure *by construction* (their twists are subfield curves)
  $\implies$ unsuitable for Diffie–Hellman

$\mathbb{Q}$-curve reductions (S., ASIACRYPT 2013)

Reduce low degree $\mathbb{Q}$-curve families modulo inert primes p to get $\mathcal{E}, \phi/\mathbb{F}_{p^2}$ with $\deg_{\mathrm{sep}}(\phi) = $ tiny, $\deg_{\mathrm{insep}}(\phi) = p$.

Example: Take *any* $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\Delta})$. For every $t \in \mathbb{F}_p$, the curve

$$\mathcal{E}_t/\mathbb{F}_{p^2} : y^2 = x^3 - 6(5 - 3t\sqrt{\Delta})x + 8(7 - 9t\sqrt{\Delta})$$

has an efficient (faster than doubling) endomorphism

$$\phi : (x, y) \longmapsto \left(f(x^p), \frac{y^p}{\sqrt{-2}} f'(x^p) \right) \text{ where } f(x^p) = \frac{-x^p}{2} - \frac{9(1 - t\sqrt{\Delta})}{(x^p - 4)} .$$

We have $\phi^2 = [\pm 2]\pi$, so $\lambda_\phi = \pm\sqrt{\pm 2}$ on cryptographic subgroups.

On the x-line: $\phi_*(x) = f(x^p)$ is fast, but
$(1 - \phi)_*(x) =$ quartic beurk with a $(p + 1)/2$-powering in $\mathbb{F}_{p^2}$.

Implementation: Costello–Hisil–S. (EUROCRYPT 2014)

C/Assembly implementation targeting 128-bit security level

Platform: Intel Ivy Bridge

Based on $\mathbb{Q}$-curve reduction over $\mathbb{F}_{p^2}$ with $p = 2^{127} - 1$

For comparison, without endomorphisms:
Montgomery ladder (uniform, const. time) same curve: 159 kCycles
`Curve25519` (uniform, const. time), 182 kCycles

Chain	unif.	const. time	steps /128	per step $\oplus$	per step [2]	kCycles
PRAC	NO	NO	~ 0.9	~ 1.6	~ 0.6	109
A-K	YES	NO	~ 1.4	1	1	133
Bernstein	YES	YES	1	2	1	148

Next challenge:

Go faster, cleaner