Revisiting discrete logarithms in the Medium prime case

Antoine Joux

ESC'2013 – Mondorf-les-bains

January 15th,2013

Medium prime fields – practical interest

Medium prime fields – practical interest

- Choose p a prime that fits on 32-bits

Medium prime fields – practical interest

- Choose p a prime that fits on 32-bits
- Then computing in $\mathbb{F}_{p^k}$ means "polynomials mod p"

Medium prime fields – practical interest

- Choose p a prime that fits on 32-bits
- Then computing in $\mathbb{F}_{p^k}$ means "polynomials mod p"
- Easy to implement, esp. if irreducible polynomial defining $\mathbb{F}_{p^k}$ has low weight.
  - With restriction on p it can even be $x^k - 2$

Medium prime fields – practical interest

- Choose p a prime that fits on 32-bits
- Then computing in $\mathbb{F}_{p^k}$ means "polynomials mod p"
- Easy to implement, esp. if irreducible polynomial defining $\mathbb{F}_{p^k}$ has low weight.
  - With restriction on p it can even be $x^k - 2$
- If, in addition, p is FFT-friendly $\Rightarrow$ Very efficient implementation

Discrete Logarithms in the Medium prime case [JL06]

Discrete Logarithms in the Medium prime case [JL06]

- Finite field of the form $\mathbb{F}_{p^k}$

Discrete Logarithms in the Medium prime case [JL06]

- Finite field of the form $\mathbb{F}_{p^k}$
- Choose two univariate polynomials f_1 and f_2
  - with degrees d_1 and d_2 and $d_1 d_2 \geq k$.
  - Such that $x - f_1(f_2(x))$ has:
    - an irreducible factor of degree k (modulo p).

Discrete Logarithms in the Medium prime case [JL06]

- Finite field of the form $\mathbb{F}_{p^k}$
- Choose two univariate polynomials f_1 and f_2
  - with degrees d_1 and d_2 and $d_1 d_2 \geq k$.
  - Such that $x - f_1(f_2(x))$ has:
    - an irreducible factor of degree k (modulo p).
- This defines the finite field by the relations:
  - $x = f_1(y)$ and $y = f_2(x)$

Discrete Logarithms in the Medium prime case [JL06]

Discrete Logarithms in the Medium prime case [JL06]

- Finite field of the form $\mathbb{F}_{p^k}$

Discrete Logarithms in the Medium prime case [JL06]

- Finite field of the form $\mathbb{F}_{p^k}$
- Choose two univariate polynomials f_1 and f_2
  - with degrees d_1 and d_2 and $d_1 d_2 \geq k$.
  - Such that $x - f_1(f_2(x))$ has:
    - an irreducible factor of degree k (modulo p).

Discrete Logarithms in the Medium prime case [JL06]

- Finite field of the form $\mathbb{F}_{p^k}$
- Choose two univariate polynomials f_1 and f_2
  - with degrees d_1 and d_2 and $d_1 d_2 \geq k$.
  - Such that $x - f_1(f_2(x))$ has:
    - an irreducible factor of degree k (modulo p).
- This defines the finite field by the relations:
  - $x = f_1(y)$ and $y = f_2(x)$

Discrete Logarithms in the Medium prime case [JL06]

Discrete Logarithms in the Medium prime case [JL06]

- Optimal for $p = L_{1/3}(p^k)$

Discrete Logarithms in the Medium prime case [JL06]

- Optimal for $p = L_{1/3}(p^k)$
- Choose smoothness basis $x - \alpha$ and $y - \alpha$

Discrete Logarithms in the Medium prime case [JL06]

- Optimal for $p = L_{1/3}(p^k)$

- Choose smoothness basis $x - \alpha$ and $y - \alpha$
- Consider elements:

$$\begin{aligned} xy + ay + bx + c &= x\, f_2(x) + a f_2(x) + bx + c \\ &= y\, f_1(y) + ay + b f_1(y) + c \end{aligned}$$

Discrete Logarithms in the Medium prime case [JL06]

- Optimal for $p = L_{1/3}(p^k)$

- Choose smoothness basis $x - \alpha$ and $y - \alpha$
- Consider elements:

$$\begin{aligned} xy + ay + bx + c &= x\, f_2(x) + a f_2(x) + bx + c \\ &= y\, f_1(y) + ay + b f_1(y) + c \end{aligned}$$

- When both sides split $\Rightarrow$ Relation

Discrete Logarithms in the Medium prime case [JL06]

- Optimal for $p = L_{1/3}(p^k)$

- Choose smoothness basis $x - \alpha$ and $y - \alpha$
- Consider elements:

$$\begin{aligned} xy + ay + bx + c &= x\, f_2(x) + a f_2(x) + bx + c \\ &= y\, f_1(y) + ay + b f_1(y) + c \end{aligned}$$

- When both sides split $\Rightarrow$ Relation
- Classical approach, get relations by sieving:
  - For each a, b and α, compute c such that $(x - \alpha) \mid x\, f_2(x) + ax + b f_2(x) + c$.
  - Idem for y
  - If c has enough hits $\Rightarrow$ Relation

Discrete Logarithms in the Medium prime case [JL06]

- Optimal for $p = L_{1/3}(p^k)$

- Choose smoothness basis $x - \alpha$ and $y - \alpha$
- Consider elements:

$$\begin{aligned} xy + ay + bx + c &= x\, f_2(x) + a f_2(x) + bx + c \\ &= y\, f_1(y) + ay + b f_1(y) + c \end{aligned}$$

- When both sides split $\Rightarrow$ Relation
- Classical approach, get relations by sieving:
  - For each a, b and α, compute c such that $(x - \alpha) \mid x\, f_2(x) + ax + b f_2(x) + c$.
  - Idem for y
  - If c has enough hits $\Rightarrow$ Relation
- Cost of finding relation is $(d+1)!\,(d'+1)!$

New idea – basic version

New idea – basic version

- Further restrict to $y = x^d$

New idea – basic version

- Further restrict to $y = x^d$
- Then:

$$xy + ay + bx + c \quad = \quad x^{d+1} + ax^d + bx + c$$

New idea – basic version

- Further restrict to $y = x^d$
- Then:

$$xy + ay + bx + c \quad = \quad x^{d+1} + ax^d + bx + c$$

- Perform change of variable: $x = aX$, we get:

$$a^{d+1}(X^{d+1} + X^d + b \cdot a^{-d}(X + c/(ab)).$$

New idea – basic version

- Further restrict to $y = x^d$
- Then:

$$xy + ay + bx + c \quad = \quad x^{d+1} + ax^d + bx + c$$

- Perform change of variable: $x = aX$, we get:

$$a^{d+1}(X^{d+1} + X^d + b \cdot a^{-d}(X + c/(ab)).$$

- Change of variable does not affect splitting property

New idea – basic version

- Further restrict to $y = x^d$
- Then:

$$xy + ay + bx + c \quad = \quad x^{d+1} + ax^d + bx + c$$

- Perform change of variable: $x = aX$, we get:

$$a^{d+1}(X^{d+1} + X^d + b \cdot a^{-d}(X + c/(ab)).$$

- Change of variable does not affect splitting property
- One good left-hand side $\Rightarrow$ p good left-hand sides

New idea – basic version

- Further restrict to $y = x^d$
- Then:

$$xy + ay + bx + c \quad = \quad x^{d+1} + ax^d + bx + c$$

- Perform change of variable: $x = aX$, we get:

$$a^{d+1}(X^{d+1} + X^d + b \cdot a^{-d}(X + c/(ab)).$$

- Change of variable does not affect splitting property
- One good left-hand side $\Rightarrow$ p good left-hand sides
- Amortized cost of relation reduced to

$$\left(\frac{(d+1)!}{p-1} + 1\right) \cdot (d'+1)!$$

Further improvement – Kummer extensions

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$
- If $k = dd' - 1$, let $y = x^d$ and $tx = y^{d'}$
- If $k = dd' + 1$, let $y = x^d$ and $x = t/y^{d'}$

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$
- If $k = dd' - 1$, let $y = x^d$ and $tx = y^{d'}$
- If $k = dd' + 1$, let $y = x^d$ and $x = t/y^{d'}$
- Then $xy + ay + bx + c$ has the previous form on both sides:

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$
- If $k = dd' - 1$, let $y = x^d$ and $tx = y^{d'}$
- If $k = dd' + 1$, let $y = x^d$ and $x = t/y^{d'}$
- Then $xy + ay + bx + c$ has the previous form on both sides:
  - $x^{d+1} + ax^d + bx + c \Rightarrow a^{d+1}(X^{d+1} + X^d + b \cdot a^{-d}(X + c/(ab))$.

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$
- If $k = dd' - 1$, let $y = x^d$ and $tx = y^{d'}$
- If $k = dd' + 1$, let $y = x^d$ and $x = t/y^{d'}$
- Then $xy + ay + bx + c$ has the previous form on both sides:
  - $(y^{d'+1} + by^{d'})/t + ay + c \Rightarrow$
    $b^{d'+1}\left((Y^{d'+1} + Y^{d'})/t + a \cdot b^{-d'}(Y + c/(ab)\right).$

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$
- If $k = dd' - 1$, let $y = x^d$ and $tx = y^{d'}$
- If $k = dd' + 1$, let $y = x^d$ and $x = t/y^{d'}$
- Then $xy + ay + bx + c$ has the previous form on both sides:

  - $(ay^{d'+1} + cy^{d'} + ty + bt)/y^{d'} \Rightarrow$
    $b\left(a \cdot b^{d'}(Y^{d'+1} + c/(ab)Y^{d'}) + t(Y+1)\right).$

Further improvement – Kummer extensions

- Assume $k|p-1$, then $\mathbb{F}_{p^k}$ can be defined by $x^k - t$
- If $k = dd' - 1$, let $y = x^d$ and $tx = y^{d'}$
- If $k = dd' + 1$, let $y = x^d$ and $x = t/y^{d'}$
- Then $xy + ay + bx + c$ has the previous form on both sides:
  - $x^{d+1} + ax^d + bx + c \Rightarrow a^{d+1}(X^{d+1} + X^d + b \cdot a^{-d}(X + c/(ab))$.
  - $(ay^{d'+1} + cy^{d'} + ty + bt)/y^{d'} \Rightarrow$
    $b\left(a \cdot b^{d'}(Y^{d'+1} + c/(ab)Y^{d'}) + t(Y+1)\right)$.
- In both cases $\lambda = c/(ab)$ is shared by the two sides

Kummer extensions – Reassembling two sides

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.
- Find a and b such that $\theta_X = b \cdot a^{-d}$ and $\theta_Y = a \cdot b^{-d'}$?

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.
- Find a and b such that $\theta_X = b \cdot a^{-d}$ and $\theta_Y = a \cdot b^{-d'}$?
- This implies $\theta_X^{d'}\theta_Y = a^{-dd'+1} = a^{-k}$.

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.
- Find a and b such that $\theta_X = b \cdot a^{-d}$ and $\theta_Y = a \cdot b^{-d'}$?
- This implies $\theta_X^{d'}\theta_Y = a^{-dd'+1} = a^{-k}$.
  - Possible iff $\theta_X^{d'}\theta_Y$ is a k-th power

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.
- Find a and b such that $\theta_X = b \cdot a^{-d}$ and $\theta_Y = a \cdot b^{-d'}$?
- This implies $\theta_X^{d'}\theta_Y = a^{-dd'+1} = a^{-k}$.
  - Possible iff $\theta_X^{d'}\theta_Y$ is a k-th power
  - Gives k (conjugate) solutions !

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.
- Find a and b such that $\theta_X = b \cdot a^{-d}$ and $\theta_Y = a \cdot b^{-d'}$?
- This implies $\theta_X^{d'}\theta_Y = a^{-dd'+1} = a^{-k}$.
  - Possible iff $\theta_X^{d'}\theta_Y$ is a k-th power
  - Gives k (conjugate) solutions !
  - From a recover b and c

Kummer extensions – Reassembling two sides

- Assume that:
  - $X^{d+1} + X^d + \theta_X(X + \lambda)$ splits and
  - $(Y^{d'+1} + Y^{d'})/t + \theta_Y(Y + \lambda)$ splits.
- Find a and b such that $\theta_X = b \cdot a^{-d}$ and $\theta_Y = a \cdot b^{-d'}$?
- This implies $\theta_X^{d'}\theta_Y = a^{-dd'+1} = a^{-k}$.
  - Possible iff $\theta_X^{d'}\theta_Y$ is a k-th power
  - Gives k (conjugate) solutions !
  - From a recover b and c
  - Roots obtained by change of variable

Kummer extensions – conjugation

Kummer extensions – conjugation

- The conjugates solutions mentioned earlier come from:

$$(X+\alpha)^p = X^p + \alpha = t^{(p-1)/k}X + \alpha = \mu(X + \alpha/\mu),$$

where μ is a k-th root of unity in $\mathbb{F}_p$.

Kummer extensions – conjugation

- The conjugates solutions mentioned earlier come from:

$$(X+\alpha)^p = X^p + \alpha = t^{(p-1)/k}X + \alpha = \mu(X + \alpha/\mu),$$

  where μ is a k-th root of unity in $\mathbb{F}_p$.
- Similarly:

$$(Y+\alpha)^p = \mu^d(Y + \alpha/\mu^d).$$

Kummer extensions – conjugation

- The conjugates solutions mentioned earlier come from:

$$(X+\alpha)^p = X^p + \alpha = t^{(p-1)/k}X + \alpha = \mu(X + \alpha/\mu),$$

  where μ is a k-th root of unity in $\mathbb{F}_p$.
- Similarly:

$$(Y+\alpha)^p = \mu^d(Y + \alpha/\mu^d).$$

- Reduces the smoothness basis by a factor k

Impact of the new idea

Impact of the new idea

- In theory, complexity of function field sieve:
  - Reduce in the best case from $L_{1/3}(3^{1/3}) \approx L_{1/3}(1.44)$ to $L_{1/3}(2 \cdot 3^{-2/3}) \approx L_{1/3}(0.96)$
  - Regardless of Kummer extension or not

Impact of the new idea

- In theory, complexity of function field sieve:
  - Reduce in the best case from $L_{1/3}(3^{1/3}) \approx L_{1/3}(1.44)$ to $L_{1/3}(2 \cdot 3^{-2/3}) \approx L_{1/3}(0.96)$
  - Regardless of Kummer extension or not
- In practice, new records:
  - First 1175-bit field $\mathbb{F}_{p^{47}}$ with p close to 2^{25}
  - Then 1425-bit field $\mathbb{F}_{p^{57}}$ with p close to 2^{25}
  - Previous record was 923 bits
  - Kummer extensions very useful for records

Experiments

Bitsize	923 bits	1175 bits	1425 bits
Time	813 000 CPU.h	32 000 CPU.h	32 000 CPU.h
Relations	270 000 CPU.h	3 CPU.h	6 CPU.h
Algebra	483 000 CPU.h	32 000 CPU.h	32 000 CPU.h
Indiv.	60 000 CPU.h	4 CPU.h	$<$ 12 CPU.h

Typical results

- $p = 33\,341\,353$, $X^{57} = 2$, Basis of logs $g = X - 11$
- Cardinality has two big prime factors (446 and 900 bits)
- Choose:

$$Z = \sum_{i=0}^{56} \left(\lfloor \pi \, p^{i+1} \rfloor \bmod p \right) X^i.$$

- After solving a linear system on 714 931 unknowns, we can find:

$$\log_g(Z) =$$

$$3869672795484867234025199634356061668992156541203$$
$$1083259217543064490314474088839541268684766235143$$
$$0377499473537441208379213189393975471631517424844$$
$$0299271293657607241850991250364535044122994973576$$
$$0120052465348429757817687904797819402906339667295$$
$$7652694830528789608330411939696620270005822826745$$
$$5228614682567866764560024936105482975290632000822$$
$$0524565954227246144528633607026598459910186711625$$
$$4083433078280438473992495655221202 02$$

Conclusion

Questions ?