Two Topics from Pairings and Towers

Florian Hess (Oldenburg)

Paris, June 21, 2013

Multilinear Pairings

First Part

Overview

Have seen recent breakthrough in construction of multilinear pairings ...

In first part of this talk:

Security aspects in a generic model:

- Simplify ideas of Verheul, Galbraith, Karabina-Knapp-Menezes.
- Generalise to multilinear pairings.
- Joint work with Uzunkol.

Number theoretic aspects of pairing inversion:

- Observe that there is a community that has researched a closely related problem for a long time.
- But here no actual improvement for pairing inversion.

Generic Model

Multilinear Pairings:

- $G_1, \ldots, G_{r+1}$ cyclic groups of squarefree order n.
- $e : G_1 \times \cdots \times G_r \to G_{r+1}$ non-deg multilinear map.
- $G_1 = \cdots = G_r$: symmetric pairing.
- $G_1 = \cdots = G_r = G_{r+1}$: self pairing.
- $r = 1$: homomorphism, $r = 2$: bilinear map.

Generic model:

- Oracle access to compute $a = b$, $a + b$ and $-a$.
- Oracle access to compute $e(a_1, \ldots, a_r)$.
- Unit cost for oracle access and storage of a.

Inversion

We say all pairings on the G_i are efficiently invertible when given by oracle access, iff:

- Consider a multilinear e on a subset of the G_i with oracle access.
- Can solve $e(a_1, \ldots, a_d) = a_{d+1}$ efficiently, given a_{d+1} and all but one argument, for the missing argument.
- Can do this for every such e and parameters.

We say all pairings on the G_i are efficiently computable when given by pointwise definition iff:

- Consider a multilinear e on a subset of the G_i, defined by $e(u_1, \ldots, u_d) = u_{d+1}$ for generators u_j.
- Can compute $e(a_1, \ldots, a_d)$ given the u_j and a_j.
- Can do this for every such e and parameters.

Inversion

We say all pairings on the G_i are efficiently invertible when given by pointwise definition iff:

- Consider a multilinear e on a subset of the G_i, defined by $e(u_1, \ldots, u_d) = u_{d+1}$ for generators u_j.
- Can solve $e(a_1, \ldots, a_d) = a_{d+1}$ efficiently, given a_{d+1} and all but one argument, for the missing argument.
- Can do this for every such e and parameters.

This includes the computational Diffie-Hellman problem or variants on all G_i:

- Given a pointwise defined homomorphism $f : G_i \mapsto G_i$, $f : P \to aP$, compute $f(bP) = abP$.
- Given a non-deg pairing $G_i \times G_i \to G_i$ and $Q = e(P, P)$, compute $e(aP, bP) = abQ$.

Bilinear Self Pairings

Key observation: Given cyclic G or order n, e self pairing on G. Then

$$(G, +, e) \cong (\mathbb{Z}/n\mathbb{Z}, +, \cdot).$$

Remarks:

- Can suppose $G = \mathbb{Z}/n\mathbb{Z}$.
- Let $w = e(1, 1)$. Then $e(a, b) = wab$.
- $f : \mathbb{Z}/n\mathbb{Z} \to G$, $x \mapsto w^{-1}x$ is ring isomorphism.
- Specificially $1_e = w^{-1}$.

Note

- similarity to Montgomery multiplication.
- is generalisation of Boneh-Lipton black box fields via CDH oracle, since self pairing gives only variant of CDH and n might be composite.

Bilinear Self Pairings: Theorem

Let G be a cyclic group of order n in the generic group model with oracle access to a bilinear self-pairing $\cdot$ of G.

If $\phi(n)$ is known then all pairings of r arguments on G are efficiently invertible when given by oracle access, and are efficiently computable and efficiently invertible when given by pointwise definition, for every $r \geq 1$.

Remarks:

- One shows that 1 and a^{-1} can be efficiently computed from a generator of G via powering.
- The rest is linear algebra.
- Thm applies also to isomorphisms defined by their images on a generator ($r = 1$) and provides „existence“ of multilinear pairings with arbitrary r.
- Thm encompasses Verheul and other results in a very easy and compact way.

Application to Asymmetric Pairings

Let G_1, G_2, G_3 be cyclic groups of order n in the generic group model with oracle access to a bilinear pairing

$$e : G_1 \times G_2 \to G_3.$$

Suppose $\phi(n)$ and generators of G_1 and G_2 are known, and that oracle access to isomorphisms

$$G_3 \to G_2, \ G_2 \to G_1 \ \text{ or } \ G_3 \to G_1, G_3 \to G_2$$

exists.

Then all pairings of r arguments on G_1, G_2, G_3 are efficiently invertible when given by oracle access, and are efficiently computable and efficiently invertible when given by pointwise definition, for every $r \geq 1$.

Discussion

- Feeding back values of multilinear pairings into arguments potentially dangerous and should not be possible!
- Proof nicely relates to encoding of elements $x \mapsto w^{-1}x$ in the recent schemes.

Number Theoretic Aspect of Inversion

Consider inversion of Tate paring function:

- t Tate pairing on $E(\mathbb{F}_q)[r]$, $\quad t(P,Q) = f_Q(P)^{(q-1)/r}$.
- Given Q, z find P with $f_Q(P)^{(q-1)/r} = z$.
- This is equivalent to finding a $\mathbb{F}_q$-rational point on the curve C defined as a cover of E via

$$wy^r = f_Q,$$

  where w is easily computed satisfying $w^{(q-1)/r} = z$.
- $C \to E$ is unramified, so C is an elliptic curve r-isogenous to E.
- Can we compute the j-invariant and the dual isogeny?

This computation is the same as is carried out when computing $E(\mathbb{Q})$ using descent. But there $r \leq 10$, say.

Towers of Curves

Second Part

Towers of Curves

A tower of curves $\mathcal{C}$ is a sequence of surjective morphisms

$$\cdots \to C_3 \to C_2 \to C_1 \to X$$

of regular, complete and absolutely irreducible curves C_i and X over a finite field $\mathbb{F}_q$.

Uses of towers of curves with specific properties:

- Construction of error-correcting codes
- Secret sharing schemes and secure multi-party computation.
- Bilinear complexity of multiplication
- Codices ...

Specific properties

Main goal:

Construct curves C with

- $\#C(\mathbb{F}_q)$ large,
- $g(C)$ small (i.e. C has small defining equations).

Interpolation shows these are opposing requirements.

The tower is supposed to provide such C_i with

$$\#C_i(\mathbb{F}_q), g(C_i) \to \infty.$$

First invariant

Let d_i be the degree of $C_i \to X$.

Then

- d_i grows exponentially in i.
- $\#C_i(\mathbb{F}_q) = O(d_i)$ for $i \to \infty$.
- $g(C_i) = \Omega(d_i)$ for $i \to \infty$.
- $\lim_{i\to\infty} \#C_i(\mathbb{F}_q)/g(C_i)$ exists.

Define

$$\beta_1(\mathcal{C}) = \lim_{i\to\infty} \frac{\#C_i(\mathbb{F}_q)}{g(C_i)}.$$

The goal is to find $\mathcal{C}$ such that

$$\beta_1(\mathcal{C}) > 0.$$

Then $\mathcal{C}$ is called asymptotically good (in degree one).

Some known facts

Upper bounds:

- $A_1(q) := \limsup_{\mathcal{C}} \beta_1(\mathcal{C})$.
- Then $A_1(q) \leq \sqrt{q} - 1$ (Drinfeld-Vladut).

Some lower bounds:

- q square then $A_1(q) = \sqrt{q} - 1$ (Ihara, Tsfasman-Vladut-Zink).
- $A_1(q^n) = \Omega((n \log(q))^2/(n + \log(q)))$ any q, n (Serre, Temkine)
- $A(2) \geq 0.316999$, $A(3) \geq 0.492876$ (Duursma-Mak).
- $A(p^{2m+1}) \geq 2(p^{m+1} - 1)/(p + 1 + (p - 1)/(p^m - 1))$ for p^{2m+1} with $2m + 1 \geq 3$ (Garcia-Stichtenoth-Bassa-Beelen)

Constructions

Constructions:

- Modular curves.
- Class field towers.
- Recursive towers.

Lower bounds for $A_1(q)$ proved by these constructions.

Non-square q by class field towers.

Non-square $q = p^{2m+1}$ with $2m + 1 \geq 3$ by recursive towers only recently. Yield much better lower bound than class field towers.

Higher Invariants: Definitions and Facts

Higher invariants of degree r:

- $B_r(C) = \#\{P \in C \mid \deg(P) = r\}$
- $\beta_r(\mathcal{C}) = \lim_{i\to\infty} B_r(C_i)/g(C_i)$.
- $A_r(q) = \limsup_{\mathcal{C}} \beta_r(\mathcal{C})$.

Some facts:

- $\sum_{r=1}^{\infty} r\beta_r(\mathcal{C})/(q^{r/2}-1) \leq 1$ (Serre, Tsfasman).
- $A_r(q) \leq (q^{r/2}-1)/r$.
- Exists $\mathcal{C}$ with finitely many prescribed $\beta_r(\mathcal{C}) > 0$ using class field towers (Hasegawa, Lebacque).
- Exists $\mathcal{C}$ with $\beta_4(\mathcal{C}) = A_4(2)$ (Ballet-Rolland).
- Exists $\mathcal{C}$ with $\beta_2(\mathcal{C}) = A_2(q)$ for any q (Ballet-Rolland).

Our Results

Joint work with Stichtenoth and Tutdere.

Our results:

- Explicit construction for $\mathcal{C}$ with finitely many prescribed $\beta_r(\mathcal{C}) > 0$.
- Explicit construction for $\mathcal{C}$ with at least one positive $\beta_r(\mathcal{C})$ and certain prescribed $\beta_s(\mathcal{C}) = 0$.
- Examples of $\mathcal{C}$ with all but one $\beta_r(\mathcal{C}) = 0$.
- Exists $\mathcal{C}$ with $\beta_r(\mathcal{C}) = A_r(q)$ if q^r is square.
- $A_1(q^r)/r \geq A_r(q)$ and some lower bounds on $A_r(q)$.

Main Idea

The main idea behind the paper is as follows:

Start with $\mathcal{C}$ and $\beta_1(\mathcal{C}) > 0$.

Construct $E \to X$ such that

- $E \times_X C_i$ is irreducible.
- Define E_i to be the normalisation of $E \times_X C_i$.
- The preimages in E_i of points of degree one of C_i that are split completely in $\mathcal{C}$ consist of points of E_i of prescribed degrees.
- The maps $C_i \to C_{i-1}$ extend to $E_i \to E_{i-1}$.

We then get a tower of curves $\mathcal{E}$ where the many points of degree one of $\mathbb{C}$ have been distributed in higher degrees and the genus does not increase too much.

Recursive towers: Definition

Provide explicit constructions. The most common form is:

Let $f \in \mathbb{F}_q[X, Y]$. Then $X = \mathbb{P}^1$ and C_i is defined by

$$\begin{aligned} f(x_0, x_1) &= 0, \\ f(x_2, x_3) &= 0, \\ &\dots \\ f(x_{i-1}, x_i) &= 0. \end{aligned}$$

The maps $C_i \to C_{i-1}$ are $(x_0, \dots, x_i) \mapsto (x_0, \dots, x_{i-1})$.

$K(C_i) = K(x_0, x_1, \dots, x_i)$ with $f(x_{i-1}, x_i) = 0$.

Example:

- $f = Y^q X^{q-1} + Y - X^q \in \mathbb{F}_{q^2}[X, Y]$,
- yields $\beta_1(\mathcal{C}) = A_1(q) = q - 1$.

Graphs

Very nice recent study by Hallouin-Perret.

- Consider properties of a graph associated to a recursive tower.
- Use intersection theory of correspondences, in particular to count cycles in the graph.
- Combine algebraic graph theory and Frobenius-Perron theory to deduce structure of the graph.
- d-regular strongly connected components of the graph are precisely responsible for many points.
- Under some mild hypotheses, there is at most one one such component and hence at most one $\beta_r(\mathcal{C}) > 0$.

Challenge

Open problem:

Construct asymptotically good recursive tower over $\mathbb{F}_p$.

Construct f with nice graphs over $\mathbb{F}_p$:

- Need d-regular strongly connected component.
- The singular part of the graph must allow/imply small genus.