Trilinear and found wanting

Steven Galbraith + Benjamin Smith

ANTS XIII, Madison, Wisconsin // July 19, 2018

University of Auckland, New Zealand
Inria + Laboratoire d'Informatique de l'École polytechnique (LIX), France

Multilinear maps:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \times \cdots \times \mathbb{G}_n \longrightarrow \mathbb{G}_T$$

$$e(a_1 P_1, a_2 P_2, \ldots, a_n P_n) = e(P_1, P_2, \ldots, P_n)^{a_1 a_2 \cdots a_n}$$

The case $n = 2$: **pairings**.

Secure multilinear maps with $n > 2$ are
a near-mythical cryptographic silver bullet.

March 2018: Ming-Deh Huang (arXiv:1803.10325)
gives a concrete proposal for secure **trilinear** maps.

Huang's proposal

Basic ingredients: an abelian variety $A/\mathbb{F}_q$ equipped with many **explicit endomorphisms**, and a **pairing** η_r on $A[r]$.

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_3 \longrightarrow \mathbb{G}_T$$

where $\mathbb{G}_1 = \langle P \rangle \subset A[r]$, $\mathbb{G}_2 = \langle Q \rangle \subset A[r]$, and

$$\mathbb{G}_3 = \mathbb{Z} + U_{P,Q} \subset \mathrm{End}(A)$$

where $\eta_r(P,Q) \neq 1$ and $U_{P,Q}$ is a set of "noise":

$$U_{P,Q} \subseteq \{\xi \in \mathrm{End}(A) : \eta_r(P, \xi(Q)) = 1 \, .$$

The **trilinear map**:

$$e : (aP, bQ, \psi = c + \xi) \longmapsto \eta_r(aP, \psi(bQ)) = \eta_r(P,Q)^{abc} \, .$$

Attacking the third group

The trilinear map:

$$e : (aP, bQ, \psi = [c] + \xi) \longmapsto \eta_r(aP, \psi(bQ)) = \eta_r(P,Q)^{abc}.$$

We can assume η_r, $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2 = \langle Q \rangle$, and $\mathbb{G}_T = \mu_r$ are secure.
We need to **attack the new group**, $\mathbb{G}_3$.

Public keys in $\mathbb{G}_3$ are $\psi = [c] + x_1\xi_1 + \cdots + x_s\xi_s$, where

- c is the secret key, an exponent in $\mathbb{Z}/r\mathbb{Z}$
- $x_1, \ldots, x_s$ are randomly sampled from $\mathbb{Z}/r\mathbb{Z}$ (noise)
- $1, \xi_1, \ldots, \xi_s$ is a (public) basis for a subring of $\mathrm{End}(A)$

Attack: recover c, or even the whole vector $(c, x_1, \ldots, x_s)$.

Identifying endomorphisms

We have a **pairing** $\mathrm{End}(A) \times \mathrm{End}(A) \to \mathbb{Z}$ defined by

$$\langle \psi_1, \psi_2 \rangle := \mathrm{Tr}(\psi_1 \circ \psi_2{}^\dagger)\,,$$

where $\psi \leftrightarrow \psi^\dagger$ is the Rosati involution.

Attack: Given the public basis $(\xi_0 = 1, \xi_1, \ldots, \xi_s)$
and a public key $\psi = c + x_1\xi_1 + \cdots + x_s\xi_s$,

1. (Pre)compute $M = (m_{ij}) = (\langle \xi_i, \xi_j \rangle)$ for $0 \leq i, j \leq s$;
2. Compute $v = (v_i) = (\langle \psi, \xi_i \rangle)$ for $0 \leq i \leq s$;
3. Solve for $(c, x_1, \ldots, x_s) = vM^{-1}$ (over $\mathbb{Z}/r\mathbb{Z}$).

Toy example

Let $\mathscr{E}$ be a supersingular elliptic curve, with $\mathrm{End}(\mathscr{E}) \supseteq \mathbb{Z}\langle i, j, k\rangle$ where $i^2 = -a$, $j^2 = -b$, $k^2 = ab$. Suppose $(\xi_1, \xi_2, \xi_3) = (i, j, k)$.

Endomorphism pairing:

$$\langle \alpha, \beta \rangle = \mathrm{Tr}(\alpha\beta^\dagger) = \alpha\beta^\dagger + \beta\alpha^\dagger$$

where $(t + xi + yj + zk)^\dagger = t - (xi + yj + zk)$.

Given $\psi = [c] + x_1 i + x_2 j + x_3 k$, we have

$$\begin{aligned}
\langle \psi, 1 \rangle &= (c + x_1 i + x_2 j + x_3 k) + (c - x_1 i - x_2 j - x_3 k) &&= 2 \cdot c \\
\langle \psi, i \rangle &= (c + x_1 i + x_2 j + x_3 k)(-i) + i(c - x_1 i - x_2 j - x_3 k) &&= 2a \cdot x_1 \\
\langle \psi, j \rangle &= (c + x_1 i + x_2 j + x_3 k)(-j) + j(c - x_1 i - x_2 j - x_3 k) &&= 2b \cdot x_2 \\
\langle \psi, k \rangle &= (c + x_1 i + x_2 j + x_3 k)(-k) + k(c - x_1 i - x_2 j - x_3 k) &&= -2ab \cdot x_3
\end{aligned}$$

Computing the endomorphism pairing

How do you compute the endomorphism pairing $\langle \cdot, \cdot \rangle$?

Classical solution (see e.g. Mumford): **intersection theory**.

- If endomorphisms are presented using **divisors/bundles** on A, then use intersection theory on those divisors.

Computing the endomorphism pairing

How do you compute the endomorphism pairing $\langle \cdot, \cdot \rangle$?

Classical solution (see e.g. Mumford): **intersection theory**.

- If endomorphisms are presented using **divisors/bundles** on A, then use intersection theory on those divisors.
- If endomorphisms are presented as **rational maps**, then use intersection theory on the graphs.

Computing the endomorphism pairing

How do you compute the endomorphism pairing $\langle \cdot, \cdot \rangle$?

Classical solution (see e.g. Mumford): **intersection theory**.

- If endomorphisms are presented using **divisors/bundles** on A, then use intersection theory on those divisors.
- If endomorphisms are presented as **rational maps**, then use intersection theory on the graphs.
- If $A = J_C$ and endomorphisms are **correspondences** on $C \times C$, then use intersection theory on correspondences (see e.g. S's thesis).

Computing the endomorphism pairing

How do you compute the endomorphism pairing $\langle \cdot, \cdot \rangle$?

Classical solution (see e.g. Mumford): **intersection theory**.

- If endomorphisms are presented using **divisors/bundles** on A, then use intersection theory on those divisors.
- If endomorphisms are presented as **rational maps**, then use intersection theory on the graphs.
- If $A = J_C$ and endomorphisms are **correspondences** on $C \times C$, then use intersection theory on correspondences (see e.g. S's thesis).
- In some situations, one could compute the matrices of $\psi_1 \circ \psi_2{}^\dagger$ on **low-degree torsion** subgroups $A[\ell]$, and **CRT** the traces of these matrices.

The moral of the story

If you can compute efficiently with elements of $\mathbb{G}_3$, then you can compute the pairing $\langle \cdot, \cdot \rangle$ on $\mathbb{G}_3$.

So: if you can efficiently compute the trilinear map, then you can efficiently break its $\mathbb{G}_3$.