The fall and rise and fall and rise of supersingular elliptic curves (in cryptography)

Steven Galbraith
University of Auckland, New Zealand
Thanks

- Alice Silverberg.
- Karl Rubin, Kristin Lauter, Nathan Kaplan.
- David Kohel, Bryan Birch, Victor Miller, Gerhard Frey, George Rück, Florian Hess, Nigel Smart, Alfred Menezes, Scott Vanstone, David Jao, Drew Sutherland, Gaetan Bisson, Christophe Petit, Luca de Feo.
- Anton Stolbunov, Ilya Chevyrev, Chang-An Zhao, Fangqian (Alice) Qiu, Christina Delfs, Barak Shani, Yan Bo Ti, Javier Silva, Joel Laity.
Plan

Miller & Koblitz

1980

Menezes
Okamoto
Vanstone
Frey-Rück

2000

SOK
Joux
BF

Charles
Goren
Lauter

Jao
DeFeo

2020

Joux et al
Granger et al

Steven Galbraith
Supersingular Elliptic Curves
Discrete Logarithm Problem and Diffie-Hellman

Let $G$ be a subgroup of $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$ of prime order. Given $g \in G$ and $h = g^a$, it is hard to compute $a$.

Diffie-Hellman key exchange:
- Alice chooses $a$ and sends $t_A = g^a$ to Bob.
- Bob chooses $b$ and sends $t_B = g^b$ to Alice.
- Alice computes $t_B^a = g^{ab}$.
- Bob computes $t_A^b = g^{ab}$. 

Steven Galbraith
Supersingular Elliptic Curves
Enter Elliptic Curves

- V. Miller “Use of elliptic curves in cryptography” (CRYPTO 1985).
Since \( E(\mathbb{F}_q) \) is a finite Abelian group one can do the Diffie-Hellman protocol using elliptic curves.

An elliptic curve \( E \) over \( \mathbb{F}_p \) is supersingular if \( \#E(\mathbb{F}_p) \equiv 1 \) (mod \( p \)).

Koblitz suggests to use \( y^2 + y = x^3 \) over \( \mathbb{F}_{2^n} \) because if \( P = (x, y) \) then

\[
\]

“The formulas for doubling a point are particularly simple”

“In addition, there is an easy formula”

\[
\#E(\mathbb{F}_{2^n}) = 2^n + 1 - 2(-2)^{n/2}.
\]
Pairings

- Let $E$ be an elliptic curve over $\mathbb{F}_q$ and $N$ coprime to $q$ and $E[N] = \{ P \in E(\mathbb{F}_q) : [N]P = 0 \}$.
- The Weil pairing is a function $e_N : E[N] \times E[N] \to \mathbb{F}_q^*$.
- V. Miller (1986) explained how to efficiently compute the Weil pairing.
- A. Menezes, T. Okamoto and S. Vanstone (1993) showed that one can reduce the DLP on a supersingular elliptic curve over $\mathbb{F}_q$ to a finite field DLP in $\mathbb{F}_{q^k}^*$ for $k \leq 6$, where one has more efficient algorithms for DLP.
- G. Frey and H.-G. Rück (1994) also described and generalised this approach.
Early 1990s

- Miller & Koblitz
- Menezes, Okamoto, Vantone, Frey-Rück

2000:
- SOK
- Joux BF
- Charles, Goren, Lauter

2020:
- Jao DeFeo
- Joux et al. Granger et al.
Supersingular curves are weak for crypto

- When I started working on ECC in 1997 the mantra was: Avoid supersingular curves, they are weak for crypto.
- N. Koblitz, “An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm”, CRYPTO 1998. Let $E$ be the elliptic curve $y^2 = x^3 - x - (-1)^a$ over $\mathbb{F}_3$, then for odd $n$
  \[
  \#E(\mathbb{F}_{3^n}) = 3^n + 1 - (-1)^a(\frac{3}{n})3^{(n+1)/2}.
  \]
Pairing-based crypto

- These papers suggested supersingular curves would be perfect for pairing-based crypto.
Embedding degrees

- Embedding degree of $E(\mathbb{F}_q)$ and $N \mid \#E(\mathbb{F}_q)$ is minimal $k$ such that $e_N : E[N] \times E[N] \to \mathbb{F}_{q^k}^*$.

- There became an industry to determine curves such that the field extension $\mathbb{F}_{q^k}$ for the pairing was appropriately sized.

  - Supersingular curves in characteristic 2 or 3 good for pairings.
  - Largest embedding degree for supersingular elliptic curves $E/\mathbb{F}_{2^n}$ is $k = 4$, and for $E/\mathbb{F}_{3^n}$ is $k = 6$.


Early 2000s

1980
Miller & Koblitz

1990
Menezes
Okamoto
Vanstone
Frey-Rück

2000
SOK
Joux
BF
Charles
Goren
Lauter

2020
Jao
DeFeo

Joux et al
Granger et al

Supersingular Elliptic Curves
Finite field discrete logs

- In early 2013 two teams announced major breakthroughs:
  - Antoine Joux, A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic.

- New computational records:
  - $F_{2^{1778}}$ ($1778 = 14 \times 127$) (Joux, Feb 2013)
  - $F_{2^{1971}}$ ($1971 = 3^3 \times 73$) (Granger et al, Feb 2013)
  - $F_{2^{3164}}$ ($3164 = 2^2 \times 7 \times 113$) (Granger et al, March 2013)
  - $F_{2^{4080}}$ ($4080 = 2^4 \times 3 \times 17$) (Joux, March 2013)
  - $F_{2^{6120}}$ ($6120 = 2^3 \times 3 \times 255$) (Granger et al, April 2013)
  - $F_{2^{6168}}$ ($257 \times 24 = 6168$) (Joux, May 2013)
  - $F_{2^{9234}}$ ($9234 = 2 \times 3^5 \times 19$) (Granger, Kleinjung, Zumbrägel, January 2014)
Incomplete list of references


- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Weakness of $GF(3^{6\cdot509})$ for Discrete Logarithm Cryptography (2013)

- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Computing Discrete Logarithms in $GF(3^{6\cdot137})$ and $GF(3^{6\cdot163})$ Using Magma (2014)

- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Weakness of $GF(3^{6\cdot1429})$ and $GF(2^{4\cdot3041})$ for discrete logarithm cryptography (2015)
New Cryptographic applications of supersingular curves

- D. X. Charles, K. E. Lauter and E. Z. Goren, Cryptographic hash functions from expander graphs (2005)
- D. Jao and L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (2011)
- L. De Feo, D. Jao and J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (2014)
Generalised Discrete Logarithm Problem: Homogenous Spaces

(Couveignes 1997)

Let $G$ be a subgroup of $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$ of prime order $p$. For $a \in \mathbb{Z}/(p - 1)\mathbb{Z}$ (or, better, $a \in (\mathbb{Z}/(p - 1)\mathbb{Z})^*$) and $g \in G$ define $a * g := g^a$. Given $g \in G$ and $h = a * g$, hard to compute $a$.

Generalised Diffie-Hellman key exchange:

- Alice chooses $a \in \mathbb{Z}_p$ and sends $t_A = a * g$ to Bob.
- Bob chooses $b \in \mathbb{Z}_p$ and sends $t_B = b * g$ to Alice.
- Alice computes $a * t_B$.
- Bob computes $b * t_A$.
Isogenies

- An isogeny $\phi : E_1 \to E_2$ of elliptic curves is a (non-constant) morphism and a group homomorphism.
- An isogeny has finite kernel.
- Given a finite subgroup $G \subseteq E_1(\overline{\mathbb{F}}_q)$ there is a (unique separable) isogeny $\phi_G : E_1 \to E_2$ with kernel $G$.
- Can compute $\phi_G$ using Vélu.
- We will write $E_2 = E_1 / G$.
- We focus on separable isogenies, in which case $\deg(\phi) = \# \ker(\phi)$.
- $\text{End}(E) = \{\text{isogenies } \phi : E \to E \text{ over } \overline{\mathbb{F}}_q \} \cup \{0\}$. 

Steven Galbraith
Supersingular Elliptic Curves
Let $E$ be an ordinary elliptic curve over $\mathbb{F}_q$ with $\text{End}(E) \cong \mathcal{O}$ an order in an imaginary quadratic field.

Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal.

Can define the subgroup

$$E[\mathfrak{a}] = \{ P \in E(\overline{\mathbb{F}}_q) : \phi(P) = 0 \ \forall \phi \in \mathfrak{a} \}.$$  

(Waterhouse 1969)

There is an isogeny $E \to E'$ with kernel $E[\mathfrak{a}]$. Define $\mathfrak{a} \ast E$ to be $E' = E/E[\mathfrak{a}]$.

$\mathfrak{a} \ast E$ depends only on the ideal class of $\mathfrak{a}$.

This gives an action of the ideal class group $\text{Cl}(\mathcal{O})$ on the set of $E$ with $\text{End}(E) \cong \mathcal{O}$.  

Steven Galbraith  
Supersingular Elliptic Curves
Ordinary Isogeny Graph

Credit: Dustin Moody
Class Group Actions from Isogenies

- A. Stolbunov “Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves” (2010)
- Couveignes describes a Diffie-Hellman-type key exchange based on group actions. Does not mention post-quantum security.
- Rostovtsev and Stolbunov give key exchange and encryption. Suggest isogenies could be post-quantum secure.
- Stolbunov’s thesis describes also mentions signatures.
Generalised Diffie-Hellman using Group Action

\[ a \ast E \quad \rightarrow \quad ab \ast E \]
\[ E \quad \rightarrow \quad b \ast E \]

Steven Galbraith
Supersingular Elliptic Curves
Computational problems and algorithms

- Given $E$ and $E' = \alpha \ast E$ to determine the ideal (class) $\alpha$.
- Equivalently: Find any efficiently computable isogeny $\phi : E \to E'$.
- Classical algorithms due to Galbraith and Galbraith-Hess-Smart in time $\tilde{O}(\sqrt{\#G})$ (bug fixed by Stolbunov).
- Hidden shift problem: $G$ an abelian group and $f, g : G \to S$ such that, for some $s \in G$, $g(x) = f(xs)$ for all $x \in G$. Problem: find $s$.
- Idea: Given $(E, E' = \alpha \ast E)$ define $f(b) = b \ast E$ and $g(b) = b \ast E' = f(b\alpha)$. 

Steven Galbraith

Supersingular Elliptic Curves
Quantum algorithms for hidden shift

- Kuperberg (2004, 2011) gave subexponential-time quantum algorithms for hidden shift. Complexity\(^1\) \(2^{O(\sqrt{\log(\#G)})}\).
- For certain groups Kuperberg states the time complexity is \(\tilde{O}(2^{1.8\sqrt{\log(\#G)}})\).
- Require massive quantum storage, which may be unrealistic.

\(^1\)This is taking cost \(O(1)\) for the functions \(f\) and \(g\).
Kuperberg for isogenies

A. Childs, D. Jao and V. Soukharev were the first to analyse Kuperberg’s algorithm in the isogeny setting.

Subexponential complexity arises twice in their work:

- Computing $a \ast E$ requires smoothing the ideal class over a factor base.\(^2\)
- Kuperberg itself.


Claim there is a quantum algorithm in the isogeny case with running time $\tilde{O}(2^{1.8 \sqrt{\log(\#G)})}$, but details are sketchy.

Also see:


\(^2\)This step improved by Biasse, Fieker and Jacobson in ANTS 2016.
Open problems

- The Kuperberg and Regev algorithms mostly classical and combinatorial. Very like the Blum-Kalai-Wasserman (BKW) and Wagner algorithms.


- Algorithmic number theorists should study these algorithms.

- Kuperberg/Regev has only been used as a black box. Are there further optimisations/approaches/algorithms that exploit the specific features of isogenies?
Efficient group action DH protocol

\[ E \xrightarrow{a} a \ast E \xrightarrow{ab} ab \ast E \xleftarrow{b} b \ast E \]
Efficient group action DH protocol

- Need to sample ideal class as product of powers of small prime ideals:

\[ a \equiv \prod_{i} l_i^{e_i} \]

where \( l_i \) are non-principal \( \mathcal{O} \)-ideals of small prime norm.

- Then compute corresponding isogenies.

- Couveignes and Stolbunov do this by choosing random small split primes ("Elkies primes"), using modular polynomials and action of Frobenius on kernels.

- Couveignes: time required "a few hours".

- Stolbunov: compute \( a \ast E \) in 4 minutes or so.

- De Feo, Kieffer and Smith (eprint 2018/485) discuss choosing a special curve to make the isogeny computations faster.
Let $X$ be the set of isomorphism classes of supersingular elliptic curves $E$ with $j$-invariant in $\mathbb{F}_p$.

All $E \in X$ have $\text{End}_{\mathbb{F}_p}(E)$ an order in $\mathbb{Q}(\sqrt{-p})$. Here $\text{End}_{\mathbb{F}_p}(E) = \{ \phi : E \to E \text{ defined over } \mathbb{F}_p \}$.

C. Delfs and S. D. Galbraith (2016) showed that one can define class group actions on $X$.

CSIDH is an instantiation of group action crypto using supersingular curves, which gives massive performance improvements.

Advantages over Jao-De Feo (SIDH) include:

- No public key validation needed, so can do non-interactive key exchange.
- Better bandwidth.

Con: only sub-exponentially quantum secure.
Open problems

▶ How close to uniform is the distribution

\[ a \equiv \prod_{i} l_i^{e_i} \]

over uniform \( e_i \in [-B, B] \), for fixed small prime ideals \( l_i \)?
(Let’s assume \( \{l_i\} \) generates the class group.)

▶ Can small prime factors of \( \#\text{Cl}(\mathcal{O}) \) be determined?
Can subgroups of ideal class group be exploited?

▶ (Boneh): Find other homogeneous spaces/torsors for group actions that are efficient and secure for crypto.
Candidate post-quantum pairing

Recent paper by Boneh, Glass, Krashen, Lauter, Sharif, Silverberg, Tibouchi and Zhandry (eprint 2018/665).

- Fix **ordinary** $E / \mathbb{F}_q$
- Fact: $(a_1 * E) \times (a_2 * E) \cong (a_1 a_2 * E) \times E$ as unpolarized abelian varieties.
  (Result holds more generally for $n$ terms; see Kani 2011.)
- This is essentially a bilinear pairing (resp. multilinear map).
- Not used for key exchange, but other more complex protocols.
- **Open problem:** To find a computable invariant of the isomorphism class.
- **Application:** Algorithm to solve the decisional Diffie-Hellman problem for class group actions in the ordinary case (but not the supersingular case).
Jao and De Feo key exchange (SIDH)

- D. Jao and L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (2011)
- Different use of supersingular curves.
- Best algorithm to solve the isogeny problem is exponential-time.
- I won’t explain in this talk.
SIKE submission to NIST PQ Standardisation

- SIKE = Supersingular Isogeny Key Exchange.
- Submission to the NIST standardization process on post-quantum cryptography.
- Authors: Jao, Azarderakhsh, Campagna, Costello, De Feo, Hess, Jalali, Koziel, LaMacchia, Longa, Naehrig, Renes, Soukharev and Urbanik.
- Submission contains specification of an IND-CCA KEM.
- http://sike.org/
- Advantage over lattice crypto: very short ciphertexts. CSIDH is even better.
Public Key Signatures

- L. De Feo and S. Galbraith “SeaSign: Compact isogeny signatures from class group actions”, eprint 2018/824.
- Public key: $E$ and $E_A = a \ast E$ where
  \[ a \equiv \prod_i l_i^{e_i} \]
  and $l_i$ ideals of small prime norm, $|e_i| \leq B$.
- Signer generates random ideals $b_k = \prod_{i=1}^n l_i^{f_{k,i}}$ for $1 \leq k \leq t$ and computes $E_k = b_k \ast E$.
- Compute $H(j(E_1), \ldots, j(E_t), \text{message})$ where $H$ is a cryptographic hash function with $t$-bit output $b_1, \ldots, b_t$.
- If $b_k = 0$ signature includes $f_k = (f_{k,1}, \ldots, f_{k,n})$ and if $b_k = 1$ it includes
  \[ f_k - e = (f_{k,1} - e_1, \ldots, f_{k,n} - e_n). \]
- Use Lyubashevsky’s “Fiat-Shamir with aborts”.

Steven Galbraith
Supersingular Elliptic Curves
Today

1980
Miller & Koblitz

1990
Menezes
Okamoto
Vanstone
Frey-Rück

2000
SOK
Joux
BF

2010
Charles
Goren
Lauter

2020
Jao
DeFeo

Joux et al
Granger et al
The future of supersingular elliptic curves

Steven Galbraith

Supersingular Elliptic Curves
Conclusion

- Elliptic curve crypto is still very active after more than 30 years, and supersingular elliptic curves have been a major character in the drama.
- There are (still) plenty of good problems for arithmetic geometers and algorithmic number theorists to study.
- I’m happy to discuss these problems with you during the workshop.
Thank You