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

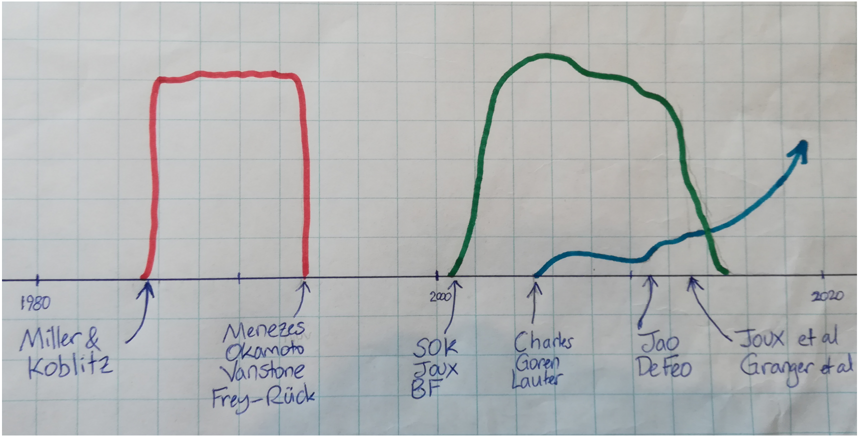
Steven Galbraith

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


1980
2000
2020
Miller &
Koblitz
Menezes
Okamoto
Vanstone
Frey-Rück
SOK
Joux
BF
Charles
Goren
Lauter
Jao
De Feo
Joux et al
Granger et al

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 $t_A^b = g^{ab}$.

Enter Elliptic Curves

- R. Schoof. Polynomial-time algorithm to count points on elliptic curves over $\mathbb{F}_p$.
  (Technical report 1983; Math. Comp. 1985)
- H. W. Lenstra Jr. Elliptic curve factoring.
  (Announced 1984/1985 ; Annals 1987)
- V. Miller "Use of elliptic curves in cryptography" (CRYPTO 1985).
- N. Koblitz "Elliptic Curve Cryptosystems" (Math. Comp. 1987).

Supersingular Elliptic Curves

- 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 $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$.
- Koblitz suggests to use $y^2 + y = x^3$ over $\mathbb{F}_{2^n}$ because if $P = (x, y)$ then

$$[2]P = P + P = (x^4, y^4 + 1).$$

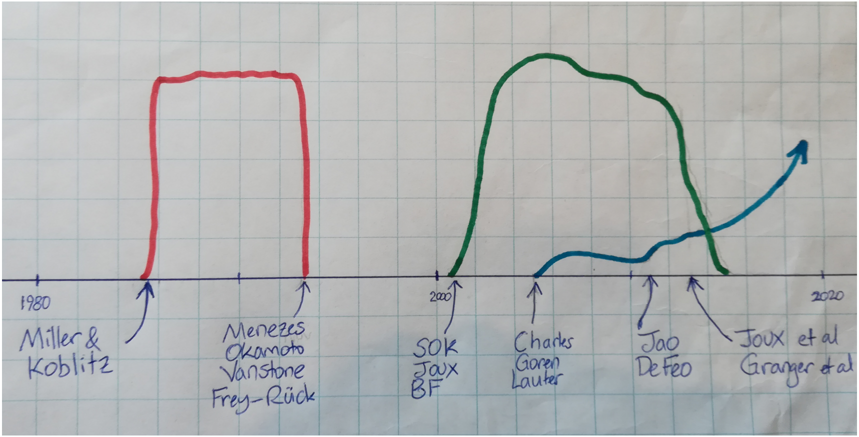
  "The formulas for doubling a point are particularly simple"
- "In addition, there is an easy formula"

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

Pairings

- Let E be an elliptic curve over $\mathbb{F}_q$ and N coprime to q and $E[N] = \{P \in E(\overline{\mathbb{F}}_q) : [N]P = 0\}$.
- The Weil pairing is a function $e_N : E[N] \times E[N] \to \overline{\mathbb{F}}_q^*$.
- 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


1980
2000
2020
Miller & Koblitz
Menezes Okamoto Vanstone
Frey–Rück
SOK
Joux
BF
Charles
Goren
Lauter
Jao
De Feo
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

$$\#E(\mathbb{F}_{3^n}) = 3^n + 1 - (-1)^a (\tfrac{3}{n}) 3^{(n+1)/2}.$$

- A. K. Lenstra and E. R. Verheul, "The XTR public key system", CRYPTO 2000.
- E. R. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", EUROCRYPT 2001.

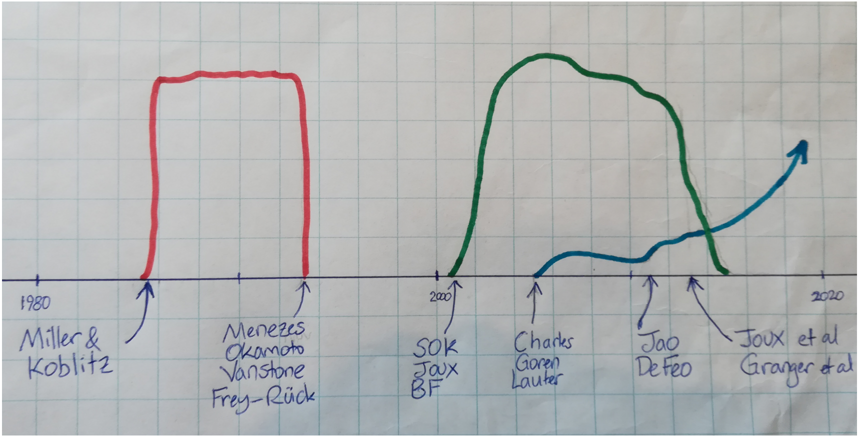
Pairing-based crypto

- R. Sakai, K. Ohgishi, M. Kasahara "Cryptosystems based on pairing" (2000)
- A. Joux, "A one round protocol for tripartite DiffieHellman" (2000)
- D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing" (2001)
- 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.
- S. Galbraith, "Supersingular Curves in Cryptography", ASIACRYPT 2001.
  - 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 $k = 6$.
- K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology", CRYPTO 2002.
- K Rubin, A. Silverberg, "Torus-based cryptography", CRYPTO 2003.

Early 2000s


1980
2000
2020
Miller & Koblitz
Menezes
Okamoto
Vanstone
Frey–Rück
SOK
Joux
BF
Charles
Goren
Lauter
Jao
De Feo
Joux et al
Granger et al

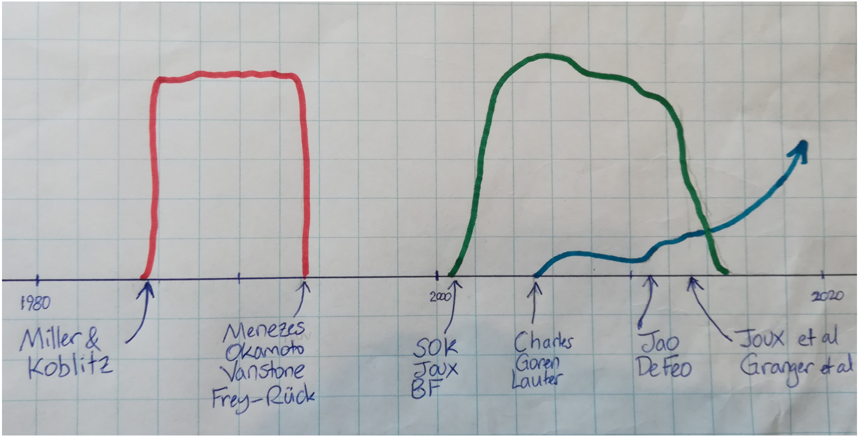
Finite field discrete logs

- 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.
  - Faruk Gölogl u, Robert Granger, Gary McGuire and Jens Zumbrägel, On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $F_{2^{1971}}$.
- New computational records:
  - $\mathbb{F}_{2^{1778}}$ $(1778 = 14 * 127)$ (Joux, Feb 2013)
  - $\mathbb{F}_{2^{1971}}$ $(1971 = 3^3 * 73)$ (Granger et al, Feb 2013)
  - $\mathbb{F}_{2^{3164}}$ $(3164 = 2^2 * 7 * 113)$ (Granger et al, March 2013)
  - $\mathbb{F}_{2^{4080}}$ $(4080 = 2^4 * 3 * 17)$ (Joux, March 2013))
  - $\mathbb{F}_{2^{6120}}$ $(6120 = 2^3 * 3 * 255)$ (Granger et al, April 2013)
  - $\mathbb{F}_{2^{6168}}$ $(257 * 24 = 6168)$ (Joux, May 2013)
  - $\mathbb{F}_{2^{9234}}$ $(9234 = 2 * 3^5 * 19)$ (Granger, Kleinjung, Zumbrägel, January 2014)

Incomplete list of references

- R. Barbulescu, P. Gaudry, A. Joux and E. Thomé, A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic (2014)
- F. Göloglu, R. Granger, G. McGuire, J. Zumbrägel, On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$, (2013)
- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Weakness of $GF(3^{6\cdot 509})$ for Discrete Logarithm Cryptography (2013)
- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Computing Discrete Logarithms in $GF(3^{6\cdot 137})$ and $GF(3^{6\cdot 163})$ Using Magma (2014)
- G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez, Weakness of $GF(3^{6\cdot 1429})$ and $GF(2^{4\cdot 3041})$ for discrete logarithm cryptography (2015)

2013-2015


1980
2000
2020
Miller &
Koblitz
Menezes
Okamoto
Vanstone
Frey–Rück
SOK
Joux
BF
Charles
Goren
Lauter
Jao
De Feo
Joux et al
Granger et al

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 ϕ_G using Vélu.
- We will write $E_2 = E_1/G$.
- We focus on separable isogenies, in which case $\deg(\phi) = \# \ker(\phi)$.
- $\mathrm{End}(E) = \{\text{isogenies } \phi : E \to E \text{ over } \overline{\mathbb{F}}_q\} \cup \{0\}$.

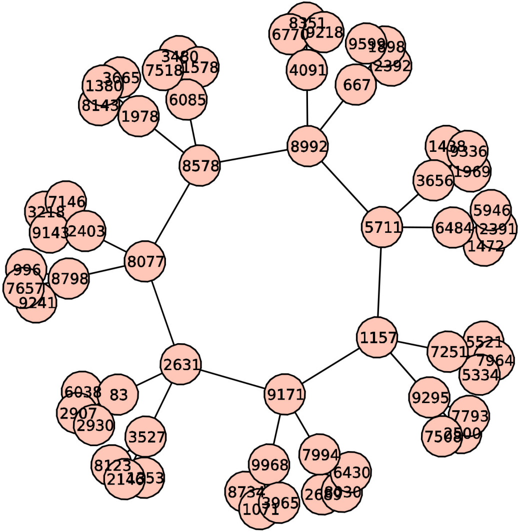
Class Group Action on Elliptic Curves

- Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}(E) \cong \mathcal{O}$ 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 $\mathfrak{a} * E$ to be $E' = E/E[\mathfrak{a}]$.
- $\mathfrak{a} * E$ depends only on the ideal class of $\mathfrak{a}$.
- This gives an action of the ideal class group $\mathrm{Cl}(\mathcal{O})$ on the set of E with $\mathrm{End}(E) \cong \mathcal{O}$.

Ordinary Isogeny Graph



Credit: Dustin Moody

Class Group Actions from Isogenies

- J.-M. Couveignes “Hard Homogeneous Spaces”, preprint (1997/2006)
- A. Rostovtsev, A. Stolbunov, preprint (2006)
- 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

$$\begin{tikzcd}
 & \mathfrak{a} * E \arrow[dr] & \\
E \arrow[ur] \arrow[dr] & & \mathfrak{a}\mathfrak{b} * E \\
 & \mathfrak{b} * E \arrow[ur] &
\end{tikzcd}$$

Computational problems and algorithms

- Given E and $E' = \mathfrak{a} * E$ to determine the ideal (class) $\mathfrak{a}$.
- 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 $(E, E' = \mathfrak{a} * E)$ define $f(\mathfrak{b}) = \mathfrak{b} * E$ and $g(\mathfrak{b}) = \mathfrak{b} * E' = f(\mathfrak{b}\mathfrak{a})$.

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.
- Regev (2004) gave low quantum storage variant.

[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 $\mathfrak{a} * E$ requires smoothing the ideal class over a factor base.[2]
  - Kuperberg itself.
- X. Bonnetain and A. Schrottenloher, "Quantum security analysis of CSIDH and ordinary isogeny-based schemes", eprint 2018/537. 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:
  - J.-F. Biasse, A. Iezzi and M. Jacobson, "A note on the security of CSIDH", arXiv:1806.03656.
  - D. Jao, J. LeGrow, C. Leonardi and L. Ruiz-Lopez, "A polynomial quantum space attack on CRS and CSIDH" (MathCrypt 2018)

[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.
- Regev ("Quantum computation and lattice problems", SIAM J. Comput. 2004) reduces shortest vector problem in lattice to dihedral hidden subgroup.
  Conversely, should be able to improve Kuperberg by using lattice methods.
- 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

$$\begin{tikzcd}
 & \mathfrak{a} * E \arrow[dr] & \\
E \arrow[ur] \arrow[dr] & & \mathfrak{a}\mathfrak{b} * E \\
 & \mathfrak{b} * E \arrow[ur] &
\end{tikzcd}$$

Efficient group action DH protocol

- Need to sample ideal class as product of powers of small prime ideals:
$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$
where $\mathfrak{l}_i$ 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 $\mathfrak{a} * E$ in 4 minutes or so.
- De Feo, Kieffer and Smith (eprint 2018/485) discuss choosing a special curve to make the isogeny computations faster.

CSIDH (Castryck, Lange, Martindale, Panny, Renes 2018)

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

$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$

  over uniform $e_i \in [-B, B]$, for fixed small prime ideals $\mathfrak{l}_i$? (Let's assume $\{\mathfrak{l}_i\}$ generates the class group.)
- Can small prime factors of $\#\mathrm{Cl}(\mathcal{O})$ 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: $(\mathfrak{a}_1 * E) \times (\mathfrak{a}_2 * E) \cong (\mathfrak{a}_1\mathfrak{a}_2 * E) \times E$ 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 supersigular 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 $E_A = \mathfrak{a} * E$ where

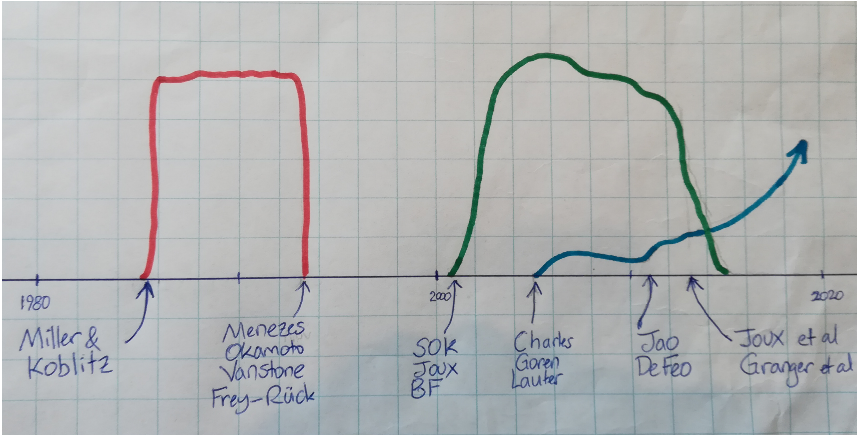
$$\mathfrak{a} \equiv \prod_i \mathfrak{l}_i^{e_i}$$

  and $\mathfrak{l}_i$ ideals of small prime norm, $|e_i| \leq B$.
- Signer generates random ideals $\mathfrak{b}_k = \prod_{i=1}^n \mathfrak{l}_i^{f_{k,i}}$ for $1 \leq k \leq t$ and computes $\mathcal{E}_k = \mathfrak{b}_k * E$.
- Compute $H(j(\mathcal{E}_1), \ldots, j(\mathcal{E}_t), \text{message})$ where H is a cryptographic hash function with t-bit output $b_1, \ldots, b_t$.
- If $b_k = 0$ signature includes $\mathbf{f}_k = (f_{k,1}, \ldots, f_{k,n})$ and if $b_k = 1$ it includes

$$\mathbf{f}_k - \mathbf{e} = (f_{k,1} - e_1, \ldots, f_{k,n} - e_n).$$

- Use Lyubashevsky's "Fiat-Shamir with aborts".

Today



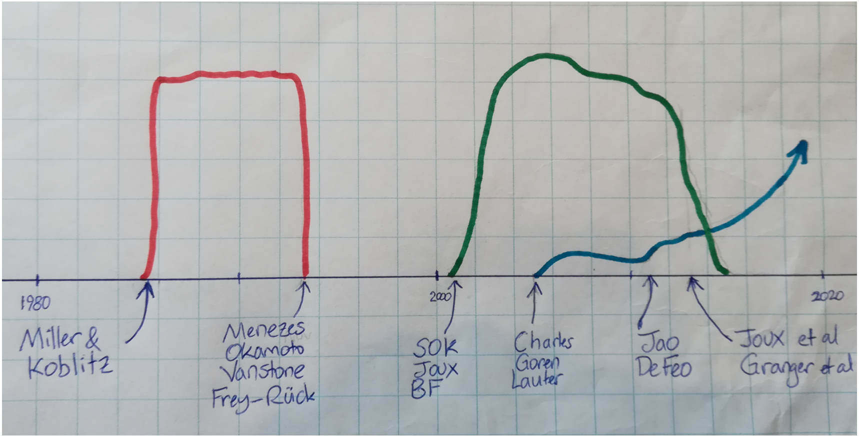
1980
2000
2020
Miller & Koblitz
Menezes Okamoto Vanstone
Frey-Rück
SOK
Joux
BF
Charles
Goren
Lauter
Jao
De Feo
Joux et al
Granger et al

The future of 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


1980
2000
2020
Miller &
Koblitz
Menezes
Okamoto
Vanstone
Frey–Rück
SOK
Joux
BF
Charles
Goren
Lauter
Jao
De Feo
Joux et al
Granger et al