Arpin and Martindale - Lecture I
Mathematics of Isogeny-Based Crypto

Generally: over $\mathbb{F}_p$, $\mathbb{F}_q$ w/ $q = p^n$, or $\overline{\mathbb{F}}_p$

"The Isogeny Problem"

> Given: E, E' supersingular $/\overline{\mathbb{F}}_p$,
> find $\varphi : E \to E'$.

Tate: $E, E' / \mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ iff $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$

~~Move~~ Moreover, supersingular e.c.'s over $\overline{\mathbb{F}}_p$ form a single isogeny class, and $\exists\, \varphi : E \to E'$ w/ $\deg \varphi = \ell^e$, for any $\ell \neq p$.

"Endomorphism Ring Problem"

> Given E supersingular $/\overline{\mathbb{F}}_p$, compute $\mathrm{End}\,E$.

Deuring: $\mathrm{End}(E)$ is a max. order in the quaternion alg.

$$\mathrm{End}\,E \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$$

$$\mathrm{End}\,E \cong \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$$

"One Endomorphism Problem"

... find one nonscalar endomorphis

$$\mathrm{OEP} = \mathrm{ERP} = \mathrm{IP}$$

Page Wesolowski

Eisenträger-Hallgren Lauter-Morrison-Petit Wesolowski

Cryptography:

Computations are efficient, but security relies on some hard problems (computationally)

Efficient: $E/\mathbb{F}_p$ supersing. has $j(E) \in \mathbb{F}_{p^2}$, and isogenies of smooth degree are easy to compute.

Hard: Specifying E and E', it's hard to find $\varphi: E \to E'$.

Endomorphism Rings + Isogenies

$p = 103$; $E : y^2 = x^3 - x \quad / \mathbb{F}_p$

$\mathrm{End}(E) \subseteq B_{p,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$

with $i^2 = -1$, $j^2 = -p$, $ij = -ji$

$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+ij}{2}$

w/ $j = (x, y) \longmapsto (x^p, y^p)$

$i = (x, y) \mapsto (-x, \sqrt{-1}\,y)$

Left ideal $I = \left(2, 2i, \frac{1+j}{2}, \frac{i+ij}{2}\right)$

$N(I) = 2$; $E[I] = \{P \in E : \alpha(P) = O_E \ \forall \alpha \in I\}$

$E[I] \subseteq E[2] = \{O_E, \underbrace{(0,0)}_{P}, \underbrace{(1,0)}_{Q}, (-1,0)\}$

What is $E[I]$?

$\mathbb{F}_{103^2} = \mathbb{F}_{103}[s]/(s^2+1)$

$[2]$ and $[2i]$ kill all of $E[2]$.

$\rightsquigarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ wrt P, Q

For $\frac{1+j}{2}$, $\frac{i+ij}{2}$, look at $E[4]$:

$E[4] = \langle R = (66, 67), T = (s, -s+1) \rangle$

$[2]R = Q$ and $[2]T = P$.

$$\left(\frac{1+j}{2}\right)(Q) = \left(\frac{1+j}{2}\right)(2R) = (1+j)(R)$$
$$= Q$$

$$\left(\frac{1+j}{2}\right)(P) = (1+j)(T) = Q$$

Likewise for $\frac{i+ij}{2}$

$$E[I] = \{O_E, P+Q\}$$

SQIsign De Feo - Kohel - Leroux - Petit - Wesolowski

Digital Signature built from a Σ-protocol: 3 round proof of knowledge.

Public Parameters: E_0 supersingular over $\overline{\mathbb{F}}_p$ with known $\mathrm{End}(E_0)$

Prover		Verifier
$\tau : E_0 \to E_p$		
E_p	$\xrightarrow{\text{public key}}$	
$\varphi_{com} : E_0 \to E_{com}$		
E_{com}	$\xrightarrow{\text{commit.}}$	
	$\xleftarrow{\text{chal}}$	$\{\varphi_{chal} : E_{com} \to E_{chal}$

$\eta = \varphi_{chal} \circ \varphi_{com} \circ \hat{\tau}$

$\eta : E_p \to E_{chal}$

$\eta \neq \varphi_{resp.} : E_p \to E_{chal} \xrightarrow{\text{resp.}}$

$$\begin{tikzcd}
E_0 \arrow[r, "\tau"] \arrow[d, "\varphi_{com}"'] & E_p \arrow[d, "\eta"'] \arrow[d, bend left=60, "\varphi_{resp}"] \\
E_{com} \arrow[r, "\varphi_{chal}"] & E_{chal}
\end{tikzcd}$$

$$\eta \overset{?}{\rightsquigarrow} \varphi_{resp}.$$

<u>KLPT</u>