Multiparty Non-Interactive Key Exchange From Isogenies on Elliptic Curves

Shahed Sharif

1 Introduction

The following is joint work with Dan Boneh, Darren Glass, Daniel Krashen, Kristin Lauter, Alice Silverberg, Mehdi Tibouchi, and Mark Zhandry.

Our goal is to describe an incomplete protocol, and a description of what is necessary to make it complete.

2 Multiparty protocol

2.1 CM curves

We fix an ordinary elliptic curve \( E/\mathbb{F}_q \). Let \( \mathcal{O} = \text{End} E \) and \( K = \mathcal{O} \otimes \mathbb{Q} \). We know that \( K \) is an iqf and \( \mathcal{O} \) is an order in \( K \); we will assume for convenience that \( \mathcal{O} \) is the maximal order. Let \( S_1 \) be the set of isomorphism classes of elliptic curves over \( \mathbb{F}_q \) which have endomorphism ring isomorphic to \( \mathcal{O} \), and hence are isogenous to \( E \). (Note these are isogenous over \( \mathbb{F}_q \) since the endomorphism rings are the same.) By the theory of complex multiplication, there is a transitive action of the class group \( \text{Cl} \mathcal{O} \) on \( S_1 \). The action can be defined in two different ways. The more intrinsic way is as follows: for \( I \subset \mathcal{O} \) an (integral) ideal, define \( E[I] := \{ P \in E : f(P) = O \forall f \in I \} \).

Let \( E_I \) to be the quotient \( E/E[I] \), and \( \varphi_I : E \to E_I \) the canonical projection. We say that \( [I] * E = E_I \). Observe that \( E_I \in S_1 \). Also observe that if \( I = (\alpha) \), then \( \varphi_I = \alpha \) and so \( E_I = E \). It follows that \( E_I \) depends only on the ideal class of \( I \).

The other way to define our action is to use the Deuring lift: that is, there is a curve \( \bar{E} \) over a number field \( H \) and a prime \( p \) of \( H \) lying over \( p \) such that

- \( \bar{E} \) reduces to \( E \) mod \( p \),
- \( \bar{E} \) has CM by \( \mathcal{O} \), and
- the action of \( \mathcal{O} \) is compatible with the reduction mod \( p \).
Base-extending to the complex numbers, \( \tilde{E} \cong \mathbb{C}/\Lambda \) for some lattice \( \Lambda \). We define \( \tilde{E}_I \) to be \( \mathbb{C}/I^{-1}\Lambda \). By the theory of complex multiplication, \( \tilde{E}_I \) has a model over \( H \). Then we define \([I] \ast E\) to be \( \tilde{E}_I \mod p \).

**Theorem 2.1.** The two actions are the same.

If you believe the constructions, this isn’t too hard to see. The inclusion \( \Lambda \subset I^{-1}\Lambda \) induces an isogeny \( \tilde{E}_I \rightarrow \tilde{E}_I \). One checks that the kernel is \( \tilde{E}_I \). The Deuring lift respects the action of \( I \), so that the reduction of \( \tilde{E}_I \mod p \) is precisely \( E[I] \).

### 2.2 Key exchange protocol

With the above setup, we need one additional property before describing our multiparty protocol.

**Proposition 2.2.** If \([I], [J] \in \text{Cl} \Omega\), then

\[
([I] \ast E) \times ([J] \ast E) \cong ([IJ] \ast E) \times E.
\]

**Proof.** We may assume that \( I \) and \( J \) are integral representatives whose norms are relatively prime; say \( N(I) = m \), \( N(J) = n \). Let \( a, b \in \mathbb{Z} \) satisfy \( am + bn = 1 \). Consider the natural isogenies

\[
\begin{align*}
\varphi_I : E &\rightarrow E_I \\
\varphi_J : E &\rightarrow E_J \\
\psi_J : E_I &\rightarrow E_{IJ} \\
\psi_I : E_J &\rightarrow E_{IJ}.
\end{align*}
\]

Then

\[
\begin{bmatrix} \psi_J & \psi_I \\ -a\hat{\varphi}_I & b\hat{\varphi}_J \end{bmatrix} : E_I \times E_J \rightarrow E_{IJ} \times E
\]

is an isomorphism with inverse

\[
\begin{bmatrix} b\hat{\psi}_J & -\varphi_I \\ a\hat{\psi}_I & \varphi_J \end{bmatrix}.
\]

The theorem can be restated in a category theoretic context, for example in Waterhouse, or more recent results of Centeleghe-Stix.

In any case, the protocol is as follows. Suppose we have \( n \) users who wish to agree on a shared secret key. We fix an ordinary elliptic curve \( E/\mathbb{F}_q \) as above. The \( k \)th user chooses an ideal class \( c_k \) and publishes \( E_k := c_k \ast E \). The shared key is then the isomorphism class of the \( n - 1 \) dimensional abelian variety

\[
A := ([\prod c_k] \ast E) \times E^{n-2}.
\]
Party 1, for instance, computes $A$ as $(c_1 \times E_2) \times E_3 \times \cdots \times E_n$. From the proposition, it immediately follows that all users have computed the same abelian variety (up to isomorphism). One also sees that the space of possible $A$ has size the order of $\text{Cl}(\mathcal{O})$. We can choose $p, E$ so that the class number is large, guaranteeing security against brute force attacks.

It should be apparent that this construction is a direct descendant of the 2-party isogeny schemes of Jao-de Feo-Plut and Castryk-Lange-Martindale-Panny-Renes.

### 2.3 Obstruction

Unfortunately, an abelian variety is not suitable as the output of the protocol. We need a number; namely, an isomorphism invariant of the abelian variety. Specifically, let $S$ be the set of isomorphism classe of finite products $\prod E_i$ where the $E_i$ are in $S_1$. We need an invariant map

$$\text{inv} : S \rightarrow X$$

which takes as input a product of elliptic curves in the isogeny class of $E$ and outputs a number (in some unspecified domain $X$), such that for $A, A' \in S$ of the same dimension,

- if $A \cong A'$, then $\text{inv}(A) = \text{inv}(A')$;
- if $A \not\cong A'$, then $\text{inv}(A) \neq \text{inv}(A')$; and
- $\text{inv}$ is efficiently computable.

The second condition can be relaxed to “$\text{inv}(A) \neq \text{inv}(A')$ with high probability”.

A way of restating the requirement is given pairwise isogenous elliptic curves $E_1, \ldots, E_n$ and $E'_1, \ldots, E'_n$ such that

$$E_1 \times \cdots \times E_n \cong E'_1 \times \cdots \times E'_n,$$ 

come up with an invariant which can be computed independent of which model is used.

There are several obvious candidates for such a map, but they all fail. The problems are one of the following: either the map depends on choice of a polarization, or being able to efficiently compute the map would lead to a solution of the isogeny problem and hence break the security of the protocol.

### 3 Potential invariants

**Naïve invariant.** For simplicity, we consider the case $n = 3$, so that we are looking for an invariant for abelian surfaces which are products of isogenous ordinary elliptic curves $A = E_1 \times E_2$. Let $\mathcal{S}_2 \subset S$ be the isomorphism classes of these surfaces. The most straightforward idea is to use $j(E_1)j(E_2)$. But in the
protocol, different users have different models of $A$, in particular as products of different elliptic curves $E_3 \times E_4$. For example, let $K = \mathbb{Q}(\sqrt{-59})$. The prime $p = 71$ splits in the Hilbert class field of $K$, and the Hilbert class polynomial mod 71 has roots 51, 54, and 67. Let $E_1, E_2$ be elliptic curves over $\mathbb{F}_{71}$ with these respective $j$-invariants. As the class group is cyclic of order 3, we have

$$E \times E \cong E_1 \times E_2.$$ However, $51^2 \equiv 45 \pmod{71}$ while $54 \cdot 67 \equiv 68 \pmod{71}$. Since the map depends on our particular pair of elliptic curves, it is not an isomorphism invariant.

The deeper reason this doesn’t work is that the choice of model amounts to a choice of polarization. The product of $j$-invariants is in a sense an invariant of the polarized abelian variety.

**Polarizations.** Let me give some background on polarizations. Given an arbitrary abelian variety $A$, there is an dual abelian variety $\hat{A}$ that classifies “degree 0” divisor classes on $A$. Any divisor $D$ on $A$ gives rise to an algebraic homomorphism

$$\lambda_D : A \to \hat{A}$$

via

$$\lambda_D(x) = [\tau_x(D)] - [D].$$

Here, $\tau_x$ means translation by $x$. A polarization $\lambda$ is any isogeny $A \to \hat{A}$ which arises in this way. The set of $\lambda_D$ inherits a group structure from the set of divisors. When $A \cong E \times E'$ a product of elliptic curves, this group looks like $\mathbb{Z}^2 \oplus \text{Hom}(E, E')$. This is where the problem with many invariants comes from! Two different polarizations on $A$ are overwhelmingly likely to differ by an isogeny between $E$ and $E'$. Thus knowledge of two polarizations can allow us to solve the isogeny problem for the pair $(E, E')$. This is fairly explicit: on $E \times E'$, we of course have the product polarization; that is, the isogeny resulting from the divisor $E \times \{0\} + \{0\} \times E'$. Given a random other polarization, it is likely that it comes from a divisor with some nonvertical, nonhorizontal component, call it $\Gamma$. Translating if necessary, we may assume that $\Gamma$ passes through the origin. Then we can use $\Gamma$ to construct an isogeny $E \to E'$; specifically, let $x \in E$. We take $\{x\} \times E'$, intersect with $\Gamma$, project down to $E'$, then take the sum in $E'$.

This issue comes up less directly with related invariants, as we will see.

**Theta nulls.** One idea for an invariant is to compute the theta nulls of $A$. These are an invention of Mumford which he used to explicitly compute a moduli space for abelian varieties. A theta null for $A$ is the image of the identity under a specific projective embedding $\varphi : A \to \mathbb{P}^N$. Without getting into too much detail, the choice of $\varphi$ is given by some additional structure on $A$, including the choice of a polarization. If $A \cong E_1 \times E_2$ and we use the product polarization, then the theta nulls are obtained by taking the corresponding theta nulls of $E_1$ and $E_2$, and then combining them via the Segre embedding

$$([x_0 : \cdots : x_n], [y_0 : \cdots : y_n]) \mapsto [x_0 y_0 : x_0 y_1 : \cdots : x_n y_n]$$
But the amazing thing is that the theta nulls are, under very mild conditions, a complete isomorphism invariant. In fact, given a theta null, we can recover associated projective model of the abelian variety $A$. In our particular case, one can recover $E_1$ and $E_2$ from the theta nulls. But conversely, we should not get the theta nulls associated with the model (say) $E_3 \times E_4$.

**Igusa invariants.** In most cases [Hayashida-Nishi 1965; Kani 2014], $A$ can be viewed as the Jacobian of a genus 2 curve $C$; in fact, such a curve $C$ can be found embedded inside of $A$. Given a hyperelliptic equation for $C$, we can write down invariants for $C$ as polynomials in its coefficients—the so-called Igusa invariants. These are the genus 2 analogues of the $j$-invariant.

The Torelli Theorem says that if two curves $C_1, C_2$ with respective Jacobians $J_1, J_2$ have $J_1 \cong J_2$, then $C_1 \cong C_2$. This fact seems to imply that the Igusa invariants could solve our problem. Unfortunately, it doesn’t work: Torelli’s theorem requires the isomorphism $J_1 \cong J_2$ to be as polarized abelian varieties. It can occur that $C_1 \not\cong C_2$ but that $J_1 \cong J_2$ as unpolarized abelian varieties. [Hayashida-Nishi 1967, Howe 1996, Kani 2014] In particular, there are in general many genus 2 curves lying on $A$.

**Kummer surfaces.** Given an abelian surface $A$, we can easily compute the Kummer surface $K := A/\langle -1 \rangle$. There is a nice theory of invariants of Kummer surfaces. Unfortunately, this entire theory depends on having a projective embedding of $K$, which arises from a polarization on $A$.

**Deligne invariant.** The reason so many natural invariants depend on a polarization is that the moduli space of unpolarized abelian varieties is, in Mumford’s words, pathological. Thus a priori it is hard to imagine a suitable computable invariant.

However, we are not looking for an invariant for all abelian varieties; rather, we need only consider abelian varieties which are the product of elliptic curves with CM by some fixed $\Theta$. Deligne in 1969 constructed such an invariant, given as follows. Fix our base field $\mathbb{F}_q$, and let $A$ be as before. There is a canonical lift, the Serre-Tate lift of $A$ to an abelian scheme $\hat{A}$ over the Witt ring $W(q)$, and a corresponding lift of the Frobenius endomorphism to an endomorphism $F$ of $\hat{A}$. If you don’t know what the Witt ring is, an instantiation is just given by an appropriate $p$-adic ring; namely, the valuation ring in $K/\mathbb{Q}_p$ for which $K/\mathbb{Q}_p$ is unramified, and for which the residue field is $\mathbb{F}_q$. Next, fix an embedding of $W(q)$ into $\mathbb{C}$ and let $\tilde{A}$ be the base-extension. We also write $F$ for the corresponding endomorphism of $\tilde{A}$. Let $T(A)$ denote the period lattice of $\tilde{A}$, viewed as a $\mathbb{Z}[F]$-module.

**Theorem 3.1** (Deligne 1969). $T(A)$ is an isomorphism invariant for $A$.

The problem is that $T(A)$ is not, using current techniques, efficiently computable. For example, if $A$ is an elliptic curve $E$, then the simplest way of computing $T(E)$ is by choosing a Deuring lift and using its period lattice. But
computing with the Deuring lift involves arithmetic over the Hilbert class field of $K = \text{End}(E) \otimes \mathbb{Q}$. More generally, instead of computing the entire embedding $W(q) \hookrightarrow \mathbb{C}$, it suffices to restrict to a copy of the Hilbert class field $H$ of $K$ lying inside $W(q)$. But this number field will have large absolute degree.

An added wrinkle is the following:

**Theorem 3.2.** Given an oracle to compute $T(A)$, we can solve the isogeny problem over $S_1$ in polynomial time.

To solve the isogeny problem over $S_1$ means that given $E, E' \in S_1$, find an ideal class $[I]$ such that $E' = I \ast E$.

The proof of the theorem is as follows. Let $A$ be an elliptic curve $E$. Then the action of $F$ gives $T(E)$ the structure of a rank 1 projective $O$-module, and so if $E$ is an elliptic curve, then $T(E)$ can be specified by an element of $\text{Cl} O$. Furthermore, recall that if $\bar{E} \cong \mathbb{C}/\Lambda$, then $\bar{E}_I \cong \mathbb{C}/I^{-1}\Lambda$. It follows that

$$T(E) \cong I \otimes O T(E_I).$$

In particular, $T(I \ast E)^{-1} \otimes T(E) \cong I$.

**Hope.** Is there any reason to hope that a suitable invariant exists? I personally think there is some hope, though perhaps slim. The reason is that there are invariants which neither depend on a polarization nor leak information in any obvious way. One such invariant, if $A \cong E_1 \times E_2$, is

$$\sum j(c \ast E_1) j(c^{-1} \ast E_2)$$

where the sum is over ideal classes $c \in \text{Cl} O$. Another option is to construct a symmetric polynomial in the Igusa invariants of (isomorphism classes of) genus 2 curves lying on $A$. The problem is that it is unclear how to compute either invariant efficiently.

### 3.1 Ancillary issues

**Supersingular curves.** Supersingular elliptic curves are typically preferred, since the associated isogeny problem is more difficult to solve for such curves. Such curves can even fit in the class group framework, as in the CSIDH scheme: simply restrict to supersingular curves over $\mathbb{F}_p$, so that the ring of $\mathbb{F}_p$-endomorphisms is an order in an iqf. Then the CM theory goes through.

However, the problem of invariants is likely much harder. This is due to a result of Deligne; namely, that if $n \geq 2$, then any two products of supersingular elliptic curves are isomorphic over $\overline{\mathbb{F}}_p$. Thus there can be no geometric invariant. There is the possibility of an arithmetic invariant, and in fact recent results of Xue-Yang-Yu (2016 and 2018) show that there is quite a lot of entropy available. However, one suspects that an arithmetic invariant is very difficult to compute.
**Decisional Diffie-Hellman.** The Decisional Diffie-Hellman problem for 2-parties is, given \(c^*E\) and \(d^*E\), to determine if \(E'\) is \(cd^*E\). If we have an invariant map, this is easy to solve; namely, check whether \((c^*E) \times (d^*E) \cong E' \times E\). Analogously we have an \(n\)-party Decisional Diffie-Hellman, and an invariant map for \(n\)-dimensional abelian varieties (or equivalently a working protocol for \(n+1\) parties) would lead to a solution to the \(n\)-party DDH. This is a general feature of multiparty Diffie-Hellman and more generally to cryptographic multilinear maps.

Our security assumption is instead the *Computational Diffie-Hellman problem*; that is, given \(c_1^*E, \ldots, c_n^*E\), it should be difficult to compute

\[
(\prod c_i)^*E \times E^{n-2}.
\]