Research Article

Dan Boneh*, Darren Glass, Daniel Krashen, Kristin Lauter, Shahed Sharif, Alice Silverberg, Mehdi Tibouchi, and Mark Zhandry

Multiparty Non-Interactive Key Exchange and More From Isogenies on Elliptic Curves

https://doi.org/10.1515/jmc-2015-0047
Received Feb 04, 2020; accepted Feb 05, 2020

Abstract: We describe a framework for constructing an efficient non-interactive key exchange (NIKE) protocol for n parties for any $n \geq 2$. Our approach is based on the problem of computing isogenies between isogenous elliptic curves, which is believed to be difficult. We do not obtain a working protocol because of a missing step that is currently an open mathematical problem. What we need to complete our protocol is an efficient algorithm that takes as input an abelian variety presented as a product of isogenous elliptic curves, and outputs an isomorphism invariant of the abelian variety.
Our framework builds a *cryptographic invariant map*, which is a new primitive closely related to a cryptographic multilinear map, but whose range does not necessarily have a group structure. Nevertheless, we show that a cryptographic invariant map can be used to build several cryptographic primitives, including NIKE, that were previously constructed from multilinear maps and indistinguishability obfuscation.

Keywords: Multilinear maps, Non-Interactive Key Exchange, Isogenies

2010 Mathematics Subject Classification: 14K02, 14Q20, 11Y16, 94A60

1 Introduction

Let $\mathbb{F}_q$ be a finite field, let E be an ordinary elliptic curve over $\mathbb{F}_q$, and let X be the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ that are $\mathbb{F}_q$-isogenous to E. The set X is almost always large (containing on the order of $\sqrt{q}$ elements). Moreover, under suitable conditions on E, the set X is endowed with a free and transitive action $\star$ by a certain abelian group G, which is the ideal class group of the endomorphism ring of E. The action $\star$ maps a given $g \in G$ and $E \in X$ to a curve $g \star E \in X$.

This action, originally defined by Deuring [16], has a number of properties that makes it useful in cryptography. First, for a fixed curve $E \in X$, the map $G \to X$ defined by $g \mapsto g \star E$ is believed to be a one-way function. In other words, given a random curve $E' \in X$ it is difficult to find an element $g \in G$ such that $E' = g \star E$. This suggests a Diffie–Hellman two-party key exchange protocol, proposed by Couveignes [14] and Rostovtsev and Stolbunov [38]: Alice chooses a random $a \in G$ and publishes $E_a := a \star E$; Bob chooses a random $b \in G$ and publishes $E_b := b \star E$. Their shared key is the curve $E_{ab} := (ab) \star E = a \star E_b = b \star E_a$, which they can both compute. To ensure that both parties obtain the same key, their shared key is the j-invariant of the curve E_{ab}. More recently, De Feo, Jao, and Plût [20], Galbraith [24], Castryck et al. [11], and De Feo, Kieffer, and Smith [21]

***Corresponding Author: Dan Boneh:** Stanford University, United States of America; Email: dabo@cs.stanford.edu
Darren Glass: Gettysburg College, United States of America; Email: dglass@gettysburg.edu
Daniel Krashen: Rutgers University, United States of America; Email: daniel.krashen@gmail.com
Kristin Lauter: Microsoft Research, United States of America; Email: klauter@microsoft.com
Shahed Sharif: California State University San Marcos, United States of America; Email: ssharif@csusm.edu
Alice Silverberg: University of California, Irvine, United States of America; Email: asilverb@uci.edu
Mehdi Tibouchi: NTT Corporation, Japan; Email: tibouchi.mehdi@lab.ntt.co.jp
Mark Zhandry: Princeton University, United States of America; Email: mzhandry@princeton.edu

proposed variants of this protocol with better security and efficiency. Moreover, a supersingular version of the isogeny problem was introduced and proposed as the basis for a collision resistant hash function [12]. Security of this one-way function was further studied in [19].

Second, as alluded to above, the star operator satisfies the following useful property: the abelian varieties $A_1 := (g_1 \star E) \times \cdots \times (g_n \star E)$ and $A_2 := (g_1 \cdots g_n) \star E \times E^{n-1}$ are isomorphic for all $g_1, \ldots, g_n \in G$ (see Appendix A.4 of [3]). As we will see in the next section, this suggests an n-party non-interactive key exchange protocol, as well as many other cryptographic constructions. This property leads to a more general cryptographic primitive that we call a **cryptographic invariant map**, defined in the next section. This primitive has properties that are similar to those of cryptographic multilinear maps [6, 25], which have found numerous applications in cryptography (e.g, [4, 7, 26, 27]). We discuss applications of cryptographic invariant maps in Section 3. In Remark 4.4 we explain why we use ordinary and not supersingular elliptic curves. Section 4 describes our approach to constructing cryptographic invariant maps from isogenies. This work leads to the following question in algebraic geometry.

An open problem. To make the cryptographic applications discussed above viable we must first overcome an important technical challenge. While the varieties A_1 and A_2 defined above are isomorphic, they are presented differently. Our applications require an efficient way to compute an invariant that is the same for A_1 and A_2. In addition, the invariant must distinguish non-isomorphic varieties. We do not know any such computable isomorphism invariant, and we present this as an open problem. In Section 5 we explain why some natural proposals for isomorphism invariants do not seem to work. In Remarks 2.4 and 4.2 we show that a solution to this open problem, even for $n = 2$, would solve the isogeny decision Diffie–Hellman problem. Further, we give evidence that computing a particular isomorphism invariant might be equivalent to solving the elliptic curve isogeny problem, which is believed (or hoped) to be a quantum-resistant hard problem. Thus, Section 5 might be useful from the point of view of cryptanalysis of isogeny-based cryptography.

2 Cryptographic invariant maps

Definition 2.1. Let X be a finite set and let G be a finite abelian group. We say that G **acts efficiently on** X **freely and transitively** if there is an efficiently computable map $\star : G \times X \to X$ such that:

- the map is a group action: $g\star(h\star x) = (gh)\star x$, and there is an identity element $\mathrm{id} \in G$ such that $\mathrm{id} \star x = x$, for all $x \in X$ and all $g, h \in G$;
- the action is transitive: for every $(x, y) \in X \times X$ there is a $g \in G$ such that $g \star x = y$; and
- the action is free: if $x \in X$ and $g, h \in G$ satisfy $g \star x = h \star x$, then $g = h$.

Definition 2.2. By a **cryptographic invariant map** we mean a randomized algorithm `MapGen` that inputs a security parameter λ, outputs public parameters $\mathtt{pp} = (X, S, G, e)$, and runs in time polynomial in λ, where:

- X and S are sets, and X is finite,
- G is a finite abelian group that acts efficiently on X freely and transitively,
- e is a deterministic algorithm that runs in time polynomial in λ and n, such that for each $n > 0$, algorithm e takes λ as input and computes a map $e_n : X^n \to S$ that satisfies:
  - **Invariance property** of e_n: for all $x \in X$ and $g_1, \ldots, g_n \in G$,

$$e_n(g_1 \star x, \ldots, g_n \star x) = e_n\big((g_1 \cdots g_n) \star x, x, \ldots, x\big);$$

  - **Non-degeneracy** of e_n: for all i with $1 \le i \le n$ and

$$x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in X,$$

    the map $X \to S$ defined by $y \mapsto e_n(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n)$ is injective.

In our candidate instantiation for cryptographic invariant maps the set X is a set of isogenous elliptic curves and the group G acting on X is a class group. The elements of S are isomorphism invariants of products of elliptic curves.

Definition 2.2 is quite ambitious in that it asks that e_n be defined for all $n > 0$ and run in polynomial time in n (and λ). A cryptographic invariant map that is defined even for a single $n > 2$, and satisfies the security assumptions in the next subsection, would still be quite interesting. We require a construction that works for all n because our framework using elliptic curve isogenies seems to support it. Similarly, we note that a construction that works for all $n > 0$, but runs in time exponential in n is still useful. It would limit our ability to evaluate e_n to relatively small n, but that is still of great interest. In the first three proposals in Section 5 we study candidates for e_n that run in time exponential in n, satisfy the non-degeneracy property, but do not satisfy the invariance property. It is an open problem to find a map that also satisfies the invariance property.

Security assumptions. Next, we define some security assumptions on cryptographic invariant maps. The notation $x \xleftarrow{R} X$ will denote an independent uniform random variable x over the set X. Similarly, we use $x' \xleftarrow{R} A(y)$ to define a random variable x' that is the output of a randomized algorithm A on input y.

The n-way computational Diffie–Hellman assumption states that, given only the public parameters and $(g_1 \star x, \ldots, g_n \star x) \in X^n$, it is difficult to compute $e_{n-1}\big((g_1 \cdots g_n) \star x, x, \ldots, x\big)$. A precise definition is the following:

Definition 2.3. We say that MapGen satisfies the n-way **computational Diffie–Hellman assumption (n-CDH)** if for every polynomial time algorithm $\mathcal{A}$,

$$\Pr\left[\mathcal{A}(\mathsf{pp},\ g_1 \star x, \ldots, g_n \star x) = e_{n-1}\big((g_1 \cdots g_n) \star x, x, \ldots, x\big)\right]$$

is a negligible function of λ, when $\mathsf{pp} \xleftarrow{R} \mathsf{MapGen}(\lambda)$, $g_1, \ldots, g_n \xleftarrow{R} G$, and $x \xleftarrow{R} X$.

Remark 2.4. The natural n-way decision Diffie–Hellman assumption on X does not hold when invariant maps exist. That is, for all $n > 0$ it is easy to distinguish $(g_1 \cdots g_n) \star x \in X$ from a random element of X, given only $x, g_1 \star x, \ldots, g_n \star x$. Given a challenge $y \in X$, simply check if

$$e_n(y, x, \ldots, x) = e_n(g_1 \star x, \ldots, g_n \star x).$$

Equality holds if and only if $y = (g_1 \cdots g_n) \star x$. However, in Definition 2.5 we define an n-way decision Diffie–Hellman assumption for e_{n-1}. It states that it is hard to distinguish $e_{n-1}\big((g_1 \cdots g_n)\star x, x, \ldots, x\big)$ from a random element in the image of e_{n-1}, given only the public parameters, x, and $(g_1 \star x, \ldots, g_n \star x) \in X^n$.

Definition 2.5. We say that MapGen satisfies the n-way **decision Diffie–Hellman assumption (n-DDH)** if the following two distributions, $\mathcal{P}_0$ and $\mathcal{P}_1$, are polynomially indistinguishable, when $\mathsf{pp} \xleftarrow{R} \mathsf{MapGen}(\lambda)$, $g_1, \ldots, g_n \xleftarrow{R} G$, and $x \xleftarrow{R} X$:

- $\mathcal{P}_0$ is $(\mathsf{pp},\ g_1 \star x, \ldots, g_n \star x,\ s_0)$ where $s_0 = e_{n-1}\big((g_1 \cdots g_n) \star x, x, \ldots, x\big)$,
- $\mathcal{P}_1$ is $(\mathsf{pp},\ g_1 \star x, \ldots, g_n \star x,\ s_1)$ where s_1 is random in $\mathrm{Im}(e_{n-1}) \subseteq S$.

3 Applications

We show that suitable cryptographic invariant maps can be used to solve a number of important problems in cryptography.

***n*-way Non-Interactive Key Exchange (NIKE).** We show how to use a cryptographic invariant map to construct a Non-Interactive Key Exchange (NIKE) protocol in which n parties create a shared secret key that only they can efficiently calculate, without any interaction among the n parties. Currently, secure n-party NIKE for $n > 3$ is only known from general purpose indistinguishability obfuscation (e.g., [8]). Our NIKE construction is similar to the one in [6, 25, 32] and satisfies a "static" notion of security.

- Setup(λ): run $(X, S, G, e) \xleftarrow{R} \mathsf{MapGen}(\lambda)$ and choose $x \xleftarrow{R} X$. Output $\mathsf{pp} := (X, S, G, e, x)$.
- For $i = 1, \ldots, n$, party i chooses a random $g_i \xleftarrow{R} G$, computes $x_i := g_i * x \in X$, and publishes x_i on a public bulletin board.
- The shared key between the n-parties is

$$k := e_{n-1}\big((g_1 \cdots g_n) * x, x, \ldots, x\big) \in S.$$

  Party $i \in \{1, \ldots, n\}$ computes k by obtaining $x_1, \ldots, x_n$ from the bulletin board, then choosing some $j \in \{1, \ldots, n\}$ where $j \neq i$, and computing

$$k = e_{n-1}(x_1, \ldots, x_{j-1},\ g_i * x_j,\ x_{j+1}, \ldots, x_n) \in S,$$

  where x_i is omitted from the input to e_{n-1}.

All n parties obtain the same key k by the invariance property of e_{n-1}. Static security follows from the n-way decision Diffie–Hellman assumption, as in [6]. Alternatively, we can rely on the weaker n-way computational Diffie–Hellman assumption by applying a hash function $H : S \to K$ to the key k. We model H as a random oracle in the security analysis. We leave the question of an adaptively-secure NIKE, in the sense of [22, 37], from an invariant map for future work.

Unique signatures and verifiable random functions (VRF). A digital signature scheme is made up of three algorithms: a key generation algorithm that outputs a public key and a secret key, a signing algorithm that signs a given message using the secret key, and a verification algorithm that verifies a signature on a given message using the public key. A signature scheme is a **unique signature scheme** if for every public key and every message, there is at most one signature that will be accepted as a valid signature for that message under the public key. While a number of unique signature schemes are known in the random oracle model (e.g., [2, 5]), it is quite hard to construct unique signatures without random oracles [17, 35]. Unique signatures are closely related to a simpler object called a verifiable random function, or VRF [36]. Previous results show how to construct unique signatures and VRFs from multilinear maps without random oracles [6]. The same constructions work with a cryptographic invariant map. The unique signature scheme works as follows: The secret key is a random $(g_{1,0}, g_{1,1}, \ldots, g_{n,0}, g_{n,1}) \xleftarrow{R} G^{2n}$. The public key is $(x, y_{1,0}, \ldots, y_{n,1}) \in X^{2n+1}$ where $x \xleftarrow{R} X$ and $y_{i,b} := g_{i,b} * x$ for $i = 1, \ldots, n$ and $b = 0, 1$. The signature on an n-bit message $m \in \{0,1\}^n$ is $\sigma := (\prod_{i=1}^{n} g_{i,m_i}) * x \in X$. To verify a signature σ, check that $e_n(\sigma, x, \ldots, x) = e_n\big(y_{1,m_1}, \ldots, y_{n,m_n}\big)$. The security analysis of this construction is the same as in [6].

Constrained PRFs and broadcast encryption. We next describe how to construct *constrained pseudorandom functions* [7, 9, 33] for *bit-fixing constraints* from a cryptographic invariant map. Such constrained PRFs in turn can be used to build broadcast encryption with short ciphertexts [7].

A pseudorandom function (PRF) is a function $F : \mathcal{K} \times \mathcal{A} \to \mathcal{B}$ that is computable in polynomial time. Here, $\mathcal{K}$ is the key space, $\mathcal{A}$ is the domain, and $\mathcal{B}$ is the codomain. Intuitively, PRF security requires that, for a random key $k \in \mathcal{K}$, an adversary who obtains pairs $\big(a,\ F(k, a)\big)$, for $a \in \mathcal{A}$ of its choice, cannot distinguish these pairs from pairs $\big(a, f(a)\big)$ where f is a random function $\mathcal{A} \to \mathcal{B}$.

A *bit-fixing constrained PRF* is a PRF where a key $k \in \mathcal{K}$ can be constrained to only evaluate the PRF on a subset of the domain $\mathcal{A}$, where $\mathcal{A} = \{0,1\}^n$. Specifically, for $V \subseteq [n] = \{1, \ldots, n\}$ and a function $v : V \to \{0,1\}$, let $\mathcal{A}_v = \{a \in \mathcal{A} : \forall i \in V, a_i = v(i)\}$. A constrained key k_v enables one to evaluate $F(k, a)$ for all $a \in \mathcal{A}_v$, but reveals nothing about $F(k, a)$ for $a \notin \mathcal{A}_v$. We refer to [7] for the complete definition of this concept, and its many applications.

We now explain how to construct bit-fixing constrained PRFs from cryptographic invariant maps. The construction and security proof are essentially the same as in Boneh and Waters [7], but translated to our setting. One complication is that the construction of Boneh and Waters requires a way to operate on invariants in S. We get around this by delaying the evaluation of the invariant to the very last step. We thus obtain the following bit-fixing constrained PRF:

- $\mathsf{Setup}(\lambda)$: run $(X, S, G, e) \xleftarrow{R} \mathsf{MapGen}(\lambda)$ and choose $x \xleftarrow{R} X$.
  Next choose $\alpha \xleftarrow{R} G$ and $d_{i,b} \xleftarrow{R} G$ for $i \in [n]$ and $b \in \{0, 1\}$.
  Output the key $k = (X, S, G, e, \alpha, \{d_{i,b}\}_{i,b})$.
- The PRF is defined as: $F(k, a) = e_n\big((\alpha \times \prod_{i=1}^{n} d_{i,a_i}) \star x,\ x,\ \ldots,\ x\big)$.
  Here, $a \in \{0, 1\}^n$ specifies a subset product of the set of $d_{i,b}$'s.
- $\mathsf{Constrain}(k, v)$: Let $V \subseteq [n]$ be the support of the function v, and assume V is not empty. The constrained key k_v is constructed as follows. Set $D_{i,b} = d_{i,b} \star x$ for $i \notin V$. Let i_0 be the smallest element of V. Choose $|V| - 1$ random $g_i \in G$ for $i \in V \setminus \{i_0\}$, and set $g_{i_0} = \alpha \times \prod_{i \in V} d_{i,v_i} \times (\prod_{i \in V \setminus \{i_0\}} g_i)^{-1} \in G$. Let $h_i = g_i \star x$ for $i \in V$.
  The constrained key is $k_v = \big(\{D_{i,b}\}_{i \notin V, b \in \{0,1\}},\ \{h_i\}_{i \in V}\big)$.
- $\mathsf{Eval}(k_v, a)$: To evaluate $F(k, a)$ using the constrained key k_v do the following. If $a \notin \mathcal{A}_v$, output $\diamond$. Otherwise, for $i = 1, \ldots, n$, let $C_i = D_{i,a_i}$ if $i \notin V$, and let $C_i = h_i$ otherwise. Output $e_n(C_1, \ldots, C_n)$. Then, by construction,

$$e_n(C_1, \ldots, C_n) = e_n\left(\left(\prod_{i \notin V} d_{i,a_i} \prod_{i \in V} g_i\right) \star x, x, \ldots, x\right) = F(k, a).$$

The security proof is as in [7]. This construction can be further extended to a verifiable random function (VRF) by adapting Fuchsbauer [23] similarly.

Witness encryption. Witness encryption, due to Garg et al. [27], can be used to construct Identity-Based Encryption, Attribute-Based Encryption, broadcast encryption [42], and secret sharing for NP statements. Witness encryption is a form of encryption where a public key is simply an NP statement, and a secret key is a witness for that statement. More precisely, a witness encryption scheme is a pair of algorithms:

- $\mathsf{Enc}(x, m)$ is a randomized polynomial-time algorithm that takes as input an NP statement x and a message m, and outputs a ciphertext c;
- $\mathsf{Dec}(x, w, c)$ is a deterministic polynomial-time algorithm that takes as input a statement x, supposed witness w, and ciphertext c, and attempts to produce the message m.

We require that if w is a valid witness for x, then for any message m, if $c \xleftarrow{R} \mathsf{Enc}(x, m)$, then $\mathsf{Dec}(x, w, c)$ outputs m with probability 1.

The basic notion of security for witness encryption is *soundness security*, which requires that if x is false, then $\mathsf{Enc}(x, m)$ hides all information about m. A stronger notion called *extractable security*, due to Goldwasser et al. [28], requires, informally, that if one can learn any information about m from $\mathsf{Enc}(x, m)$, then it must be the case that one "knows" a witness for x.

We briefly describe how to construct witness encryption from invariant maps. It suffices to give a construction from any NP-complete problem. There are at least two natural constructions from multilinear maps that we can use. One approach is to adapt the original witness encryption scheme of Garg et al. [27] based on the Exact Cover problem. This approach unfortunately also requires the same graded structure as needed by Boneh and Waters [7]. However, we can apply the same ideas as in our constrained PRF construction to get their scheme to work with invariant maps. Another is the scheme of Zhandry [42] based on Subset Sum.[1]

As with the constructions of Garg et al. and Zhandry, the security of these constructions can be justified in an idealized attack model for the cryptographic invariant map, allowing only the operations explicitly allowed by the map—namely the group action and the map operation. Justification in idealized models is not a proof, but provides heuristic evidence for security.

1 The basic scheme shown by Zhandry requires an "asymmetric" multilinear map, where the inputs to the map come from different sets. However, Zhandry also explains how to instantiate the scheme using symmetric multilinear maps. The symmetric scheme easily translates to use invariant maps.

4 Cryptographic invariant maps from isogenies

We begin by recalling some facts that are presented in more detail in Appendix A of [3]. Let E be an ordinary elliptic curve over a finite field $\mathbb{F}_q$ such that the ring $\mathbb{Z}[\pi]$ generated by its Frobenius endomorphism π is integrally closed. This implies in particular that $\mathbb{Z}[\pi]$ is the full endomorphism ring $\mathcal{O}$ of E. Let $\mathrm{Cl}(\mathcal{O})$ denote the ideal class group of this ring, and let $\mathrm{Ell}(\mathcal{O})$ denote the isogeny class of E; that is, isomorphism classes of elliptic curves over $\mathbb{F}_q$ which are $\mathbb{F}_q$-isogenous to E. There exists a free and transitive action $\star$ of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$, and there is a way to represent elements of $\mathrm{Cl}(\mathcal{O})$ (namely, as products of prime ideals of small norm) that makes this action efficiently computable. Moreover, one can efficiently sample close to uniform elements in $\mathrm{Cl}(\mathcal{O})$ under that representation. In addition, the "star operator" $\star$ satisfies the following property: for any choice of ideal classes $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{a}'_1, \ldots, \mathfrak{a}'_n$ in $\mathrm{Cl}(\mathcal{O})$, the abelian varieties

$$(\mathfrak{a}_1 \star E) \times \cdots \times (\mathfrak{a}_n \star E) \quad \text{and} \quad (\mathfrak{a}'_1 \star E) \times \cdots \times (\mathfrak{a}'_n \star E) \tag{1}$$

are isomorphic over $\mathbb{F}_q$ if and only if $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}'_1 \cdots \mathfrak{a}'_n$ in $\mathrm{Cl}(\mathcal{O})$. In particular:

$$(\mathfrak{a}_1 \star E) \times \cdots \times (\mathfrak{a}_n \star E) \cong (\mathfrak{a}_1 \cdots \mathfrak{a}_n) \star E \times E^{n-1}. \tag{2}$$

Denote by $\mathrm{Ab}(E)$ the set of abelian varieties over $\mathbb{F}_q$ that are a product of the form (2), and assume that we can efficiently compute an isomorphism invariant for abelian varieties in $\mathrm{Ab}(E)$. In other words, assume that we have an efficiently computable map $\mathrm{isom}\colon \mathrm{Ab}(E) \to S$ to some set S that to any tuple $E_1, \ldots, E_n$ of elliptic curves isogenous to E associates an element $\mathrm{isom}(E_1 \times \cdots \times E_n)$ of S such that $\mathrm{isom}(E_1 \times \cdots \times E_n) = \mathrm{isom}(E'_1 \times \cdots \times E'_n)$ if and only if the products $E_1 \times \cdots \times E_n$ and $E'_1 \times \cdots \times E'_n$ are isomorphic as abelian varieties. The curves E_i are given for example by their j-invariants, and in particular, the ideal classes $\mathfrak{a}_i$ such that $E_i \cong \mathfrak{a}_i \star E$ are not supposed to be known.

Based on such an isomorphism invariant isom, we construct a cryptographic invariant map as follows. The algorithm $\mathsf{MapGen}(\lambda)$ computes a sufficiently large base field $\mathbb{F}_q$, and an elliptic curve E over $\mathbb{F}_q$ such that the ring $\mathbb{Z}[\pi]$ generated by its Frobenius endomorphism is integrally closed (this can be done efficiently: see again Appendix A of [3]). The algorithm then outputs the public parameters $\mathsf{pp} = (X, S, G, e)$ where:

- $X = \mathrm{Ell}(\mathcal{O})$ is the isogeny class of E over $\mathbb{F}_q$;
- S is the codomain of the isomorphism invariant isom;
- $G = \mathrm{Cl}(\mathcal{O})$ is the ideal class group of $\mathcal{O}$; and
- the map $e_n\colon X^n \to S$ is given by $e_n(E_1, \ldots, E_n) = \mathrm{isom}(E_1 \times \cdots \times E_n)$.

The facts recalled at the beginning of this section show that G acts efficiently on X freely and transitively in the sense of Definition 2.1, and that the properties of Definition 2.2 are satisfied. In particular, the invariance property follows from (2), and the non-degeneracy from the fact that the abelian varieties in (1) are isomorphic *only if* the corresponding products of ideal classes coincide. Thus, this approach does provide a cryptographic invariant map assuming isom exists.

Remark 4.1. In the 2-party case, the NIKE protocol obtained from this construction coincides with the isogeny key exchange protocols over ordinary curves described by Couveignes [14] and Rostovtsev–Stolbunov [38].

Remark 4.2. The existence of isom breaks the isogeny decision Diffie–Hellman problem. Indeed, given three elliptic curves $(\mathfrak{a} \star E, \mathfrak{b} \star E, \mathfrak{c} \star E)$ isogenous to E, one can check whether $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$ by testing whether the surfaces $(\mathfrak{c} \star E) \times E$ and $(\mathfrak{a} \star E) \times (\mathfrak{b} \star E)$ are isomorphic. This does not prevent the construction of secure NIKE protocols (as those can be based on the computational isogeny Diffie–Hellman problem by applying a hash function: see Section 3), but currently, no efficient algorithm is known for this isogeny decision Diffie–Hellman problem.

Remark 4.3. For certain applications, it would be interesting to be able to hash to the set $X = \mathrm{Ell}(\mathcal{O})$, i.e., construct a random-looking curve E' in the isogeny class of E without knowing an isogeny walk from E to E'. An equivalent problem is to construct a random-looking elliptic curve with exactly $\#E(\mathbb{F}_q)$ points over $\mathbb{F}_q$. This seems difficult, however; the normal way of doing so involves the CM method, which is not efficient when the discriminant is large.

Remark 4.4. One can ask whether this construction extends to the supersingular case. Over $\mathbb{F}_{p^2}$ with p prime, the answer is clearly no, as the isogeny class of a supersingular elliptic curve is not endowed with a natural free and transitive group action by an abelian group. More importantly, isomorphism classes of products of isogenous supersingular elliptic curves over $\mathbb{F}_q$ are essentially trivial at least in a geometric sense. Indeed, according to a result of Deligne (see [39, Theorem 3.5]), if $E_1, \ldots, E_n, E'_1, \ldots, E'_n$ are all isogenous to a supersingular elliptic curve E, then $E_1 \times \cdots \times E_n \cong E'_1 \times \cdots \times E'_n$ over $\overline{\mathbb{F}_q}$ as soon as $n \geq 2$. In fact, the result holds over any extension of the base field over which all the endomorphisms of E are defined, so already over $\mathbb{F}_{p^2}$. However, for a supersingular elliptic curve E over a prime field $\mathbb{F}_p$, the number of $\mathbb{F}_p$-isomorphism classes of products $E_1 \times \cdots \times E_n$ with all E_i isogenous to E can be large. For example, this is shown when $n = 2$ in [41, Section 5]. Therefore, one could conceivably obtain a "commutative supersingular" version of the construction above, which would generalize the recent 2-party key exchange protocol CSIDH [11], assuming that $\mathbb{F}_p$-isomorphism invariants can be computed in that setting. Since those invariants must be arithmetic rather than geometric in nature, however, this seems even more difficult to achieve than in the ordinary case.

5 Some natural candidate cryptographic invariant maps

In order to instantiate a cryptosystem based on the ideas in this paper, it remains to find an efficiently computable map $\mathrm{isom}\colon \mathrm{Ab}(E) \to S$ for some set S, as in the previous section. Below we give evidence that several natural candidates fail, either because efficiently computing them would break the cryptographic security, or because they are not in fact isomorphism invariants.

Our primary roadblock is that while $E_1 \times \cdots \times E_n$ and $E'_1 \times \cdots \times E'_n$ can be isomorphic as unpolarized abelian varieties, they are not necessarily isomorphic as polarized abelian varieties with their product polarizations. The first three proposals below for invariants are invariants of the isomorphism class as polarized abelian varieties, but are not invariants of the isomorphism class as unpolarized abelian varieties. We do not know a way for the different parties to choose polarizations on their product varieties in a compatible way, to produce the same invariant, without solving the elliptic curve isogeny problem.

At present, we do not know an invariant of abelian varieties in dimension ≥ 2 that does not require choosing a polarization, with the exception of what we call the "Deligne invariant", described below.

The theta null invariant. One natural candidate is given by Mumford's *theta nulls*, presented in detail in Appendix B of [3]. Unfortunately, in order to compute even a single theta null, one must first choose a principal polarization, and the resulting invariant does depend on this choice of polarization in a crucial way. In [3, Proposition B.7] we show that, as a result, the theta nulls do not in fact provide an isomorphism invariant as unpolarized abelian varieties.

Igusa invariants. Suppose $n = 2$ and $\mathrm{End}\, E \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{N}$ square-free. If $d \neq 1, 3, 7, 15$, then for E_1 and E_2 in the isogeny class of E, the product $E_1 \times E_2$ is the Jacobian of a genus 2 curve C (see [30]). It is possible to compute such a genus 2 curve C, given a suitable principal polarization on $E_1 \times E_2$. For each such C, one could then compute the Igusa invariants [31] of C. The number of genus 2 curves C such that $E_1 \times E_2$ is isomorphic to the Jacobian variety of C is large ([29] and [34, Theorem 5.1]), and unfortunately the Igusa invariants are different for different choices of C. There are many principal polarizations on each element of $\mathrm{Ab}(E)$, and no compatible way for the different parties to choose the same one.

Invariants of Kummer surfaces. When $n = 2$, another approach is to consider the Kummer surface of $A = E_1 \times E_2$, which is the quotient $K = A/\{\pm 1\}$. The surface K itself does not depend on a polarization. But extracting an invariant from K, for example as in [10, Chapter 3], *does* depend on having a projective embedding of K.

Deligne invariant. A natural candidate is an isomorphism invariant studied by Deligne [15]. Suppose A is an ordinary abelian variety over $k = \mathbb{F}_q$. The Serre-Tate canonical lift of A to characteristic 0 produces an

abelian variety over the ring of Witt vectors $W(\bar{k})$. Fixing an embedding α of $W(\bar{k})$ into $\mathbb{C}$, we can view this lift as a complex abelian variety $A^{(\alpha)}$. Let $T_\alpha(A)$ denote the first integral homology group of $A^{(\alpha)}$. The Frobenius endomorphism F of A also lifts to characteristic 0 and defines an action of F on $T_\alpha(A)$. The theorem in [15, §7] shows that ordinary abelian varieties A and B over $\mathbb{F}_q$ are isomorphic if and only if there is an isomorphism $T_\alpha(A) \to T_\alpha(B)$ that respects the action of F.

A natural candidate for a cryptographic invariant map is the map that sends $(E_1, \ldots, E_n)$ to the isomorphism invariant

$$T_\alpha(E_1 \times \cdots \times E_n) = T_\alpha(E_1) \oplus \cdots \oplus T_\alpha(E_n).$$

Specifying the isomorphism class of $T_\alpha(E_1 \times \cdots \times E_n)$ as a $\mathbb{Z}[F]$-module is equivalent to specifying the action of F as a $2n \times 2n$ integer matrix, unique up to conjugacy over $\mathbb{Z}$. However, we show in Theorem 5.1 below that being able to compute $T_\alpha(E)$ for an elliptic curve E in polynomial time would yield a polynomial-time algorithm to solve the elliptic curve isogeny problem of recovering $\mathfrak{a}$ given E and $\mathfrak{a} \star E$, and conversely.

Theorem 5.1. *An efficient algorithm to compute Deligne invariants $T_\alpha(E)$ on an isogeny class of ordinary elliptic curves over a finite field k gives an efficient algorithm to solve the elliptic curve isogeny problem in that isogeny class. Conversely, an efficient algorithm to solve the elliptic curve isogeny problem on an isogeny class of ordinary elliptic curves over k yields an efficient algorithm to compute, for some embedding $\alpha : W(\bar{k}) \hookrightarrow \mathbb{C}$, the Deligne invariants $T_\alpha(E)$ on the isogeny class.*

Proof. Suppose that E_1 and E_2 are in the isogeny class, and suppose that for $i = 1, 2$ we have a $\mathbb{Z}$-basis $\{u_i, v_i\}$ for $T_\alpha(E_i)$ and a 2×2 integer matrix giving the action of F with respect to this basis. We will efficiently compute a fractional ideal $\mathfrak{a}$ such that $\mathfrak{a} \star E_1 \cong E_2$.

Let $f(t)$ be the characteristic polynomial of Frobenius acting on E_1 or E_2; these are the same since E_1 and E_2 are isogenous. Let $R = \mathbb{Z}[t]/(f)$ and $R_\mathbb{Q} = R \otimes_\mathbb{Z} \mathbb{Q}$. Then $T_\alpha(E_i)$ is a rank one R-module, with t acting as F. Compute $a_i, b_i \in \mathbb{Z}$ such that $F(u_i) = a_i u_i + b_i v_i$. Let $\mathfrak{a}_i$ be the fractional R-ideal generated by 1 and $(t - a_i)/b_i$. Compute and output $\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2^{-1}$.

We claim that $\mathfrak{a} \star E_1 \cong E_2$. Define $\lambda_i : T_\alpha(E_i) \hookrightarrow R_\mathbb{Q}$ by sending $w \in T_\alpha(E_i)$ to the unique $\lambda_i(w) \in R_\mathbb{Q}$ such that $\lambda_i(w) \cdot u_i = w$. Then $\lambda_i(u_i) = 1$ and $\lambda_i(v_i) = (t - a_i)/b_i$, so the fractional ideal $\mathfrak{a}_i$ is the image of the map λ_i. Suppose M is a positive integer such that $M\mathfrak{a}$ is an integral ideal of R, and let $h = \lambda_2^{-1} \circ M\lambda_1$. Then $h(T_\alpha(E_1))$ is an R-submodule of $T_\alpha(E_2)$. By [15, §7], the map $E \mapsto T_\alpha(E)$ is a fully faithful functor, i.e., it induces a bijection

$$\mathrm{Hom}_k(E_1, E_2) \to \mathrm{Hom}_R(T_\alpha(E_1), T_\alpha(E_2)).$$

Thus h arises from a unique isogeny $\phi : E_1 \to E_2$. By [15, §4], the kernel of ϕ is isomorphic as an R-module to $T_\alpha(E_2)/h(T_\alpha(E_1))$. The latter R-module is isomorphic to $R/M\mathfrak{a}$, and hence is exactly annihilated by $M\mathfrak{a}$. Thus $\ker(\phi) \cong E_1[M\mathfrak{a}]$, so $E_2 \cong E_1/E_1[M\mathfrak{a}] \cong (M\mathfrak{a}) \star E_1$. Since $M\mathfrak{a}$ and $\mathfrak{a}$ are in the same ideal class, we have $E_2 \cong \mathfrak{a} \star E_1$, as desired. Fractional ideals can be inverted in polynomial time by [1, Algorithm 5.3] or [13, §4.8.4] (see [1, p. 21] for the complexity).

Conversely, suppose we have an algorithm that efficiently solves the isogeny problem in the isogeny class of an ordinary elliptic curve E_0. Take R as above. We show below that there exists an embedding $\alpha : W(\bar{k}) \hookrightarrow \mathbb{C}$ such that $T_\alpha(E_0) \cong R$. Given E isogenous to E_0, use the isogeny problem algorithm to compute $\mathfrak{a}$ such that $E_0 \cong \mathfrak{a} \star E$. Output $T_\alpha(E) = \mathfrak{a}$.

It remains to show that an embedding $\alpha : W(\bar{k}) \hookrightarrow \mathbb{C}$ exists such that $T_\alpha(E_0) \cong R$ and $T_\alpha(E) = \mathfrak{a}$. We follow an argument in the proof of [18, Theorem 2.1]. There exists an elliptic curve E' over $\mathbb{C}$ with CM by R for which $H_1(E', \mathbb{Z}) \cong R$ as R-modules. Take any embedding $\beta : W(\bar{k}) \hookrightarrow \mathbb{C}$. Then the complex elliptic curve $E_0^{(\beta)}$ has CM by R, and by the theory of complex multiplication there exists $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ such that $E' = \sigma(E_0^{(\beta)}) = E_0^{(\sigma\circ\beta)}$. Let $\alpha = \sigma \circ \beta$. By construction, $T_\alpha(E_0) = H_1(E', \mathbb{Z}) \cong R$. Further, by [40, Prop. II.1.2], $T_\alpha(E) \cong \mathfrak{a} \otimes_R T_\alpha(E_0) \cong \mathfrak{a}$, as claimed. □

Acknowledgement: We thank the American Institute of Mathematics (AIM) for supporting a workshop on multilinear maps where the initial seeds for this work were developed, and the Banff International Research

Station (BIRS) where our collaboration continued. We also thank Michiel Kosters and Yuri Zarhin. Boneh was partially supported by NSF, DARPA, and ONR. Silverberg was partially supported by a grant from the Alfred P. Sloan Foundation and NSF grant CNS-1703321.

References

[1] Karim Belabas, Topics in computational algebraic number theory, *J. Théor. Nombres Bordeaux* **16** (2004), 19–63.
[2] Mihir Bellare and Phillip Rogaway, The Exact Security of Digital Signatures: How to Sign with RSA and Rabin, in: *EUROCRYPT'96* (Ueli M. Maurer, ed.), LNCS 1070, pp. 399–416, Springer, Heidelberg, May 1996.
[3] Dan Boneh, Darren Glass, Daniel Krashen, Kristin Lauter, Shahed Sharif, Alice Silverberg, Mehdi Tibouchi and Mark Zhandry, *Multiparty Non-Interactive Key Exchange and More From Isogenies on Elliptic Curves*, Cryptology ePrint Archive, Report 2018/665, 2018, https://eprint.iacr.org/2018/665.
[4] Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry and Joe Zimmerman, Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation, in: *EUROCRYPT 2015, Part II* (Elisabeth Oswald and Marc Fischlin, eds.), LNCS 9057, pp. 563–594, Springer, Heidelberg, April 2015.
[5] Dan Boneh, Ben Lynn and Hovav Shacham, Short Signatures from the Weil Pairing, in: *ASIACRYPT 2001* (Colin Boyd, ed.), LNCS 2248, pp. 514–532, Springer, Heidelberg, December 2001.
[6] Dan Boneh and Alice Silverberg, Applications of multilinear forms to cryptography, *Contemporary Mathematics* **324** (2003), 71–90.
[7] Dan Boneh and Brent Waters, Constrained Pseudorandom Functions and Their Applications, in: *ASIACRYPT 2013, Part II* (Kazue Sako and Palash Sarkar, eds.), LNCS 8270, pp. 280–300, Springer, Heidelberg, December 2013.
[8] Dan Boneh and Mark Zhandry, Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation, *Algorithmica* **79** (2017), 1233–1285, Extended abstract in Crypto 2014.
[9] Elette Boyle, Shafi Goldwasser and Ioana Ivan, Functional Signatures and Pseudorandom Functions, in: *PKC 2014* (Hugo Krawczyk, ed.), LNCS 8383, pp. 501–519, Springer, Heidelberg, March 2014.
[10] John W. S. Cassels and E. Victor Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series 230, Cambridge University Press, Cambridge, 1996.
[11] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny and Joost Renes, *CSIDH: An Efficient Post-Quantum Commutative Group Action*, Cryptology ePrint Archive, Report 2018/383, 2018, https://eprint.iacr.org/2018/383.
[12] Denis Xavier Charles, Kristin E. Lauter and Eyal Z. Goren, Cryptographic Hash Functions from Expander Graphs, *Journal of Cryptology* **22** (2009), 93–113.
[13] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin, 1993.
[14] Jean-Marc Couveignes, *Hard Homogeneous Spaces*, Cryptology ePrint Archive, Report 2006/291, 2006, http://eprint.iacr.org/2006/291.
[15] Pierre Deligne, Variétés abéliennes ordinaires sur un corps fini, *Invent. Math.* **8** (1969), 238–243.
[16] Max Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.
[17] Yevgeniy Dodis and Aleksandr Yampolskiy, A Verifiable Random Function with Short Proofs and Keys, in: *PKC 2005* (Serge Vaudenay, ed.), LNCS 3386, pp. 416–431, Springer, Heidelberg, January 2005.
[18] W. Duke and Á. Tóth, The splitting of primes in division fields of elliptic curves, *Experiment. Math.* **11** (2002), 555–565 (2003).
[19] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison and Christophe Petit, Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions, in: *EUROCRYPT 2018, Part III* (Jesper Buus Nielsen and Vincent Rijmen, eds.), LNCS 10822, pp. 329–368, Springer, Heidelberg, April / May 2018.
[20] Luca De Feo, David Jao and Jérôme Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *J. Mathematical Cryptology* **8** (2014), 209–247.
[21] Luca De Feo, Jean Kieffer and Benjamin Smith, *Towards practical key exchange from ordinary isogeny graphs*, Cryptology ePrint Archive, Report 2018/485, 2018, https://eprint.iacr.org/2018/485.
[22] Eduarda S. V. Freire, Dennis Hofheinz, Eike Kiltz and Kenneth G. Paterson, Non-Interactive Key Exchange, in: *PKC 2013* (Kaoru Kurosawa and Goichiro Hanaoka, eds.), LNCS 7778, pp. 254–271, Springer, Heidelberg, February / March 2013.
[23] Georg Fuchsbauer, Constrained Verifiable Random Functions, in: *SCN 14* (Michel Abdalla and Roberto De Prisco, eds.), LNCS 8642, pp. 95–114, Springer, Heidelberg, September 2014.
[24] Steven D. Galbraith, *Authenticated key exchange for SIDH*, Cryptology ePrint Archive, Report 2018/266, 2018, https://eprint.iacr.org/2018/266.
[25] Sanjam Garg, Craig Gentry and Shai Halevi, Candidate Multilinear Maps from Ideal Lattices, in: *EUROCRYPT 2013* (Thomas Johansson and Phong Q. Nguyen, eds.), LNCS 7881, pp. 1–17, Springer, Heidelberg, May 2013.

[26] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai and Brent Waters, Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits, in: *54th FOCS*, pp. 40–49, IEEE Computer Society Press, October 2013.

[27] Sanjam Garg, Craig Gentry, Amit Sahai and Brent Waters, Witness encryption and its applications, in: *45th ACM STOC* (Dan Boneh, Tim Roughgarden and Joan Feigenbaum, eds.), pp. 467–476, ACM Press, June 2013.

[28] Shafi Goldwasser, Yael Tauman Kalai, Raluca A. Popa, Vinod Vaikuntanathan and Nickolai Zeldovich, How to Run Turing Machines on Encrypted Data, in: *CRYPTO 2013, Part II* (Ran Canetti and Juan A. Garay, eds.), LNCS 8043, pp. 536–553, Springer, Heidelberg, August 2013.

[29] Tsuyoshi Hayashida, A class number associated with a product of two elliptic curves, *Natur. Sci. Rep. Ochanomizu Univ.* **16** (1965), 9–19.

[30] Tsuyoshi Hayashida and Mieo Nishi, Existence of curves of genus two on a product of two elliptic curves, *J. Math. Soc. Japan* **17** (1965), 1–16.

[31] Jun-ichi Igusa, Arithmetic variety of moduli for genus two, *Ann. of Math. (2)* **72** (1960), 612–649.

[32] Antoine Joux, A One Round Protocol for Tripartite Diffie-Hellman, *Journal of Cryptology* **17** (2004), 263–276.

[33] Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos and Thomas Zacharias, Delegatable pseudorandom functions and applications, in: *ACM CCS 13* (Ahmad-Reza Sadeghi, Virgil D. Gligor and Moti Yung, eds.), pp. 669–684, ACM Press, November 2013.

[34] Herbert Lange, *Principal polarizations on products of elliptic curves*, The geometry of Riemann surfaces and abelian varieties, Contemp. Math. 397, Amer. Math. Soc., Providence, RI, 2006, pp. 153–162.

[35] Anna Lysyanskaya, Unique Signatures and Verifiable Random Functions from the DH-DDH Separation, in: *CRYPTO 2002* (Moti Yung, ed.), LNCS 2442, pp. 597–612, Springer, Heidelberg, August 2002.

[36] Silvio Micali, Michael O. Rabin and Salil P. Vadhan, Verifiable Random Functions, in: *40th FOCS*, pp. 120–130, IEEE Computer Society Press, October 1999.

[37] Vanishree Rao, *Adaptive Multiparty Non-interactive Key Exchange Without Setup In The Standard Model*, Cryptology ePrint Archive, Report 2014/910, 2014, http://eprint.iacr.org/2014/910.

[38] Alexander Rostovtsev and Anton Stolbunov, *Public-Key Cryptosystem Based On Isogenies*, Cryptology ePrint Archive, Report 2006/145, 2006, http://eprint.iacr.org/2006/145.

[39] Tetsuji Shioda, Supersingular K3 surfaces, in: *Algebraic Geometry* (Knud Lønsted, ed.), Lecture Notes in Mathematics 732, pp. 564–591, Springer, 1978.

[40] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.

[41] Jiangwei Xue, Tse-Chung Yang and Chia-Fu Yu, On superspecial abelian surfaces over finite fields, *Documenta Mathematica* **21** (2016), 1607–1643.

[42] Mark Zhandry, How to Avoid Obfuscation Using Witness PRFs, in: *TCC 2016-A, Part II* (Eyal Kushilevitz and Tal Malkin, eds.), LNCS 9563, pp. 421–448, Springer, Heidelberg, January 2016.