

Isogeny graphs in superposition and quantum onion routing

Eleni Agathocleous¹, Tobias Hartung^{2,3}, Karl Jansen^{1,4} and Lukas Mansour⁴

¹*Computation-Based Science and Technology Research Center, The Cyprus Institute, 20 Kavafi Street, Nicosia 2121, Cyprus*

²*Department of Computing, Northeastern University–London, Devon House, St Katharine Docks, London E1W 1LP, United Kingdom*

³*Khoury College of Computer Sciences, Northeastern University, 202 West Village Residence Complex H, 440 Huntington Ave, Boston, Massachusetts 02115, USA*

⁴*Deutsches Elektronen-Synchrotron DESY, Platanenallee 6, 15738 Zeuthen, Germany*



(Received 12 January 2026; accepted 5 June 2026; published 28 July 2026)

Onion routing provides anonymity by layering encryption so that no relay can link sender to destination. A quantum analog faces a core obstacle: Layered quantum encryption generally requires symmetric encryption schemes, whereas classically one would heavily rely on public key encryption. We propose a symmetric-encryption-based quantum onion routing (QOR) scheme by instantiating each layer with the Abelian ideal class group action from the theory of complex multiplication. Session keys are established locally via a Diffie-Hellman key exchange between neighbors in the chain of communication. Furthermore, we propose a “nonlocal” key exchange between the sender and receiver. The underlying problem remains hard even for quantum adversaries and underpins the security of current postquantum schemes. We connect our construction to isogeny graphs and their association schemes, using the Bose-Mesner algebra to formalize commutativity and guide implementation. We give two implementation paths: (i) a universal quantum oracle evaluating the class group action with polynomially many quantum resources and (ii) an intrinsically quantum approach via continuous-time quantum walks, outlined here and developed in a companion paper. A small Qiskit example illustrates the mechanics (by design, not the efficiency) of the QOR.

DOI: [10.1103/9ml3-5nhy](https://doi.org/10.1103/9ml3-5nhy)

I. INTRODUCTION

Onion routing is a privacy-enhancing network protocol whose primary goal is anonymity. Beyond transport security, it uses layered encryption so no single relay can link sender to destination. Onion routing anonymises network traffic by wrapping it in multiple layers of encryption and sending it through a short chain of relays (guard $\rightarrow$ middle $\rightarrow$ exit). Each relay peels one layer and knows only the next hop, so no single node can link source and destination. If sufficient network traffic is present, then this ensures that an outside observer can only link the sender of a message to the guard server and the receiver to the exit server, but tracking the communication through the network is difficult. Thus, onion routing not only keeps the message hidden but also hides who is communicating with whom.

A quantum analog of onion-routing encounters challenges intrinsic to quantum computing. First and foremost, the fact that every quantum operation is unitary implies that any operation performed on a state is reversible with relative ease. Thus, any cryptographic setup in which the message is encoded as a state and the encryption works as a function (determined by the key) on the message state is necessarily a symmetric

encryption scheme. Public key encryption in a quantum computing setting therefore (up to further complications) has the key as a state and the message defining the operation performed or has a fixed state and both key and message define the operation. The decryption process then relies on identifying which operation was performed by the sender and reconstructing the message from that information. Although theoretically possible, such an asymmetric encryption scheme cannot easily be layered, if the message is a genuine quantum state (as opposed to a bit-state encoded in qubits).

The main goal of this paper is to overcome these problems and design a quantum onion routing through layered symmetric quantum encryption. We achieve this by basing each layer on the *ideal class group action* from number theory and specifically from the *theory of complex multiplication*. The associated group-action inversion (vectorization) problem remains hard even for quantum adversaries and underpins postquantum schemes such as CSIDH [1]. “Local session keys” are generated via Diffie-Hellman key exchange for neighboring nodes in the chain of communication. Furthermore, we propose a method of communicating a “global session key” chosen by the sender to the receiver that allows for the final decryption step.

Of course, many of the individual components of the proposed quantum onion routing scheme can be replaced with quantum encryption schemes that serve a similar role. For example, local session keys can be established using quantum key distribution and the global session key encryption layer can be replaced with a quantum public key encryption layer.

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

However, it is advantageous to base the entire scheme on a single underlying problem, such as for ease of implementation. This means that all encryption layers need to use compatible schemes. The isogeny-based postquantum cryptography scheme chosen allows for exactly that while it is also possible to use the same scheme for classical encryption problems. Thus, the here-proposed quantum onion routing scheme is also more easily compatible with larger systems requiring both classical and quantum cryptographic schemes.

Incidentally, this also allows us to further develop the intersection of postquantum cryptography with quantum computing. A secondary goal of this paper is therefore to implement an isogeny-based postquantum cryptographic scheme within a quantum-computing-based protocol and execution routine.

The paper is structured as follows. In Sec. II we provide a brief account of the main facts and definitions from the theory of complex multiplication necessary to understand the rational behind our quantum onion routing construction (QOR). Section III lifts the problem to the path-finding problem on isogeny graphs and discusses security assumptions. Section IV connects isogeny graphs to association schemes and their Bose-Mesner algebra, yielding two implementation paths for QOR. The first uses a universal quantum oracle that evaluates the class group action with polynomially many quantum resources. We also outline a second, more intrinsically quantum route based on continuous-time quantum walks (CTQWs) [2,3]; this line is developed in a companion work and not pursued further here. Section V presents a high-level overview of a fully worked example of the QOR protocol with five actors; the full details, including a Qiskit implementation, are presented in Appendix. The fully worked example is deliberately small and exponential in resources, and its purpose is to make the mechanics of QOR explicit. Finally, Sec. VI briefly discusses certain security considerations in classical vs quantum settings.

II. THE IDEAL CLASS GROUP ACTION

For any given fundamental discriminant $\Delta < 0$, we denote by $K_\Delta = \mathbb{Q}(\sqrt{\Delta})$ the corresponding imaginary quadratic number field, and by $\text{Cl}(\mathcal{O}_\Delta)$ the ideal class group of the maximal order $\mathcal{O}_\Delta$. We write $h(\Delta) = |\text{Cl}(\mathcal{O}_\Delta)|$ for the class number. Associated to $\text{Cl}(\mathcal{O}_\Delta)$ is the maximal Abelian unramified extension H_Δ of K_Δ , known as the Hilbert class field of K_Δ .

Fundamental results from class field theory and the theory of complex multiplication yield the following important result:

Theorem 1 ([4], Sec. 10.3, Theorem 5). For any imaginary quadratic number field $K_\Delta = \mathbb{Q}(\sqrt{\Delta})$ with maximal order $\mathcal{O}_\Delta$ and ideal class group $\text{Cl}(\mathcal{O}_\Delta)$, we let $\{\mathfrak{a}_s\}_{1 \leq s \leq h(\Delta)}$ be a set of representatives for the $h(\Delta)$ -many distinct ideal classes of $\text{Cl}(\mathcal{O}_\Delta)$. Then the numbers $j(\mathfrak{a}_i)$ are all conjugate over K_Δ and over $\mathbb{Q}$. For any representative $\mathfrak{a} \in \{\mathfrak{a}_s\}_{1 \leq s \leq h(\Delta)}$ the following isomorphism holds true:

$$\text{Cl}(\mathcal{O}_\Delta) \cong \text{Gal}(K(j(\mathfrak{a}))/K), \text{ via the explicit map } \mathfrak{b} \mapsto \sigma_{\mathfrak{b}}.$$

The irreducible polynomial having the $h(\Delta)$ -many algebraic integers $j(\mathfrak{a}_s)$ as roots is called the *Hilbert class polynomial*

associated to the order $\mathcal{O}_\Delta$ and is given by

$$H_\Delta(x) = \prod_{1 \leq s \leq h(\Delta)} (x - j(\mathfrak{a}_s)) \in \mathbb{Z}[x].$$

The action of $\text{Cl}(\mathcal{O}_\Delta) \cong \text{Gal}(K(j(\mathfrak{a}))/K)$ on the roots of H_Δ is given by

$$\sigma_{\mathfrak{b}} j(\mathfrak{a}) = j(\mathfrak{b}^{-1} \mathfrak{a}),$$

and this action is free and transitive.

Remark 1. Let us denote the class group action by “ $*$ ”. As the ideal class group is an Abelian group, given Theorem 1 above, we easily conclude that

$$\mathfrak{a}\mathfrak{b} * j(\mathfrak{c}) = j((\mathfrak{a}\mathfrak{b})^{-1} \mathfrak{c}) = j((\mathfrak{b}\mathfrak{a})^{-1} \mathfrak{c}) = \mathfrak{b}\mathfrak{a} * j(\mathfrak{c}).$$

The action of the fractional ideals on the roots of H_Δ defined in the Theorem 1 above, is what is referred to in cryptography as *the class group action*. Together with Deuring’s theorems (e.g., Refs. [5] and [4], Theorem 12, Sec. 13.4 and Theorem 14, Sec. 13.5), which enable the transition from characteristic zero to characteristic p and vice versa, are the key ingredients that make isogeny-based cryptography built on the ideal class group action, possible. In the ordinary case in particular, where H_Δ splits completely in $h(\Delta)$ -many distinct roots over $\mathbb{F}_q$, an elliptic curve in characteristic zero with j -invariant a root of H_Δ and an elliptic curve in characteristic p with j -invariant a root of $H_\Delta \bmod q$ have isomorphic endomorphism rings. Furthermore, the class group action in characteristic zero respects this isomorphism, and we observe the same class group action on the roots of H_Δ modulo q .

Even in the supersingular case, if instead of the full ring of endomorphisms, which is noncommutative, we consider the subring of $\mathbb{F}_p$ -rational endomorphisms, this subring is again an order in an imaginary quadratic field and the ideal class group action applies as above. The advantage is that now the supersingular elliptic curves $E/\mathbb{F}_p$ have known trace $t = 0$ and known number of points $|E(\mathbb{F}_p)| = p + 1$. Hence, with the right choice of a prime p we can have $\mathbb{F}_p$ -rational isogenies of desired degree ℓ , as long as $\ell \nmid p + 1$. That is why the existing cryptographic schemes based on the ideal class group action, such as CSIDH [1] and SCURF [6], employ supersingular curves.

The one-to-one correspondence between the classes $[\mathfrak{a}]$ of the ideal class group $\text{Cl}(\mathcal{O}_\Delta)$ and the homothety classes of lattices $[\Lambda_{\mathfrak{a}}] \cong [(1, \tau_{\mathfrak{a}})]$ with $\mathcal{O}_\Delta$ as their full ring of complex multiplication [[7], Corollary 10.20] was employed by the authors of Refs. [[8], Theorem 3.2.] in order to show that the isogeny graph $G_{\Delta,S,q}(J_\Delta, E_S)$ is isomorphic to the Cayley graph $\mathcal{G}(\text{Cl}(\mathcal{O}_\Delta), S)$, for some set S that does not contain the identity element and is closed under inversion. The set of vertices $J_\Delta = \{j_1, \dots, j_{h(\Delta)}\} \subseteq \mathbb{F}_q$ contains the $h(\Delta)$ -many distinct roots of H_Δ modulo q . Every edge $(j_1, j_2) \in E_S$ corresponds to an isogeny between elliptic curves E_1, E_2 with corresponding j -invariants $j_1, j_2 \in J_\Delta$. The degree of any such isogeny equals some positive integer b such that $b = \text{Norm}_{K_\Delta/\mathbb{Q}}(\mathfrak{b})$ for some ideal $\mathfrak{b} \in S$. When we include in S all ideals of prime norm less than some fixed bound $M \geq (\log |\Delta|)^B$, for some absolute constant $B > 2$ then, assuming GRH, the isogeny graph $G_{\Delta,S,q}$ becomes an expander graph [[8], Theorem 3.2.].

III. WALKS ON ISOGENY GRAPHS

A. The Cayley graph of the ideal class group

As the ideal class group of a number field is a finite Abelian group and the isogeny graphs are isomorphic to Cayley graphs of the underlying ideal class group, we focus our attention on Cayley graphs of finite abelian groups. For the basic facts and definitions that we quote in the following, we follow mainly Refs. [9,10].

Let us denote by Γ any finite Abelian group written multiplicatively, and with identity element 1_Γ . Let $1_\Gamma \notin S \subseteq \Gamma$ be any subset that is closed under taking inverses. Then the *Cayley graph* $\mathcal{G}(\Gamma, S)$ is the graph with vertex set $V(\mathcal{G}) = \Gamma$ and edge set

$$E(\mathcal{G}) = E(\mathcal{G}(\Gamma, S)) = \{gh \mid hg^{-1} \in S\}.$$

A *subgraph* $\mathcal{G}'$ of $\mathcal{G}$ is a graph with $V(\mathcal{G}') \subseteq V(\mathcal{G})$ and $E(\mathcal{G}') \subseteq E(\mathcal{G})$. In the case where $V(\mathcal{G}') = V(\mathcal{G})$, $\mathcal{G}'$ is called a *spanning subgraph* of $\mathcal{G}$.

The graph $\mathcal{G}(\Gamma, S)$ is an undirected graph with no loops. It is, as expected, vertex transitive. Recall from above that $G_{\Delta,S,q}(J_\Delta, E_\Delta) \cong \mathcal{G}(\text{Cl}(\mathcal{O}_\Delta), S)$ and the ideal class group action on $J_\Delta \equiv V(\mathcal{G}(\text{Cl}(\mathcal{O}_\Delta), S))$ is free and transitive. Vertex-transitive graphs are regular; i.e., each vertex has the same number of edges $k \leq |S|$. This integer k is called the *degree*. When we choose S to be a generating set for Γ , then the graph is connected.

The *adjacency matrix* $A(\mathcal{G})$ of the connected undirected regular graph $\mathcal{G}(\Gamma, S)$ is the $n \times n$ real symmetric matrix, with entries $a_{i,j} = 1$ if $(v_i, v_j) \in E(\mathcal{G})$ and $a_{i,j} = 0$ if $(v_i, v_j) \notin E(\mathcal{G})$. As a real symmetric matrix, $A(\mathcal{G})$ has real eigenvalues $\lambda_n \leq \dots \leq \lambda_1 = k$, where as above, k is the degree. Each eigenvalue of A can be given in the form

$$\lambda_\chi = \sum_{s \in S} \chi(s), \quad \chi \in \hat{\Gamma},$$

where as customary $\hat{\Gamma}$ denotes the character group of the finite Abelian group Γ , which is isomorphic (noncanonically) to Γ and hence it is of the same cardinality $n = |\Gamma| = |\hat{\Gamma}|$. Thus, the spectrum of $\mathcal{G}(\Gamma, S)$ consists of character sums ranging over the generating set S .

B. Random walks

As we mentioned in Sec. II, in the case of isogeny graphs $\mathcal{G}_{\Delta,S,q}$ and for an appropriate set S , the result of Ref. [8] guarantees that these graphs become expander graphs. In terms of the eigenvalues, what this result yields is a bound on the spectral gap. More specifically, the absolute value of every eigenvalue $\lambda \neq \lambda_1$ should be of the order $|\lambda| = O((\lambda_1 \log \lambda_1)^{1/2+1/B})$ for some absolute constant $B > 2$, and $M \geq (\log |\Delta|)^B$ is such that $S = S_M = S_M^{-1}$ contains the ideals of prime norm up to M . With such a choice of S , there exists a constant $C > 0$ such that any walk on $\mathcal{G}_{\Delta,S,q}$ of length

$$t \geq C \frac{\log |\text{Cl}(\mathcal{O}_\Delta)|}{\log \log q} \quad (1)$$

is well mixed.

Assume for simplicity that $\text{Cl}(\mathcal{O}_\Delta) \cong \mathbb{Z}/r\mathbb{Z}$ is cyclic of odd prime order r . In implementation terms, for a walk

of length t on the associated isogeny graph, choose some generator $g \in \text{Cl}(\mathcal{O})$ and also choose uniformly at random $k = C \lceil \log r \rceil$ exponents $c_1, \dots, c_k \in (\mathbb{Z}/r\mathbb{Z})^\times$, sample a random word $w = (c_{s_1}, \dots, c_{s_m})$ with $s_\ell \in \{1, \dots, k\}$, and form the class-group element

$$g^e, \quad e \equiv \sum_{\ell=1}^m c_{s_\ell} \pmod{r}. \quad (2)$$

This random element g^e is then used for the class group action on the given j -invariant, say, j_0 , to yield the end point $g^e * j_0 = j_1$ of the walk.

We rely on the *vectorization* (group-action inversion) problem for the ideal class group action, which is believed to remain hard even for quantum adversaries. Concretely: Given a pair of j -invariants (j_0, j_1) , it is not possible in quantum polynomial time to recover the secret $g^e \in \text{Cl}(\mathcal{O}_\Delta)$ such that $g^e * j_0 = j_1$. Equivalently, one cannot efficiently reconstruct a path (walk) on the underlying isogeny graph $\mathcal{G}_{\Delta,S,q}$ connecting j_0 to j_1 .

In Sec. IV B we describe these isogeny graphs via association schemes and their Bose-Mesner algebra, with emphasis on the cyclic, prime-order case; in this setting the graph is a disjoint union of undirected r -cycles. This perspective both places the path-finding problem in an algebraic-spectral context and sets the stage for a parallel line of work in which we exploit this structure to implement our quantum onion routing via CTQWs.

IV. QUANTUM ONION ROUTING BASED ON THE IDEAL CLASS GROUP ACTION

The main goal of this paper is to construct a quantum onion routing scheme based on the ideal class group action. Without loss of generality, we present our construction in the ordinary case and, as we already discussed in Sec. II, the same ideas readily extend to the supersingular setting, in the same way as CSIDH and CSURF extended the original CRS in the Diffie-Hellman context.

Given Δ , p , and $a > 0$, the ideal class group $\text{Cl}(\mathcal{O}_\Delta)$ can be computed in quantum-polynomial time [[11], Theorem 3]. We choose Δ so as $\text{Cl}(\mathcal{O}_\Delta)$ has a large-enough, for security reasons, cyclic part. Such discriminants are not hard to find since, according to the Cohen-Lenstra heuristics [12], the odd part of the class group of imaginary quadratic number fields is cyclic with probability $\sim 97.7575 \dots \%$.

In order to simplify our scheme and notation, from now on we will assume further that $\text{Cl}(\mathcal{O}) \cong \mathbb{Z}/r\mathbb{Z}$, for r a large prime of exponential size, and that $a = 1$; i.e., $q = p$. The set

$$J = \{j_i : 0 \leq i \leq r-1\} \subset F_p$$

contains the $r = |\text{Cl}(\mathcal{O})|$ -many j -invariants. The corresponding isogeny graph is isomorphic to the Cayley graph $\mathcal{G}_r := \mathcal{G}(\text{Cl}(\mathcal{O}_\Delta), S) \cong \mathcal{G}(\mathbb{Z}/r\mathbb{Z}, S)$ for a spanning set $S \subset \text{Cl}(\mathcal{O}_\Delta)$; i.e., we include in S all ideals of prime norm less than some fixed bound $M \geq (\log |\Delta|)^B$, for some absolute constant $B > 2$, as we discussed in the end of Sec. II.

In this prime-order case, every nontrivial subgraph is a spanning subgraph of $\mathcal{G}_r$, and a random element g^e , as in Eq. (2), is a walk on such a graph composed of $O(\log r)$ -many

r -cycles. As the ideal class group action is commutative (cf. Remark 1) and injective (see, e.g., Ref. [[13], Lemma 5.1]), layered encryptions are possible also in the quantum setting, as reversibility is guaranteed.

A naive sketch of the protocol, with only three users present for simplicity, is outlined below in Procedure 1. These three users will be called Alice (sender), Bob (intermediary), and Carol (receiver).

Procedure 1. High-level overview of the first part of the protocol

(1) Fix and make public a j -invariant $j_0 \in J_\Delta$.

(2) When Carol is notified by Bob that somebody wants to send her a message, she computes her secret element $c \in \text{Cl}(O_\Delta)$ as described in Eq. (2) and sends to Bob

$$c * j_0 = j_C.$$

(3) Bob encrypts with his secret $b \in \text{Cl}(O_\Delta)$ and sends to Alice

$$b * j_C = j_{BC} = j_{CB}.$$

(4) Alice does the same with her secret $a \in \text{Cl}(O_\Delta)$ and sends back to Bob

$$a * j_{BC} = j_{ABC}.$$

(5) Bob removes his encryption by applying

$$b^{-1} * j_{ABC} = j_{AC}.$$

(6) When Carol receives j_{AC} from Bob, she undoes her encryption as well and obtains Alice's key j_A , which she will now use to read Alice's message.

In terms of implementation, there are two fundamental issues. First, we need to specify how to apply the class group action $*$ and how to deal with the exponentially large isogeny graph. Second, we need to specify where and how to hide Alice's message. The subsequent sections are devoted to answering these questions.

A. The message encryption

Let $|m\rangle \in \mathcal{M}$ be the quantum message in the message space $\mathcal{M}$ of dimension 2^N . To each j -invariant $j \in J_\Delta \subseteq \mathbb{F}_p$, which can be represented by $\log p$ -many qubits, we can associate a quantum circuit $C(j)$ on N -qubits as follows:

$$C(j) = \bigotimes_{k=0}^{N-1} R_X(\vartheta_k(j)). \quad (3)$$

For the angles $\vartheta_k(j)$, we take a fixed N -dimensional (scrambled) Sobol' sequence S , choose Sobol' point S_{2^k+j} , and $\vartheta_k(j)$ is 2π times the k th coordinate of the Sobol' point. Since the Sobol' points are more uniform, the potential rotation angles are uniformly distributed in the parameter space. To make this as uniform as possible, we want the band $[2^K, 2^K + p]$ to be as close to $[2^K, 2^K]$ as possible; i.e., $p \approx 2^K$ gives the band $[2^K, 2^{K+1}]$, which is the case for our cryptographic construction since p needs to be of exponential size.

Remark 2. It should be noted that the explicit choice of R_X gates with Sobol' sequence generated angles is not critical for the implementation. The choice above is motivated by the fact that any classical bit encoded in a qubit is securely encrypted

as $\cos \frac{\vartheta_k(j)}{2} |0\rangle - i \sin \frac{\vartheta_k(j)}{2} |1\rangle$ or $-i \sin \frac{\vartheta_k(j)}{2} |0\rangle + \cos \frac{\vartheta_k(j)}{2} |1\rangle$ depending on whether the bit was in state $|0\rangle$ or $|1\rangle$, respectively. Since the $\vartheta_k(j)$ are quasiuniform in $[0, 2\pi]$, the expected probability of measuring the encrypted qubit in $|0\rangle$ is $\frac{1}{2}$ independent of the original bit value. Hence, no information about the single qubit clear text is retrievable. Of course, this may not be true for messages that are encoded in eigenstates of the R_X gates. However, replacing the message encryption method with any suitable and efficiently implementable circuit construction from the j -invariants would be viable. For example, one could choose U -gates instead and a Sobol' sequence of size $3N$. Adding entangling gates may also be considered. One may also choose mappings that do not use Sobol' sequences, however, a deterministic method mapping j -invariants to a "sufficiently random" gate set is required since sender and recipient must produce the same gate from the given j -invariant.

Going back to step (4) of the naive Procedure 1 above, Alice could send to Bob

$$(j_{ABC}, C(j_A)|m)),$$

where $|m\rangle \in \mathcal{M}$ is her secret message. Bob can undo his encryption and send

$$(j_{AC}, C(j_A)|m))$$

to Carol, and once Carol obtains j_A , then she can read Alice's message by using the inverse circuit, i.e.,

$$C(j_A)^{-1} C(j_A)|m).$$

We notice, however, that the hidden message $C(j_A)|m$ remains the same throughout the channel. Even though quantum data cannot be cloned nor observed without tampering, one can still make imperfect copies of this message and, in case they obtain a big overlap, then the communications channel will be revealed. To address this issue, we propose the following variant that makes use of an additional Diffie-Hellman setup.

Every user in the network has an established shared secret key with their neighbor (either via quantum or classical computation). The secret shared key is another j -invariant derived through Diffie-Hellman using the class group action. In this scenario, the exchange can proceed as shown in Procedure 2:

Procedure 2. Hiding the quantum message

(1) Alice sends $(j_{ABC}, C(j_{ab})C(j_A)|m))$ to Bob.

(2) Bob removes the encryption via the inverse circuit $C(j_{ab})^{-1}$ associated with his secret shared key j_{ab} with Alice and then adds the encryption $C(j_{bc})$ associated with his shared secret key j_{bc} with Carol and sends her the following $(j_{AC}, C(j_{bc})C(j_A)|m))$.

(3) By removing the encryptions, Carol can read $(j_A, C(j_A)|m))$ and she can now obtain the message m by applying the inverse circuit $C(j_A)^{-1}$.

In the next section we will define association schemes with respect to isogeny graphs—a viewpoint that clarifies and streamlines the implementation of the "quantum" class group action.

B. Cyclic association schemes and their Bose-Mesner algebra

In this section we collect basic facts and definitions for cyclic association schemes and their Bose-Mesner algebra, noting that many of these facts may still hold for association schemes in general. For more details the interested reader may refer to Ref. [14] or to Ref. [3] for a more concise account.

For any integer $n \geq 3$ we denote by C_n the cycle-graph of length n . It is a Cayley graph over $\mathbb{Z}/n\mathbb{Z}$ with generating set $\{1, n-1\}$ (modulo n). We let $d = \lfloor \frac{n}{2} \rfloor$ and for $0 \leq s \leq d$ we consider the following adjacency matrices A_s , where the indices of the matrices are computed modulo n :

$$(A_s)_{j,k} = \begin{cases} 1; & \text{if } j-k \in \{s, -s\} \\ 0; & \text{o.w.} \end{cases}.$$

For any matrix M we denote by M^t its transpose. We denote by A_0 the $n \times n$ identity matrix and by $J = J_n$ the all-ones matrix. We notice that A_1 is the adjacency matrix of C_n . The set of matrices

$$\mathcal{A}_n = \{A_0, \dots, A_d\}$$

can be proven to form a special type of a *symmetric d -class association scheme* (e.g., Ref. [3], pp. 19–20), known as the *cyclic association scheme of order n* .

Definition 1. A set of $n \times n$ -dimensional symmetric 01-matrices $\mathcal{A} = \{A_0, \dots, A_d\}$ is called a *d -class symmetric association scheme* if

- (1) $A_0 = I_n$
- (2) $\sum_{j=0}^d A_j = J_n$
- (3) $\forall A_j \in \mathcal{A}, A_j^t \in \mathcal{A}$
- (4) There are integers $p_{ij}(k)$, known as *intersection parameters*, such that

$$A_i A_j = \sum_{k=0}^d p_{ij}(k) A_k, \quad \forall 0 \leq i, j \leq d.$$

- (5) For $0 \leq j \leq d$ in particular, we have that $n_j := p_{j,j}(0)$ is the degree of the regular graph corresponding to the adjacency $A_j \in \mathcal{A}$.

Cyclic symmetric association schemes in particular, enjoy further properties, which we summarize in the following remark.

Remark 3. As a symmetric cyclic association scheme, $\mathcal{A}_n$ has the following properties:

- (1) From Definition 1 one can deduce that $A_i A_j = A_j A_i$ for all $0 \leq i, j \leq d$.
- (2) Cyclic association schemes are distance-regular graphs.
- (3) We let $\mathcal{C} \equiv C_n$ denote the adjacency matrix of the directed cycle of order n . $\mathcal{C}$ is of the form $(\mathcal{C})_{i,j} = 1$ if $j - i = 1$ and $(\mathcal{C})_{i,j} = 0$ otherwise. Then every $A_j \in \mathcal{A}$ can be written in terms of $\mathcal{C}$ as follows:

$$A_j = \begin{cases} \mathcal{C}^j + \mathcal{C}^{-j}; & \text{if } j \notin \{0, n/2\} \\ \frac{1}{2}(\mathcal{C}^j + \mathcal{C}^{-j}); & \text{if } j \in \{0, n/2\} \end{cases}.$$

- (4) The intersection numbers of $\mathcal{A}_n$ are explicitly known:

$$p_{i,j}(k) = \begin{cases} 1; & \text{if } i-j \equiv \pm k \pmod{n} \text{ or } i+j \equiv \pm k \pmod{n} \\ 0; & \text{o.w.} \end{cases}.$$

- (5) For every matrix $M \in \mathbb{C}[\mathcal{A}_n]$ there exists unique polynomial $f(x) \in \mathbb{C}[x]$ of degree $\deg(f(x)) \leq n-1$ such that $M = f(\mathcal{C})$.

- (6) Let ω be a fixed primitive n th root of unity; for example, $\omega = e^{2\pi i/n}$. The explicit eigenvalues of $\mathcal{A}_n$ are given as

$$p_j(s) = \omega^{js} + \omega^{-js}.$$

Given a symmetric association scheme $\mathcal{A}$, Definition 1 implies that the algebra $\mathbb{C}[\mathcal{A}]$, known as the *Bose-Mesner algebra* of $\mathcal{A}$, is a commutative algebra of dimension $d+1$. It is a known result that all matrices of $\mathcal{A}_d$ are simultaneously diagonalizable (see, e.g., Ref. [14]), and hence every $A \in \mathcal{A}_d$ can be written as

$$A = \sum_{0 \leq s \leq d} \theta_s E_s \in \mathcal{A}_d, \quad (4)$$

where the set $\{E_0, E_1, \dots, E_d\}$ is the set of *spectral idempotents* of the association scheme. In the special case of a cyclic symmetric association scheme, each E_s is given by

$$E_s = \begin{cases} \frac{1}{n} \sum_{k=0}^{n-1} (\omega^{ks} + \omega^{-ks}) \mathcal{C}^k; & 1 \leq s \leq \lfloor n/2 \rfloor \\ \frac{1}{n} \sum_{k=0}^{n-1} \omega^{ks} \mathcal{C}^k; & s \in \{0, n/2\}. \end{cases}$$

An isogeny graph $\mathcal{G}_r = \mathcal{G}_{\Delta, S, q}$ with ideal class group $\text{Cl}(\mathcal{O}_\Delta) \cong \mathbb{Z}/r\mathbb{Z}$ (with r an odd prime) can be written as the edge-disjoint union of $|S|/2$ undirected r -cycles. In particular, if $|S| = \Theta(\log r)$, then the graph is a union of $\Theta(\log r)$ -many r -cycles $A_s \in \mathcal{A}_d$. A walk on $\mathcal{G}_r$ corresponding to the element g^e of (2) is a sequence of m -many steps c_s , each one of them carried along one of these r -cycles.

In the next section we analyze these isogeny graphs through the lens of association schemes and their Bose-Mesner algebra, and we discuss isogeny graphs with respect to a purely quantum form of computing, namely that of CTQW, before we continue to the implementation of our QOR via a universal quantum oracle, which we define in Sec. IV E.

C. Isogeny graphs and unitaries

Let us fix a fundamental discriminant Δ and a good prime p that splits the Hilbert class polynomial completely into $h(\Delta)$ -many distinct roots over $\mathbb{F}_q$, $q = p^a$ for some $a \in \mathbb{N}$. Any subgraph of $\mathcal{G} \equiv \mathcal{G}(\text{Cl}(\mathcal{O}_\Delta), S)$ has an associated adjacency matrix A , which forms the Hamiltonian of the quantum system determined by the unitary operator

$$U_A(t) = e^{-itA},$$

also known as the time-evolution operator. The time evolution is described by

$$|\psi(t)\rangle = e^{-itA} |\psi(0)\rangle,$$

where we follow the physicists' notation and write column vectors $\psi \in \mathbb{C}^{n \times 1}$ as kets $|\psi\rangle$.

The unitary $U_A(t)$ corresponds to a walk on the graph with adjacency A , for time t . In isogeny-based schemes this would correspond to the secret walk of a user on the isogeny graph with adjacency A . As the underlying ideal class group action is commutative (cf. Remark 1), the walks are also expected to commute and hence the unitaries are expected to commute. This claim can also be verified rigorously, since one can show that the unitaries lie in the commutative Bose-Mesner algebra.

Lemma 1. Let $\mathcal{A}_d$ denote the symmetric association scheme corresponding to the Cayley graph of a finite cyclic group isomorphic to $\mathbb{Z}/n\mathbb{Z}$, and for any $A \in \mathcal{A}_d$ consider the corresponding unitary $U_A(t) = e^{-itA}$. Given any $A, B \in \mathcal{A}_d$, we have that the corresponding unitaries commute; i.e.,

$$U_A(t_A)U_B(t_B) = U_B(t_B)U_A(t_A).$$

Proof. For any $A \in \mathcal{A}_d$ it follows easily via Eq. (4) (see, e.g., Ref. [[3], Lemma 3.2.4]), that the corresponding unitary belongs to the Bose-Mesner algebra

$$U_A(t) = \sum_{0 \leq s \leq d} e^{-it\theta_{A,s}} E_s \in \mathbb{C}[\mathcal{A}_d]. \quad (5)$$

Since the algebra is commutative, the claim follows. ■

One can now express the walk on the isogeny graph induced by the action of the element g^e , $e \equiv \sum_{\ell=1}^m c_{s_\ell} \pmod{r}$ of Eq. (2), in terms of unitaries, as follows:

$$g^e * j_0 \equiv \prod_{\ell=1}^m U_{c_{s_\ell}}(t_{s_\ell}) |j_0\rangle. \quad (6)$$

Further study of the isogeny walk via a CTQW is being carried out in a parallel project. In the next section we assume the existence of a universal oracle for the class group action and describe in detail how the QOR protocol runs under this assumption, leaving the discussion for the quantum oracle in the last subsection, Sec. IV E.

D. Isogeny graphs in superposition

As above, we assume for simplicity that $\text{Cl}(\mathcal{O}) \cong \mathbb{Z}/r\mathbb{Z}$ for r a large prime of exponential size. The set

$$J = \{j_i : 0 \leq i \leq r-1\} \subseteq \mathbb{F}_p$$

contains the r -many j -invariants associated with $\text{Cl}(\mathcal{O})$, and $j_0 \in J$ is a fixed public j -invariant. The corresponding cyclic association scheme $\mathcal{A}_d$, is of order $d = \frac{r-1}{2}$, also of exponential size.

Procedure 3. Isogeny graphs in superposition and the QOR

When Bob notifies Carol that somebody wants to send her a message,

(1) Carol chooses and keeps secret a random element $\mathfrak{c} = g_C^c \in \text{Cl}(\mathcal{O})$, constructed as discussed above. The associated isogeny graph corresponding to the action of $\mathfrak{c}$ on the j -invariants of the set J is represented by an adjacency matrix, which we denote by C , and $C \in \mathcal{A}_d$.

(2) Carol furthermore chooses two secret values $\omega, \Omega \in \mathbb{Z}/r\mathbb{Z}$ satisfying $0 \leq \omega < r$ and $0 \leq \Omega < r - \omega$. Here we assume both ω and Ω to be of polynomial size, although this restriction can be lifted relative to a “global mapper oracle,” cf. Sec. IV E. Carol prepares a uniform superposition over $i \in \mathbb{Z}/\Omega\mathbb{Z}$,

$$\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle.$$

(3) She then loads $|j_0\rangle$ into another register and applies her unitary operator U_C , which we can interpret as a quantum oracle f_C , that computes in quantum parallelism the class

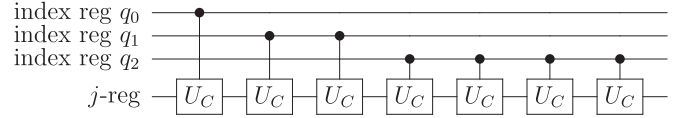


FIG. 1. Example Carol’s of the “mapper oracle” for a three-qubit index register. In general, this simple mapper oracle implementation requires $2^{\lceil \log_2 \Omega \rceil} - 1$ controlled shift oracles U_C .

group action, $*$, and gives the resulting j -invariant,

$$|i\rangle \otimes |j_0\rangle \mapsto |i\rangle \otimes |f_C(j_0)\rangle = |i\rangle \otimes |\mathfrak{c}^1 * j_0\rangle = |i\rangle \otimes |j_1\rangle.$$

Applying the oracle ω times, yields the resulting state

$$\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_\omega\rangle.$$

(4) Finally, Carol applies a “mapper oracle” as shown in Fig. 1. This mapper oracle¹ applies her oracle i many times if the control register is in the state $|i\rangle$. The resulting state is

$$\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_{i+\omega}\rangle.$$

If possible in practical implementations, then Carol should retain the index-register (containing the $|i\rangle$ factor) at all times. However, the communication scheme remains secure if both the index- and j -register qubits are sent during the protocol. For simplicity, we will assume that Carol retains the index-register.

(5) Carol sends the quantum state

$$|\psi_0\rangle = \frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |j_{i+\omega}\rangle,$$

which corresponds to a part of the isogeny-cycle in superposition produced by the element $\mathfrak{c} \in \text{Cl}(\mathcal{O}_\Delta)$ acting on the set J , to Bob.

(6) In the same way, Bob chooses $\mathfrak{b} = g_B^b \in \text{Cl}(\mathcal{O}_\Delta)$, which corresponds to his adjacency $B \in \mathcal{A}_d$. His associated quantum oracle f_B computes the class group action, i.e.,

$$f_B(j) = \mathfrak{b} * j,$$

and Bob computes and sends to Alice the following state:

$$|\psi_1\rangle = \frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |f_B(j_{i+\omega})\rangle.$$

(7) Similarly, Alice chooses her secret $\mathfrak{a} = g_A^a \in \text{Cl}(\mathcal{O}_\Delta)$, corresponding to some adjacency matrix $A \in \mathcal{A}_d$, and with her quantum oracle f_A computes her class group action. She also attaches the message $|m\rangle$ which is encrypted with the circuit $C(j_A)$, $j_A = \mathfrak{a} * j_0$ (preventing Bob from reading the message)

¹The requirement for Ω to be of polynomial size implies that this mapper oracle is constructable in polynomial time from her shift oracle U_C . As U_C needs to be compiled into a valid gate sequence, each gate in the U_C -sequence can be replaced with their controlled version to obtain a gate sequence for the controlled- U_C gate.

and the transport encryption layer $C(j_{ab})$ (preventing tracking of the message). Thus, she sends the following state:

$$|\psi_2\rangle = \frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |f_A(f_B(j_{i+\omega}))\rangle \otimes C(j_{ab})C(j_A)|m\rangle$$

back to Bob.

(8) Bob undoes his oracle f_B on the j -invariants register, modifies the message as discussed in Sec. IV A, and obtains

$$|\psi_3\rangle = \frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |f_A(j_{i+\omega})\rangle \otimes C(j_{bc})C(j_A)|m\rangle$$

which he sends on to Carol.

(9) Carol removes the transport encryption layer $C(j_{bc})$ from the message and splits the message register off. Combining the j -invariants register with the index-register again, she obtains two separate quantum states; the still encrypted message $C(j_A)|m\rangle$ and the key information state

$$|\psi_4\rangle = \frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_A(j_{i+\omega})\rangle.$$

(10) Carol now measures the key information state $|\psi_4\rangle$ and obtains a random state $|i\rangle \otimes |f_A(j_{i+\omega})\rangle$. From this, she can compute $j_A = \mathfrak{c}^{-i-\omega} f_A(j_{i+\omega})$ either classically or using her oracles (as we will in Sec. V).²

(11) Finally, Carol can now apply $C(j_A)^{-1}$ to the message register and retrieve Alice's secret message $|m\rangle$.

Remark 4. It should be noted that the message encryption via $C(j_A)|m\rangle$ could also be replaced with a quantum public key encryption system. In that case, the procedure required to communicate j_A from Alice to Carol is not necessary as Carol retains her private key and the cryptosystem is asymmetric, i.e., cannot be broken based on the public knowledge of the public key. However, that also requires combining two separate encryption systems within the quantum onion routing communications protocol, which may or may not be wise. There are multiple dimensions to consider here. On the one hand, having two different underlying hard mathematical problems means that if one is broken, then the message may still be safe. On the other, having compatible schemes is desirable in terms of design principles, as is also evident in our construction which combines circuits of j -invariants resulting from both the Diffie-Hellmann as well as the layered encryptions. At the same time, however, using the same underlying problem for both schemes can compromise the quantum onion routing protocol because breaking that underlying problem reveals everything, while using different underlying problems means that if the $C(j_A)$ layer is broken, then any intermediary (Bob) can read the message, while breaking the Diffie-Hellman layer allows for tracking of the communication; thus, doubling the failure points.

²With Carol's mapper oracle and repeated application of her shift oracle U_C , she can also compute $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |\mathfrak{c}^{-i-\omega} f_A(j_{i+\omega})\rangle = \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_A\rangle$ without measurement and then simply measure the j -register.

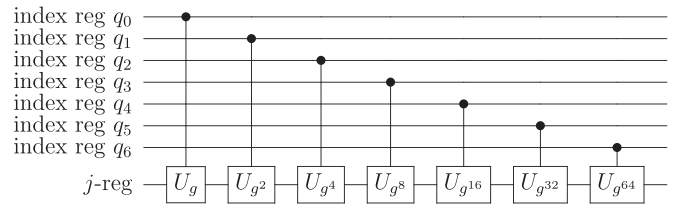


FIG. 2. Circuit for repeated squaring for the universal quantum oracle. This circuit applies g^s to the state in the j -register depending on the binary decomposition of s stored in the index register.

E. A universal quantum oracle

Define the global oracle

$$U : \text{Cl}(O_\Delta) \times J_\Delta \rightarrow J_\Delta$$

$$(g, j) \mapsto g * j,$$

and observe that is injective in each argument given the properties of the class group action, but of course it is not jointly injective.

Proposition 1. The global oracle $U(g, j)$ defined above can place an exponentially large isogeny cycle in superposition and requires only polynomially many quantum resources.

Proof. The ideal class group $\text{Cl}(O_\Delta)$ of an imaginary quadratic number field is isomorphic to the so-called *form class group* of primitive positive definite binary quadratic forms of discriminant Δ (see, e.g., Ref. [17], Theorem 5.30). The explicit isomorphism allows for a straightforward transition between the elements of the two groups. As a result, one can work in the form class group instead, which yields a very efficient arithmetic in the group, when considered as composition of forms. An algorithm of Schönage [15] shows that the time for reduction as well as composition of forms is

$$O(m(|\Delta|) \log |\Delta|) \sim O(\text{poly log } |\Delta|), \quad (7)$$

where $m(|\Delta|) \leq \log(|\Delta|)^2$ denotes the time for multiplication of two integers of size $\sim |\Delta|$.

As above, we assume that the class group G is cyclic of prime order r . Given any $g \in G$ and $1 \leq s \leq r$, we can perform exponentiation g^s by repeated squaring (see the circuit in Fig. 2) which, together with Eq. (7) above, yields the total time

$$O(\log s \text{ poly log } |D|) \sim O(\text{poly log } r). \quad (8)$$

Each user computes their random element, which is of the form g^e as in Eq. (2), and applies this global oracle accordingly. As the exponent e is of size $O(\log r)$, we need $O(\log r)$ -many controlled $U(g^{2^k}, -)$ gates, and the total time for this global oracle, given Eqs. (7) and (8), remains at $O(\text{poly log } r)$. ■

Remark 5. Like everywhere else in the paper, we do not analyze the run-time of the class-group action per se (or isogeny computation), as implementations are an active research area with steadily improving results. However, recent work suggests [16,17] that the class group action is efficiently implementable on a classical device. A naïve quantum implementation of the class group action can therefore be constructed, for example, by compiling the classical implementation into the Toffoli-only reversible gate set and

subsequently replacing all these bit and Toffoli gates with their quantum counterparts.

The controlled gates can then furthermore be constructed by controlling every individual Toffoli gate and compiling them into a Toffoli-only circuit. This only increases a constant factor gate-count overhead.

While this process guarantees an efficient compilation, more advanced compilation techniques would be required to make the implementation feasible. Finding such an implementation using quantum arithmetic is beyond the scope of this work.

Now, given such a global oracle, the restrictions on ω and Ω to be of polynomial size can be lifted, and arbitrary subintervals of the entire cycle corresponding to the chosen element g^e can be put in superposition, including the entire cycle itself. With the entire cycle in superposition, the protocol can be formed as shown in Procedure 4.

Remark 6. It should be noted that the oracle in Fig. 2 is used in two different ways. For any given g and secret exponent e , any actor can load e into the index register which turns the oracle into the shift oracle. For example, if Carol chooses e_C , then her shift oracle should act as $|j\rangle \mapsto |c * j\rangle = |g^{e_C} * j\rangle$ which executes with e_C loaded into the index register in Fig. 2. All actors need this application of Fig. 2. However, Carol also needs the mapper oracle to implement the powers of c which can be represented as in Fig. 2 but with $g = c$ and with i loaded into the index register. This executes the mapper operation $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_\omega\rangle \mapsto \frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_{i+\omega}\rangle$. Carol can implement this mapper oracle either by directly implementing the circuit of Fig. 2 with $g = c$ and loading i into the index register or by nesting Fig. 2 using one register to hold i , one register to hold e_C , and constructing the controlled $U_{g^{2^k e_C}}$ gates instead of the $U_{g^{2^k}}$ gates in Fig. 2. Instead of nesting, the latter can also be achieved using a quantum arithmetic circuit computing the products $2^k e_C$ and its output register is used as index register for Fig. 2.

V. IMPLEMENTATION WITH FIVE ACTORS

In this section we give a high-level overview of the quantum onion routing protocol involving five actors, A, B, C, D, and E, which is presented in full detail in Appendix. Here A wishes to send a message to E, with B, C, and D acting as intermediaries, similar to the classical TOR protocol. This example covers only the key-information component of the protocol, since the message component and classical communication overhead are not integral to the proposed method. The protocol flow is illustrated in Algorithm 1. In Algorithm 1, we also indicate the transmission control protocol (TCP) flags synchronize (SYN), synchronize-acknowledgment (SYN-ACK), and acknowledgment (ACK), highlighting that the proposed protocol fits within the standard TCP three-way handshake model.

For the explicit example presented in Appendix, we choose the ideal class group of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-167})$, which is of order 11. The corresponding set of j -invariants is

$$J = \{307, 248, 236, 223, 213, 209, 193, 182, 116, 12, 1\} \\ \subset \mathbb{F}_{311}.$$

Procedure 4. The entire isogeny cycle in superposition

(1) Carol prepares the state

$$|\psi_0\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |s\rangle \otimes |j_0\rangle.$$

(2) She applies her universal mapper oracle as shown in Fig. 2 with $g = c$,

$$|\psi_1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |s\rangle \otimes |c^s * j_0\rangle = \sum_s |s\rangle \otimes |j_s\rangle,$$

and sends out only the second register (j -register), retaining the first (index register)

$$|\psi_2\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |j_s\rangle.$$

(3) Bob applies the universal oracle $U(b, -)$ and sends the following state to Alice:

$$|\psi_3\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |b * j_s\rangle.$$

(4) Alice applies the universal oracle $U(a, -)$ and sends the following state back to Bob,

$$|\psi_4\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |ab * j_s\rangle.$$

(5) Bob applies the inverse oracle $U(b^{-1}, -)$ and sends to Carol the following state:

$$|\psi_5\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |a * j_s\rangle.$$

(6) Carol recombines the received j -register with the retained index register and applies her inverse universal mapper oracle and obtains

$$|\psi_{\text{final}}\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |s\rangle \otimes |a * j_0\rangle.$$

Any measurement will reveal Alice's key j_A .

This implies that there are five, $\frac{11-1}{2}$, nontrivial undirected cycles, as shown in Fig. 3, each representing a different secret choice made by each actor. All cycles are represented to start with the public j -invariant $j_0 = 1$. Explicit knowledge of these cycles is not required using the class group action implementation and these are presented here only for illustrative purposes.

The secret key that A needs to communicate to E is $j_A = f_A(j_0)$, i.e., the next j -invariant along A's cycle.

Upon obtaining the information that E is to receive a message via the quantum onion routing protocol, they choose ω and Ω which implies that $Q = \lceil \log_2 \Omega \rceil$ many qubits are required for the index register. Of course, $\omega = 0$ and $\Omega = r$ are valid choices here as well. Similarly, since the field is $\mathbb{F}_p$, E also requires $N = \lceil \log_2 p \rceil$ many qubits to represent the j -invariants.

ALGORITHM 1. Five-actor quantum onion routing.

public: characteristic p , j -invariant j_0

- 1 A wants to send message to E;
- 2 A sets up communication chain to E with intermediaries B,C,D with all neighbors (A,B), (B,C), (C,D), (D,E) executing a Diffie-Hellman key exchange: $j_{ab}, j_{bc}, j_{cd}, j_{de}$; // suppressed in Sec. V and Appendix
- 3 A informs actors in the chain of intention to send message via quantum onion routing protocol; // TCP-SYN
- 4 Each actor chooses a secret class group action shift: f_A, f_B, f_C, f_D, f_E ;
- 5 E chooses $0 \leq \omega < r$ and $1 \leq \Omega < r - \omega$;
- 6 E initializes a $Q = \lceil \log_2 \Omega \rceil$ -size index (qubit) register;
- 7 E initializes a $N = \lceil \log_2 p \rceil$ -size j -(qubit)-register;
- 8 E generates the state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_{i+\omega}\rangle$ with $j_{i+\omega} = f_E^{i+\omega} * j_0$;
- 9 E retains index register and sends j -register to D;
- 10 D acts with f_D on j -register;
- 11 D sends j -register to C;
- 12 C acts with f_C on j -register;
- 13 C sends j -register to B;
- 14 B acts with f_B on j -register;
- 15 B sends j -register to A; // TCP-SYN-ACK
- 16 A acts with f_A on j -register;
- 17 A computes $j_A = f_A(j_0)$;
- 18 A attaches message $C(j_{ab})C(j_A)|m\rangle$; // all message operations are suppressed in Sec. V and Appendix
- 19 A sends j -register to B;
- 20 B acts with f_B^{-1} on j -register and with $C(j_{bc})C(j_{ab})^*$ on message;
- 21 B sends j -register and message to C;
- 22 C acts with f_C^{-1} on j -register and with $C(j_{cd})C(j_{bc})^*$ on message;
- 23 C sends j -register and message to D;
- 24 D acts with f_D^{-1} on j -register and with $C(j_{de})C(j_{cd})^*$ on message;
- 25 D sends j -register and message to E; // TCP-ACK
- 26 E measures index and j -register: obtains pair $(i, \alpha * j_{i+\omega})$;
- 27 E acts with $f_E^{-i-\omega}$ on $f_A(j_{i+\omega})$, obtains j_A ;
- 28 E acts with $C(j_A)^*C(j_{de})^*$ on message to retrieve message;

All of this is executed by E upon being told that they are to receive a message via the quantum onion routing protocol. It should be noted that the ancilla register is only required for values of Ω that are not powers of 2.

E now prepares the state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_0\rangle$ suppressing any ancilla qubits. This is achievable with just Hadamard gates on all qubits if Ω is a power of 2. Otherwise, we can to add a single Grover derandomization step to remove any values of i between Ω and the next power of 2.

E completes the setup by applying the mapper oracle to prepare the state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_i\rangle$ as well as the class group action oracle f_E^ω for their chosen generator ϵ , producing the final state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_{i+\omega}\rangle$. E should retain the index register and send the j -register to D.

D now applies their shift producing the state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_D(j_{i+\omega})\rangle$ where the left register is retained by E and D has the j -register. D further sends the j -register up the chain eventually reaching A via C and B who all execute their respective class group action shift oracles.

After this first pass up the chain, the quantum state is $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_A(f_B(f_C(f_D(j_{i+\omega}))))\rangle$, where the index register is still retained by E and the j -register is held by A. A also attaches the encrypted message for the transmission through the forward pass back to E.

In the forward pass, A sends the registers back to E via B, C, and D who each use their inverse class group action shift oracles on the j -register as well as their respective scrambling operations for the Diffie-Hellman layer on the message. Commutativity of the group action implies commutativity of the class group action shift oracles; i.e., $f_{X^{-1}} \circ f_A \circ f_X = f_A \circ f_{X^{-1}} \circ f_X = f_A$ holds for $X \in \{B, C, D\}$, and E obtains the final quantum state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_A(j_{i+\omega})\rangle$.

Having received this final quantum state, E needs to reconstruct j_A . There are many ways this can be done. The simplest implementation is for E to measure the index and j -registers. This causes the state to project into a uniformly random selection $|i\rangle \otimes |f_A(j_{i+\omega})\rangle$. This uniform distribution is shown in Fig. 4 for the explicit example of Appendix.

E, now knowing i and ω , computes

$$\begin{aligned} |\epsilon^{-i-\omega} * f_A(j_{i+\omega})\rangle &= |f_E^{-i-\omega} \circ f_A \circ f_E^{i+\omega}(j_0)\rangle \\ &= |f_A(j_0)\rangle = |j_A\rangle. \end{aligned}$$

Thus, E has retrieved j_A and can decrypt the message.

Remark 7.

(1) Throughout this entire process, an attacker has only access to the j -register. Thus, measuring it yields exactly one of the states $|f_A(f_B(f_C(f_D(j_{i+\omega}))))\rangle$, $|f_A(f_C(f_D(j_{i+\omega})))\rangle$, $|f_A(f_D(j_{i+\omega}))\rangle$, or $|f_A(j_{i+\omega})\rangle$, depending on the point in the

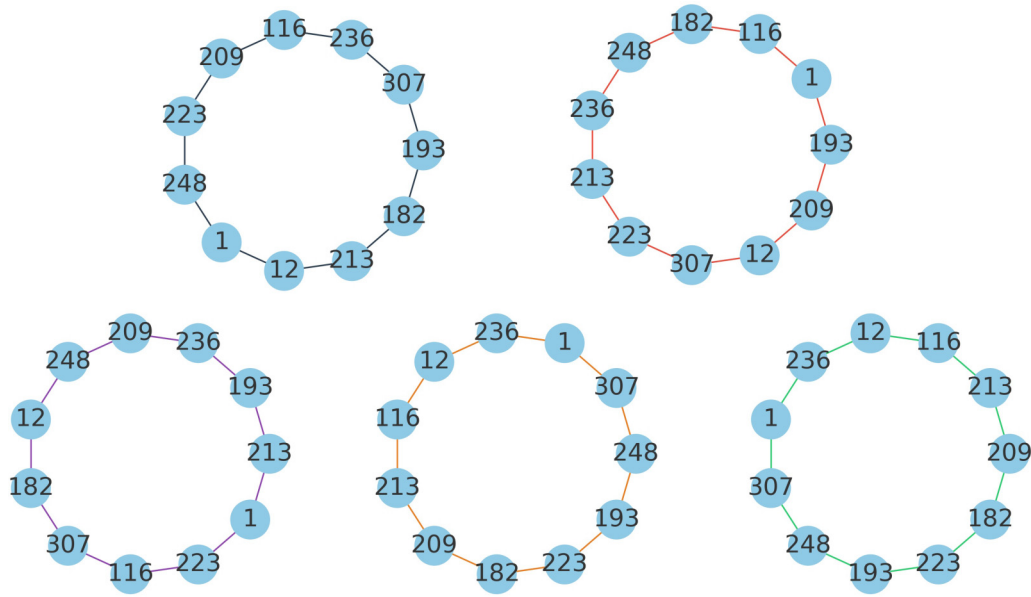


FIG. 3. The five isogeny cycles corresponding to elements of norms 3, 7, 11, 19, and 97, in the class group $\text{Cl}(O_{-167})$ of order 11. Each one connects the j -invariants in a different way.

chain they apply their attack, with i drawn uniformly. Thus, they will observe a random j -invariant drawn from a uniform distribution.

(2) If the malicious attacker makes copies via imperfect cloning at a single point in the communication chain, then they will receive a sample of j -invariants as implemented in

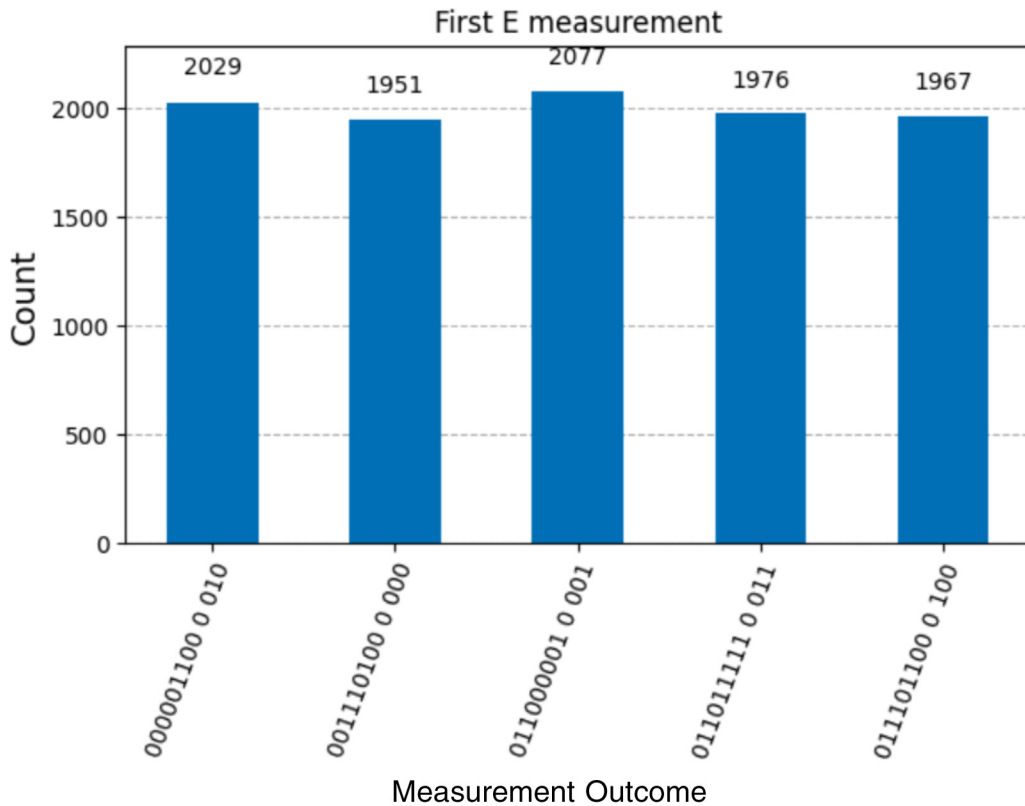


FIG. 4. Example histogram of measurements as seen by E in their first measurement process if the communication were repeated 10 000 times. The outcomes are drawn from a uniform distribution of all states $|i\rangle \otimes |f_A(j_{i+\omega})\rangle$. Here, the index register is the last set of three qubits, the j -register is the front set of nine qubits, and the single qubit in the middle is the ancilla required for the Grover step.

the cycle by E , possibly further shifted by generators from A , B , C , or D . While the attacker knows that these come from a Ω -large subsection of E 's cycle, the order is unknown. Furthermore, due to imperfect cloning errors, some of these measurements will yield nonimplemented states of the j -register, which may correspond to non- j -invariants or j -invariants that are not on the Ω -size subcycle E has put into superposition.

(3) If an attacker measures at multiple points in the chain, then the onion routing protocol has been compromised because the chain is supposed to be hidden. But even in that case, there are two options for the attacker.

(a) The attacker measures the state at each transmission. In that case, their attack is reduced to breaking the problem in the classical setting.

(b) The attacker makes imperfect copies at each transmission. Then, they receive sets of j -invariants that but they do not know how they relate, there will be $\Omega!$ many possible neighbors within the data. Furthermore, there will be errors in the data that need to be handled. For example, if the attacker measures between E and D as well as between D and C , then each imperfect copy may have a state infidelity of $1/6$. This means that with probability $5/6$ they measure a valid j -invariant from the implemented cycle, and with probability $1/6$ they end up in the erroneous contribution which comprises unknown contributions of invalid j -register states, j -invariants that do not correspond to the implemented cycle, and j -invariants that correspond to the implemented cycle. The attacker therefore needs to identify the false states and find the pairings $(j, f_D(j))$ of implemented j -invariants j with their shifts $f_D(j)$ as executed by D . There are $\Omega!$ many such pairing arrangements even if all false j -invariants have already been filtered out.

(4) Even in the case where the index register is not retained by E and the attacker intercepts at the last step, they obtain a random pair $(i, f_A(j_{i+\omega}))$ which cannot be used to compute $j_A = f_A(j_0)$ since ω is private information only E has.

The best case scenario an attacker can hope for is to observe the initial transmission from E to D and obtain the pair $(i, j_{i+\omega})$, as well as the final transmission from D to E where they obtain the pair $(i, f_A(j_{i+\omega}))$. Since the quantum state has collapsed to a classical state in the first observation, these will be the same value of i . Thus, a malicious attacker would need to find an element $m \in \text{Cl}(O_\Delta)$ such that $m * j_0 = j_{i+\omega}$, and use it to retrieve $j_A = m^{-1} * f_A(j_{i+\omega})$. Alternatively, the malicious attacker could intercept both upstream and downstream messages between any two actors attempt to find $m \in \text{Cl}(O_\Delta)$ such that $m * f_X(j_{i+\omega}) = f_A(f_X(j_{i+\omega}))$ for f_X being the identity, f_D , $f_C \circ f_D$, or $f_B \circ f_C \circ f_D$ depending on the point of the attack, and use it to retrieve $j_A = m^{-1} * f_A(f_X(j_{i+\omega}))$. Solving any of these problems is, of course, as hard as breaking the scheme itself, as this is the central hardness assumption for schemes based on the ideal class group action.

Furthermore, even if this problem is solved and the malicious attacker gains access to j_A , then they still need to break the Diffie-Hellman encryption layer, i.e., they need to successfully execute two more such attacks.

(5) The transmission of the index register should be avoided, because using imperfect copies, an attacker could now get the additional information which j -invariants corre-

spond to each other at different transmission points. This, of course, requires the chain of communication to be known, i.e., for the onion routing communication to already be partially compromised, but knowing the chain of communication now can lead to additional information that is not known in the classical case and might compromise security.

(6) If the index register needs to be contained in the transmission (e.g., for engineering reasons such as not being able to maintain entanglement if the index register is retained by E), then one should consider further encryption on the index- and j -registers.

(a) Adding a Diffie-Hellman encryption layer on the index- and j -registers prevents any external attacker from obtaining any information. However, an attacker measuring the state during transmission also destroys the state and E will only receive garbled nonsense. While this keeps the communication secure, this should be avoided as it opens up the possibility of an attacker preventing any communication reaching the receiver, unless the Diffie-Hellman layer is implemented in such a way that each classical index- j -combined register state is mapped to another classical index- j -combined register state. Furthermore, while this prevents any external attacker from executing the above-mentioned attack, each intermediary (B , C , or D) is still able to perform the attack; hence, must be trusted.

(b) E may add an encryption on the index register alone. Since nobody but E needs to access the index register, this does not impede other actors from executing their protocols. Again, an attacker measuring the index register will cause the communication to fail unless E 's secret encryption maps classical states of the index register into classical states. In other words, the encryption must be chosen as a secret permutation of the numbers $0, \dots, n-1$ with $\Omega \leq n \leq 2^{\lceil \log_2 \Omega \rceil}$.

VI. SECURITY CONSIDERATIONS AND FINAL REMARKS

For security reasons, we require the class number $h(\Delta)$ to be exponential in the security parameter. Since $h(\Delta)$ “grows like” $\sqrt{|\Delta|}$ [[18], p. 19], Δ , and hence the choice of p , should be set accordingly. Regarding the security of the class group action, there is ongoing work on appropriate parameter sets; the most up-to-date analysis is given by Campos *et al.* [19], which incorporates the best-known quantum attacks based on Kuperberg’s hidden-shift algorithm running in subexponential time $2^{O(\sqrt{\log h(\Delta)})}$. As implementation techniques for evaluating the action continue to improve (e.g., Refs. [16,17]), recommended parameters may be revised; a full treatment lies beyond the scope of this paper. It is worth mentioning, however, that a common solution is increasing the security parameter according to the explicit implemented scheme. The protocol we have described in this paper is semiclassical in the sense that it reduces to the classical vectorization problem under certain attack conditions. Thus, the classical security is an achievable lower bound on the security of the here presented protocol. Improving security beyond this lower bound may be achievable with CTQW implementations which are part of further current work.

Along the same lines, it is worth noting a distinction between a semiclassical setting such as ours and the classical

group-action protocols (as used in postquantum cryptography but analyzed against quantum adversaries). Classically, a public transcript may reveal a start point j_0 and an end point j_k , and the core hardness assumption is the vectorization problem: Find $a \in G$ such that $a * j_0 = j_k$, for which the best known quantum algorithms are subexponential at best. In a quantum construction such as the QOR however, no intermediate j -invariants are accessible unless a measurement is performed (which yields a random j -invariant); only the public j_0 is visible. An attacker must perform multiple measurements, i.e., must successfully execute multiple attacks, to obtain such a vectorization instance.

Our second remark on security addresses the properties of *uniform mixing* and *periodicity* of the underlying isogeny graph. The property of uniform mixing is desirable since a sufficiently long walk on the isogeny graph becomes indistinguishable from a random walk. In particular, *supersingular* ℓ -isogeny graphs are *Ramanujan*. Their nontrivial eigenvalues are bounded by $2\sqrt{\ell}$, so the classical walk mixes in $O(\log |V|)$ steps, $|V|$ being the number of vertices (see, e.g., Ref. [20]). For *ordinary* isogeny graphs Jao-Miller-Venkatesan (under GRH) prove in Ref. [[8], Cor. 1.3] that a walk of length

$$t \geq C \frac{\log |V|}{\log q}$$

is already near-uniform from any start. Here C is a positive constant and, in the elliptic curve scenario in Ref. [[8], Theorem 1.5], $|V| \sim \sqrt{q}$.

In the quantum setting on the other hand, uniform mixing is known only for a narrow family of graphs, so one can instead work with the relaxed notion of ε -uniform mixing. It is known that for every $p \geq 5$, every p -cycle C_p exhibits ε -uniform mixing [3], Theorem 5.5.2]. Consequently, for appropriately chosen walk lengths (or evolution times), the walkers' paths appear ε -random to any observer. Moreover, combining Ref. [[21], Theorem 2.2 and Corollary 2.3] and Ref. [[3], Theorem 4.3.2], one obtains the known result that no n -cycle C_n is periodic unless $n \in \{1, 2, 3, 4, 6\}$. Finally, Ref. [[22], Lemma 3] ensures that other than the complete graph K_p , no other circulant graph $G(p; S)$ on p -many vertices and generating set S of cardinality $|S| < p - 1$ is periodic. It therefore appears that p -cycles are good candidates for quantum cryptographic scenarios as the one considered in this paper. In the extremal case where the class group is cyclic of large prime order, the resulting isogeny graph, after d -many encryptions, is the disjoint union of d -many p -cycles C_p . Even when the class group is not of prime order, one can restrict to a large-enough prime-order subgroup and the corresponding isogeny cycles to obtain the same effect.

Our final remark turns to implementation considerations. These primarily concern the quantum oracles. If we are in the CSIDH/CSURF setting discussed in Sec. II, i.e., we work with supersingular elliptic curves over $\mathbb{F}_p$, then efficient classical computation of the action $*$ by arbitrary class group elements is becoming increasingly feasible, owing to advances such as PEGASIS [16,17]. This remains an active research area, and we do not pursue further details here as this is not in the scope of the paper. Alternatively, as already discussed in the paper, the class group action can be interpreted as continuous-time

quantum walk on the underlying isogeny graph, hence on the underlying Hamiltonian. Currently, in a parallel project, we are developing this viewpoint theoretically, and we are considering possible implementations on actual hardware.

ACKNOWLEDGMENTS

This work is supported by the European Union's Horizon Europe Framework Programme (HORIZON) under the ERA Chair scheme "QUEST" with Grant Agreement No. 101087126. This work is also supported with funds from the Ministry of Science, Research and Culture of the State of Brandenburg within the Centre for Quantum Technologies and Applications (CQTA).

DATA AVAILABILITY

No data were created or analyzed in this study.

APPENDIX: DETAILED IMPLEMENTATION OF EXAMPLE WITH FIVE ACTORS

In this Appendix we present the fully worked, minimal Qiskit example with five actors A, B, C, D, and E that we outlined in Sec. V. Here, A wants to send a message to E with B, C, and D acting as intermediaries similar to the classical TOR protocol. For simplicity, we will only cover the key information part of the protocol as the message part is equivalent to classical Diffie-Hellman exchanges and applying simple circuitry for scrambling. We also remove the classical communication overheads of setting up communications channels between actors.

For simplicity, we will implement the class group action oracles by classically precomputing the corresponding cycles and implementing the corresponding shift operators. The direct implementation of these oracle gates is beyond the scope of this implementation as we want to focus on the communication part of the protocol.

For this example, we choose the ideal class group of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-167})$, which is of order 11. The corresponding Hilbert class polynomial has very large coefficients but it splits completely into eleven linear factors over the finite field $\mathbb{F}_{311}$. The set of j -invariants containing its roots is

$$J = \{307, 248, 236, 223, 213, 209, 193, 182, 116, 12, 1\} \\ \subset \mathbb{F}_{311}.$$

This example has five, $\frac{11-1}{2}$, nontrivial undirected cycles, as shown in Fig. 3, and we attribute a different one as the secret choice made by each actor. The publicly known j_0 is chosen as 1. These computations were performed in PARI/GP [23] and SageMath [24].

For this implementation, we will use Qiskit and load the following libraries. The final library loading `basic_comparator` is not publicly available at the time of writing this paper. It supplies the comparator $i < \Omega$ which is required for the oracle in an optional Grover step to filter for only the indices $i < \Omega$. If Ω is chosen as a power

of 2, then this `basic_comparator` is not required. Its general implementation has been also used previously, cf. e.g., in Ref. [25].

We may then define the five cycles and give one to each actor. All cycles are represented to start with the public j -invariant $j_0 = 1$. In an actual implementation using oracles implementing the class group action, explicit knowledge of these cycles is not required. This means that the secret key that A needs to communicate to E is $j_A = f_A(j_0)$ or $\text{aj}[1]=213$.

We choose $\omega = 2$ and $\Omega = 5$ which implies that we require $Q = \lceil \log_2 \Omega \rceil = 3$ many qubits for the index register. Similarly, since the field is F_{311} , we require $N = \lceil \log_2 311 \rceil = 9$ many qubits to represent the j -invariants. Using the cycles defined above, we can define the oracles that shift one element to the right and act as the identity on non- j -invariants for all actors and their inverses (the left shifts) for all but A (A's inverse is not required).

We also need to implement the mapper oracle for E. However, the relatively large value of N and the fact that we do not have “real” circuitry for the oracles `UE` and `UEinv`, render the construction of the mapper—as described in Figs. 1 or 2—computationally heavy. Instead, we will implement a mapper $|i\rangle \mapsto |j_i\rangle$ according to E's cycle. Thus, rather than loading $|j_0\rangle$ into the j -register and entangling it with the index register via the mapper, we will create entanglement by producing the state $|i\rangle \otimes |i\rangle$ and then using the “fake” mapper implementation to obtain $|i\rangle \otimes |j_i\rangle$. This “fake” mapper necessarily has superpolynomial complexity as otherwise it could be used to break the cryptosystem.

All of this is executed by E upon being told that they are to receive a message via the quantum onion routing protocol. It should be noted that the ancilla register is only required for values of Ω that are not powers of 2.

At this point, the current quantum state (ignoring the ancilla qubit) is $\frac{1}{\sqrt{8}} \sum_{i=0}^7 |i\rangle \otimes |0\rangle$. In other words, we have an equal superposition of all computational basis states in the index register, and the $|0\rangle$ state in the j -invariants register. We now add the optional Grover step to filter for only the states $i < \Omega = 5$.

With this Grover step, the current quantum state is now $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |0\rangle$ (ignoring the ancilla qubit). As the ancilla is no longer required for any calculations, we will forget about its existence going forward.

Next, E needs to prepare the corresponding $|j_i\rangle$ for each $|i\rangle$ in the j -invariants register. This is done in two steps. First copy $|i\rangle$ into the j -register and then apply the “fake” mapper oracle $|i\rangle \mapsto |j_i\rangle$ to the j -invariants register. Using the correct mapper as described in Figs. 1 or 2, we would need to load

$|j_0\rangle$ into the j -register and apply the correct mapper to both index- and j -register to create $|i\rangle \mapsto |j_i\rangle$.

E also applies the shift with respect to ω to produce $|i\rangle \mapsto |j_{i+\omega}\rangle$.

Thus, E has now created the state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |j_{i+\omega}\rangle$. E should retain the index register and send the j -register to D who applies their shift. This creates the state $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_D(j_{i+\omega})\rangle$ where the left register is retained by E and D has the j -register. D further sends the j -register up the chain eventually reaching A via C and B who all execute their respective shift oracles. At this point, the current quantum state is $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_A(f_B(f_C(f_D(j_{i+\omega}))))\rangle$, where the index register is retained by E and the j -register is held by A. A also attaches the encrypted message at this point, but we will ignore that for simplicity.

A now sends the registers back to E via B, C, and D who each use their inverse oracles on the j -register as well as their respective scrambling operations for the Diffie-Hellman layer on the message. Since the group action is commutative, the oracles commute; i.e., $f_{X^{-1}} \circ f_A \circ f_X = f_A \circ f_{X^{-1}} \circ f_X = f_A$ hold for $X \in \{B, C, D\}$, and we obtain that the final quantum state sent from D to E is $\frac{1}{\sqrt{\Omega}} \sum_{i=0}^{\Omega-1} |i\rangle \otimes |f_A(j_{i+\omega})\rangle$.

Upon receipt of this final transmission, all further operations are performed by E. First, E measures the state.

This collapses the state into a single $|i\rangle \otimes |f_A(j_{i+\omega})\rangle$ which is uniformly selected from all r possible values. As shown in Fig. 4, repeating the experiment 10 000 times yields each state $|i\rangle \otimes |f_A(j_{i+\omega})\rangle$ roughly $\frac{10000}{\Omega} \approx 2000$ times.

In reality, E will measure only once and obtain, for example, the measurement outcome `key_raw = ‘‘011101100 0 100’’`, which corresponds to $i = 4$ and $f_A(j_{i+\omega}) = 236$. E now needs to uncompute their shift. They can do this by applying their inverse oracle `UEinv` $i + \omega$ times or by applying the “true” inverse mapper oracle once and the inverse oracle `UEinv` ω times. Since we do not have the “true” mapper implemented, we will use `UEinv` $i + \omega$ times. E immediately measures the j -register afterwards again.

Letting E's cycle generator be denoted as ϵ and A's as α , this last operation executes

$$|\epsilon^{-i-\omega} * f_A(j_{i+\omega})\rangle = |\epsilon^{-i-\omega} * \alpha * \epsilon^{i+\omega} * j_0\rangle = |\alpha * j_0\rangle = |j_A\rangle.$$

Thus, the final measurement lets E read out j_A .

In the example where `key_raw = ‘‘011101100 0 100’’`, E measures ‘‘011010101’’ in the j -register which is binary for $j_A = \alpha * j_0 = 213$ as it should be since `aj[1]=213`. Hence, we have successfully communicated the secret key from A to E via B, C, and D.

- [1] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, CSIDH: An efficient post-quantum commutative group action, in *Advances in Cryptology—ASIACRYPT*, Lecture Notes in Computer Science (Springer, Berlin, 2018), pp. 395–427.
- [2] A. M. Childs, *Quantum information processing in continuous time*, Ph.D. thesis, Massachusetts Institute of Technology, 2004.

- [3] N. E. Mullin, *Uniform mixing of quantum walks and association schemes*, Ph.D. thesis, University of Waterloo, 2013.
- [4] S. Lang, *Elliptic Functions* (Springer, Berlin, 1987).
- [5] M. Deuring, Die Typen der Multiplikatorringe elliptischer Funktionenkörper, *Abh. Math. Semin. Univ. Hambg.* **14**, 197 (1941).
- [6] W. Castryck and T. Decru, CSIDH on the surface, in *Post-Quantum Cryptography—11th International Conference—*

- PQCrypto*, edited by J. Ding and J.-P. Tillich (Springer, Cham, 2020), pp. 111–129.
- [7] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication* (Wiley, New York, 1989).
 - [8] D. Jao, S. D. Miller, and R. Venkatesan, Expander graphs based on GRH with an application to elliptic curve cryptography, *J. Number Theory* **129**, 1491 (2009).
 - [9] N. Biggs, *Algebraic Graph Theory*, 2nd ed. (Cambridge University Press, New York, 1992).
 - [10] C. Godsil and G. Royle, *Algebraic Graph Theory* (Chapman & Hall, New York, 1993).
 - [11] S. Hallgren, Fast quantum algorithms for computing the unit group and class group of a number field, in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2005), pp. 468–474.
 - [12] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields, in *Noordwijkerhout*, Lecture Notes in Mathematics Vol. 1068 (Springer, Berlin, 1984), pp. 33–62.
 - [13] A. M. Childs, D. Jao, and V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, *J. Math. Cryptol.* **8**, 1 (2014).
 - [14] C. Godsil, Algebraic combinatorics, *Chapman & Hall Mathematics Series* (Chapman & Hall, New York, 1993).
 - [15] A. Schönhage, Fast reduction and composition of binary quadratic forms, in *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC'91* (ACM, New York, 1991), pp. 128–133.
 - [16] P. Dartois, J. K. Eriksen, T. B. Fouotsa, A. H. Le Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren, and B. Wesolowski, PEGASIS: Practical effective class group action using 4-dimensional isogenies, in *Advances in Cryptology—CRYPTO (2025)*, Lecture Notes in Computer Science (Springer, Berlin, 2025), pp. 67–98.
 - [17] P. Dartois, J. K. Eriksen, R. Invernizzi, and F. Vercauteren, qt-Pegasis: Simpler and faster effective class group actions, *J. Instrum.* **20**, P09012 (2025).
 - [18] A. Bhand and M. R. Murty, Class numbers of quadratic fields, *Hardy-Ramanujan J.* **42**, 17 (2019).
 - [19] F. Campos, J. Chávez-Saab, J.-J. Chi-Domínguez, M. Meyer, K. Reijnders, F. Rodríguez-Henríquez, P. Schwabe, and T. Wiggers, Optimizations and practicality of high-security CSIDH, in *Advances in Cryptology—CRYPTO 2024*, Lecture Notes in Computer Science (Springer, Berlin, 2024).
 - [20] D. X. Charles, K. E. Goren, and K. E. Lauter, Cryptographic hash functions from expander graphs, *J. Cryptol.* **22**, 93 (2009).
 - [21] C. Godsil, Periodic graphs, *Electron. J. Combin.* **18**, P23 (2011).
 - [22] N. Saxena, S. Severini, and I. E. Shparlinski, Parameters of integral circulant graphs and periodic quantum dynamics, *Int. J. Quantum Inf.* **05**, 417 (2007).
 - [23] The PARI Group, PARI/GP version 2.15.5, Univ. Bordeaux, 2024, <https://pari.math.u-bordeaux.fr/>.
 - [24] The Sage Developers, SageMath, the Sage Mathematics Software System (Version 10.4), 2024, <https://www.sagemath.org/>.
 - [25] R. Babbush, C. Gidney, D. W. Berry, N. Wiebe, J. McClean, A. Paler, A. Fowler, and H. Neven, Encoding electronic spectra in quantum circuits with linear T complexity, *Phys. Rev. X* **8**, 041015 (2018).