

Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits

Élie Gouzien ^{1,*}, Diego Ruiz ^{2,3}, Francois-Marie Le Régent ^{2,3}, Jérémie Guillaud ² and Nicolas Sangouard ^{1,†}

¹ *Université Paris-Saclay, CNRS, CEA, Institut de physique théorique, 91 191, Gif-sur-Yvette, France*

² *Alice&Bob, 53 boulevard du Général Martial Valin, 75 015 Paris*

³ *Laboratoire de Physique de l'École normale supérieure,
École normale supérieure, Mines Paris, Université PSL,
Sorbonne Université, CNRS, Inria, 75 005 Paris*

(Dated: February 15, 2023)

Cat qubits provide appealing building blocks for quantum computing. They exhibit a tunable noise bias yielding an exponential suppression of bit-flips with the average photon number and a protection against the remaining phase errors can be ensured by a simple repetition code. We here quantify the cost of a repetition code and provide a valuable guidance for the choice of a large scale architecture using cat qubits by realizing a performance analysis based on the computation of discrete logarithms on an elliptic curve with Shor's algorithm. By focusing on a 2D grid of cat qubits with neighboring connectivity, we propose to implement two-qubit gates via lattice surgery and Toffoli gates with off-line fault-tolerant preparation of magic states through projective measurements and subsequent gate teleportations. All-to-all connectivity between logical qubits is ensured by routing qubits. Assuming a ratio between single-photon and two-photon losses of 10^{-5} and a cycle time of 500 nanoseconds, we show concretely that such an architecture can compute 256-bit elliptic curve logarithm in 9 hours with 126 133 cat qubits. We give the details of the realization of Shor's algorithm so that the proposed performance analysis can be easily reused to guide the choice of architecture for others platforms.

Introduction — While quantum computing can offer substantial speedups for solving specific problems [1], billions of operations are typically required for implementing large scale algorithms [2–4]. This means that the convergence of quantum algorithms can not realistically be ensured by requiring physical errors to occur with a probability smaller than the inverse of the number of required operations. Instead, the concept of fault-tolerant quantum computation [5] is envisioned. It relies on the idea that if the rate of physical errors is below a certain threshold, quantum error correction schemes suppress the logical error rate to arbitrary low levels and make possible – at least in principle – arbitrary long sequences of operations [6–8].

With its relatively high thresholds, the surface code is one of the most popular quantum error correction codes [9, 10]. As a 2D code, the number of physical qubits per logical qubits increases quadratically with the code distance. Their actual implementation hence comes at the price of a significant overhead in physical resources, with typically hundreds or even thousands of physical qubits per logical qubits to achieve the level of protection required for performing billions of noise-free operations [5].

Some physical platforms naturally exhibit a noise bias [11] which can be exploited to increase code thresholds and hence to reduce the overhead [12, 13]. Bosonic systems stabilized in a two-dimensional manifold spanned by cat states – superpositions of coherent states with opposite phases – with engineered dissipation scheme combining two-photon drive and two-photon dissipation

stand out in this framework. The noise bias is indeed tunable in this case, with bit-flips that are suppressed exponentially with the mean photon number [14–16]. The remaining phase errors can be corrected with a simple repetition code – a 1D code with a number of physical qubits per logical qubit increasing linearly with the code distance. Given that gate sets at the physical level preserving the noise asymmetry have been described and their use for the implementation of various universal sets at the logical level has been identified [17], cat qubits are becoming an option for realizing a large scale quantum computer. The gain of having a 1D over a 2D code and the details of the implementation of a large scale algorithm with cat qubits are however missing.

We here propose a generic tool for analysing the performance of quantum computing architectures using Shor's algorithm [18, 19] for computing discrete logarithms on elliptic curves over prime fields – a hard classical problem at the core of crypto-systems widely used for key exchange and digital signatures [20, 21]. The security level of these crypto-systems against classical attacks relies on precise knowledges of the performance of classical algorithms – knowledges that are useful to witness a quantum advantage. Best currently known classical algorithms to compute elliptic curve discrete logarithms are exponential in the size of the input parameters whereas there exist subexponential algorithms for factoring. This facilitates the achievements of a quantum advantage with respect to algorithms with sub-exponential speedups, including Shor's algorithm for the factorization.

We propose a concrete architecture in which cat qubits

are placed at the nodes of a 2D grid with physical connections to their neighboring qubits only. All-to-all connectivity between logical qubits is ensured by means of routing qubits. Two-qubit gates are implemented by means of lattice surgery and Toffoli gates are obtained by gate teleportation through an offline fault-tolerant magic state preparation based on projective measurements. From detailed models of physical qubits and their manipulations, we estimate precisely the errors related to the implementation of logical operations by considering a ratio between single-photon and two-photon losses of 10^{-5} . We show concretely that such an architecture can compute a discrete logarithm on **secp256k1** curve which is used for securing signatures in Bitcoin transactions [22] in 9 hours with 126 133 cat qubits.

Elliptic curve and discrete logarithm — An elliptic curve is defined as the set of points associated to the coordinates (x, y) satisfying the equation $y^2 = x^3 + ax + b$ with fixed values for a and b . We are interested in cryptographic relevant elliptic curves for which x , y , a and b belong to the field of integers modulo p , with p a prime number (n bits long). We define a binary operation on these elliptic curves, called “addition” and denoted “+”: for two points P and Q , $R = P + Q$ have, in the generic case [23], coordinates given by

$$x_R = \lambda^2 - x_P - x_Q \quad (1a)$$

$$y_R = -y_P - \lambda(x_R - x_P) \quad (1b)$$

where $\lambda = (y_Q - y_P)/(x_Q - x_P)$ is the slope of the line joining P and Q . A multiplication by an integer k naturally arises as $kP = \underbrace{P + P + \dots + P}_{k \text{ times}}$. A cyclic subgroup

can be formed from the multiples of a point G (the subgroup generator) on the curve. The security of cryptographic algorithms based on elliptic curves, such as the Elliptic Curve Digital Signature Algorithm [21] relies on the hardness to find a number k (the logarithm) from the knowledge of the generator G and the point $P = kG$, see App. A for details on elliptic curve cryptography.

Shor’s algorithm — Shor introduced an algorithm [18, 24] to compute discrete logarithm on a quantum computer with a number of gates cubic in n . It takes three steps and three registers. In the first step, two registers encoding x_1 and x_2 are each prepared in a superposition of all possible integers. In the second step, $f(x_1, x_2) = x_1G - x_2P$ is computed and stored in the third register. In the last step, a quantum Fourier transform of the two registers containing x_1 and x_2 (which corresponds to a 2D quantum Fourier transform) reveals the value of k , see App. B for more details and a discussion on Ekerå’s version of Shor’s algorithm [25].

The preparation of registers in a superposition of all integers has a linear cost. It is indeed obtained through

the preparation of qubits in state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, that is by applying a Hadamard transformation on each qubit. Since the quantum Fourier transform precedes a measurement of each qubit, it can be implemented in a semi-classical way [26], with a linear cost as well. The cost of Shor’s algorithm is largely dominated by the computation of f , which we evaluate in detail below.

Arithmetic circuits — f is the difference between the results of two scalar multiplications. The elliptic curve scalar multiplication is implemented with a windowed approach, as in [27]. The principle is to decompose the factor k into groups of bits and to rewrite the multiplication as a sequence of elliptic curve point additions

$$kG = \sum_{\substack{i=0 \\ i \equiv 0 \pmod{w_e}}}^{n_e} 2^i k_{i:i+w_e} G \quad (2)$$

with n_e the number of bits in k , w_e the width of each window and $k_{i:i+w_e}$ the number formed from w_e bits of k starting at bit i . For each term, the point $2^i k_{i:i+w_e} G$ is computed classically for all possible values of $k_{i:i+w_e}$, and loaded into a quantum register through a quantum table lookup circuit [28, 29], with the qubits encoding $k_{i:i+w_e}$ as controls.

Each point addition is realized from Eq. (1) using a quantum implementation of each operation [30]. This takes arithmetic additions, subtractions, multiplications and divisions, modulo the prime number p , see App. C 7 and App. C 8 for details.

A ripple-carry circuit from [31] is used to perform the additions. The basic idea is to start with the low-order bits of the inputs, compute the first carry with a Toffoli gate, take the value of the carry and the next bits of the inputs to compute the second carry and so on up to the high-order bits. We then work from the high-order bits back down to the low-order bits by computing the result of the addition bit by bit, store the value in the first input register and restore the value of the second input register to get a reversible computation. Note that the subtraction is obtained by conjugation of the addition. To make an addition modulo p , the standard addition is followed by a comparison of the result with p , which is obtained by subtracting p from the result of the addition and by checking the most significant bit of the result of this subtraction. A subtraction of p is then realized, conditioned on the result of the comparison. In order to save resources, the comparison and subtraction which start identically, are merged together to form a modular reduction, see the App. C 2 for the details on the circuits. Note that the modular subtraction is obtained by conjugation of the modular addition.

The multiplication can be implemented with a standard double-and-add method which can be illustrated by

considering the product of two (n bits) numbers x_1 and x_2 . From the binary representation of $x_1 = \sum_i 2^i [x_1]_i$, we have $x_1 x_2 = \sum_i 2^i [x_1]_i x_2 = [x_1]_0 x_2 + 2([x_1]_1 x_2 + 2([x_1]_2 x_2 + \dots))$, *i.e.* the result of the product is obtained by first considering the last term (x_2 conditioned on the value of $[x_1]_{n-1}$), doubling the result and adding x_2 conditioned on $[x_1]_{n-2}$ and so on up to the first term. The multiplication modulo p is then naturally obtained by performing additions and doublings modulo p , which takes $2n$ modular reductions. We used a representation (compatible with the addition), the Montgomery representation, to reduce the number of reductions [27, 32]. It simply consists in representing a number x_1 by $y_1 = x_1 2^n \bmod p$. Considering the numbers x_1 and x_2 , and their respective Montgomery representation y_1, y_2 , the product $x_1 x_2$ is represented by $x_1 x_2 2^n \bmod p$, which is obtained by computing $y_1, y_2 \mapsto y_1 y_2 2^{-n} \bmod p$ from a double-and-add multiplier in which the doubling operation is replaced by halving. In this case, the sums need a single modular reduction to realize a multiplication modulo p , hence reducing the number of modular reductions to $n + 1$ [33]. Note that the latter is further reduced by using a windowed version of the multiplication in the Montgomery representation, see App. C 4 for the details of the multiplication circuit.

The modular division between two numbers x_1 and x_2 is obtained by a modular multiplication of x_1 and the modular inverse of x_2 . The modular inversion is performed with Kalisky's algorithm [34]. This algorithm is essentially a binary version of the extended Euclidean algorithm. To make it compatible with the Montgomery representation, the result is multiplied by 2^{2n} such that starting from the representation $y_2 = x_2 2^n \bmod p$, Kalisky's algorithm returns $x_2^{-1} 2^n \bmod p = y_2^{-1} 2^{2n} \bmod p$. The circuit we use is inspired from [27], with improvements, most notably by using sub-circuits crafted for use of Toffoli gates, see App. C 5.

Given the number of point additions in the scalar multiplication at the core of the discrete logarithm computation, the decomposition of a point addition in elementary arithmetic operations and the number of gates which is required for implementing each of these elementary operations, we deduce that the implementation of Shor's algorithm takes $448n^3/w_e$ CNOT and $348n^3/w_e$ Toffoli gates at the leading order, with w_e the size of each window for the elliptic curve multiplication, see App. C 10.

Cat qubits with repetition code — We are interested in cat qubits, in which information is encoded in two coherent states of a harmonic oscillator with the same amplitude and opposite phase $|\alpha\rangle$ and $|- \alpha\rangle$ [14, 35]. Here α is assumed real, without loss of generality. To avoid that the state of the oscillator leaves the computation subspace $(|\alpha\rangle, |- \alpha\rangle)$ in the presence of loss and noise, a

stabilization mechanism is needed. We consider a mechanism combining a two-photon drive and an engineered two-photon dissipation which can be implemented appropriately in a physical realization using cavity modes coupled non-linearly by Josephson junctions. When the corresponding stabilization rate is higher than that of typical errors, the bit-flip error rate induced by single photon loss, thermal excitations or dephasing is exponentially suppressed with the mean number of photons in the cat size $\gamma_X \propto \exp(-2\alpha^2)$, while the phase-flip error rate typically scales linearly $\gamma_Z \propto \alpha^2$ [36, 37]. In this work, the amplitude α is a free parameter. Its value is chosen such that bit-flips happen with a low probability during the runtime of Shor's algorithm and a repetition code corrects phase-flip errors only [17, 38]. Details on cat qubits and their implementation are given in App. D.

As bit-flips are not corrected, it is crucial not to introduce such errors during the algorithm execution. At the physical level, this is obtained by using bias-preserving operations including the preparations $\mathcal{P}_{|0/1\rangle}$ and $\mathcal{P}_{|\pm\rangle}$ of the computational states $|\pm\alpha\rangle$ and cat states $|\mathcal{C}_\alpha^\pm\rangle = \frac{1}{\sqrt{2(1 \pm e^{-2\alpha^2})}}(|\alpha\rangle \pm |- \alpha\rangle)$ respectively, the measurements \mathcal{M}_Z and \mathcal{M}_X , the Z and X gates, CNOT and Toffoli gates, see the details in App. D.

The principle of a distance- d repetition code is to introduce redundancy in the information encoding $|\pm\rangle_L := |\pm\rangle^{\otimes d}$ and make use of $d - 1$ stabilizer measurements $S_i = X_i X_{i+1}$ to identify and correct phase flip errors after each operation. In our case, $|\pm\rangle^{\otimes d} = |\mathcal{C}_\alpha^\pm\rangle^{\otimes d}$ and S_i is measured from the bias-preserving operations $\mathcal{P}_{|+\rangle}$, CNOT, \mathcal{M}_X .

We consider the logical operations in the set $\mathcal{S}_L = \{\mathcal{P}_{|+\rangle}_L, \mathcal{P}_{|0\rangle}_L, \mathcal{M}_{Z_L}, \mathcal{M}_{X_L}, Z_L, X_L, CX^k_L, CCX_L\}$, which can all be implemented transversally on the repetition code, except for the CCX_L gate, see App. E. The transversal implementation of the CNOT $_L$ gate, however, requires all-to-all couplings between the physical qubits of the processor, which is not a realistic feature of a superconducting quantum processor. Instead, we focus on a realization based on lattice surgery using nearest-neighbour interactions only (with additional routing qubits included in the resource evaluation), as detailed in App. E. The same idea can be extended to the multiple target CX^k_L gate which applies a X gate on k qubits if the control qubit is in state $|1\rangle_L$ and the identity otherwise, see also App. E. Finally, the logical Toffoli gate CCX_L is implemented using gate teleportation [39] from a ‘‘Toffoli magic state’’ $|\mathcal{CCX}\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$, as detailed in App. E 4 (with the circuit depicted in Fig. 32). The fault-tolerant preparation of Toffoli magic state at the logical level, based on a projective measurement, is discussed in App. E 4.

Noise model — We exclusively consider the single photon loss at rate κ_1 , as in presence of two-photon dissipation, the other error mechanisms have little impact on the noise model [17]. Our resource estimates is based on the assumptions that a two-photon dissipation rate of $\kappa_2/2\pi = 1.59\text{ MHz}$ and a resonator lifetime of $T_1 = 10\text{ ms}$ can be achieved, which corresponds to a ratio $\kappa_1/\kappa_2 = 10^{-5}$ and a repetition code cycle time of $T_{\text{cycle}} = 5/\kappa_2 = 500\text{ ns}$.

For a fixed gate time of $1/\kappa_2$ (assumed to be identical for state preparation, measurement, and CNOT gates), the logical error rate per cycle of a distance d repetition code is given by [40] (see App. E 2 for details),

$$\epsilon_L = 5.6 \times 10^{-2} \left(\frac{(\alpha^2)^{0.86} \kappa_1/\kappa_2}{(\kappa_1/\kappa_2)_{\text{th}}} \right)^{\frac{d+1}{2}} + 2(d-1) \times 0.50 e^{-2\alpha^2} \quad (3)$$

where the first term is the logical phase-flip error rate and the second term is the logical bit-flip error rate, and $(\kappa_1/\kappa_2)_{\text{th}} = 1.3 \times 10^{-2}$.

ϵ_L corresponds to the error rate of all gates (including the identity gate), but the Toffoli gate. For the latter, we consider two variations of the state preparations of Toffoli magic states [38] using either error detection or error correction. The resource evaluation uses the most suitable implementation, which depends on the size of elliptic curve logarithms to compute.

Methods and results — As several parameters are involved, we run an exhaustive search to minimize the product of the average photon number, expected time to solution and total number of physical qubits (the optimization code can be found in [41]). The required resources are shown in Fig. 1 as a function of the number of bits of the prime p , see App. F for the details on the optimal parameters. We see that 126 133 qubits are needed to compute a 256-bit logarithm in 9 hours for example.

Conclusion — We gave the details of an improved quantum computation of discrete logarithm on elliptic curves, taking as an example the one used for securing signatures in Bitcoin transactions. To illustrate the benefits of using this algorithm for a performance analysis, we estimated that the implementation of Shor’s algorithm for the factorization of 2048-RSA integers would take 349 133 cat qubits and 4 days. To illustrate the gain in using a 1D code, this cost estimation can also be compared to the estimate reported in [3] showing that 20 million qubits and 8 hours would be needed for realizing the same factorization with a 2D grid of superconducting qubits and a standard surface code. Note that in both cases, the number of processing qubits can be substantially reduced by adding a quantum memory to the processor [42]. Further note that parallelization has

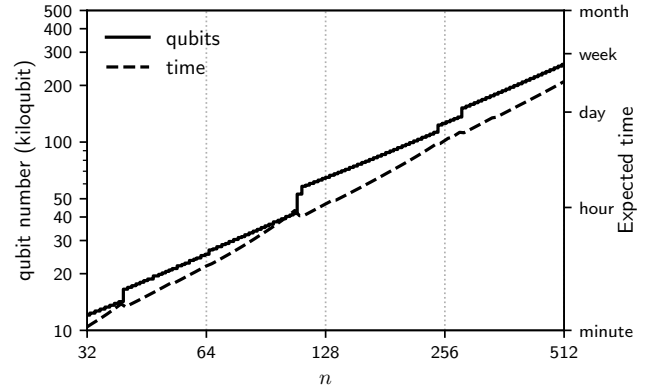


Figure 1. Number of physical cat qubits and runtime for computing a discrete logarithm on elliptic curve as a function of the number of bits in p .

not been exploited in this work. This could dramatically reduce the runtime, especially as the preparation of magical states is resource-efficient and increasing the number of their factories would not significantly increase the total number of qubits, which would allow adequate use of look-ahead adder [43].

D.R., F-M.L.R. and J.G. would like to thank Mazyar Mirrahimi for many discussions about the Toffoli magic state preparation schemes. E.G. and N.S. acknowledge funding by the Institut de Physique Théorique (IPhT), Commissariat à l’Énergie Atomique et aux Energies Alternatives (CEA), the Region Île-de-France in the framework of DIM SIRTEQ, the European Union’s Horizon 2020 research and innovation program European High-Performance Computing Joint Undertaking under grant agreement No 101018180 (HPCQS) and a French national quantum initiative managed by Agence Nationale de la Recherche in the framework of France 2030 with the reference ANR-22-PETQ-0009. D.R., F-M.L.R. acknowledge funding by Plan France 2030 through the project ANR-22-PETQ-0006.

Appendix A: Elliptic curve cryptography

This appendix introduces basic notions that are necessary to understand the discrete logarithm problem and the principles behind elliptic curve cryptographic protocols.

1. Elliptic curve group

Elliptic curve cryptographic protocols are based on elliptic curve groups which are formed from the points of an elliptic curve and an internal operation.

Elliptic curve definition

An elliptic curve is defined over a field (when the characteristic is different from 2 and 3) as the set of points (x, y) whose coordinates satisfy an equation of the form (also refereed as Weierstrass form):

$$y^2 = x^3 + ax + b \quad (\text{A1})$$

where a and b are constants. An additional point at infinity is added to the elliptical curve. In order to further define the group law, the curve has to be non-singular (no cusps nor self-intersections). This holds if $4a^3 + 27b^2 \neq 0$. Note that [Eq. \(A1\)](#) is unchanged under the transformation $y \mapsto -y$, hence the curve is symmetric with respect to the x -axis.

The coordinates and parameters of the curve can belong to any field (of characteristic different from 2 and 3 when defined with [Eq. \(A1\)](#)). Elliptic curves are best represented when the chosen field is \mathbb{R} . However, cryptographic applications typically rely on the field of integers modulo p , with p a prime number. The addition, multiplication and inversion over the coefficients and coordinates throughout this appendix are always to be understood as being modulo p .

Group law

The group law on elliptic curves is commonly referred as an addition between points of the curve, and written with the symbol $+$. We introduce the addition as geometrical operations on the curve, and then give their translation in terms of equations on the coordinates as this is more convenient for implementations on a quantum computer.

Considering two distinct points of the elliptic curve, P and Q , the line joining them usually intersects the curve at a third point R' . The result of the addition, R , is the symmetric of R' with respect to the x -axis. We write $R = P + Q$. Note that the described operation is commutative, which provides a justification of the designation as an

addition. A few particular cases need to be considered. The first one arises when the line is vertical: there is no other intersection than P and Q , and the result of the addition is the point at infinity. The second one happens when the line joining P and Q is tangent to the curve at one of these two points (say the point P). In that case, R' is the point P (it can be pictured as a double contact between the line and the curve). The third special case corresponds to $P = Q$. In this case, the line of interest is the tangent of the elliptic curve in P , and R' is the intersection between this tangent and the curve (or point at infinity if the tangent is vertical). Note that in the special case where Q is at infinity, the vertical line passing through P intersects the curve at the symmetric of P with respect to the x -axis and hence $P + Q = P$. This means that the infinite point is the neutral element. Further note that the symmetric of P with respect to the x -axis is its inverse, $-P$.

Let us now see how the group law translates into equations on the coordinates of the involved points. We study the addition of P and Q with coordinates $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. In the case where $x_P \neq x_Q$, the slope of the line joining P and Q is given by $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$. The division is well-defined as we work on a field (and consider the case $x_P \neq x_Q$). We emphasize that in the cryptographic context, the division applies on integers modulo p . The third solution (apart from P and Q) of the equation determining the intersections between the line and the curve, R' , has the coordinates

$$x_{R'} = \lambda^2 - x_P - x_Q \quad (\text{A2a})$$

$$y_{R'} = y_P + \lambda(x_{R'} - x_P). \quad (\text{A2b})$$

The result of the addition $R = P + Q = -R'$ has as coordinates $x_R = x_{R'}$ and $y_R = -y_{R'}$. Note that $\lambda = \frac{y_{R'} - y_P}{x_{R'} - x_P}$ as R' is also on the line joining P and Q . This remark is useful for uncomputing the value of λ in the context of an in-place addition on a quantum computer.

When $x_P = x_Q$ and $y_P \neq y_Q$, necessarily $y_Q = -y_P$ and $Q = -P$. Hence, the result of the addition is the neutral point, the one at infinity. When $P = Q$ and $y_P = y_Q = 0$, the tangent of the curve in P is vertical and the result of the addition is again the zero. Otherwise, in the generic case for which $P = Q$, the slope of the tangent is given by $\lambda = \frac{3x_P^2 + a}{2y_P}$. The coordinates of the result are given by the formulae used in the generic case while replacing λ by its specific value.

Multiplication

Now that the addition between two points of an elliptic curve is properly described, we can define the multipli-

cation of a point by an integer as

$$kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}. \quad (\text{A3})$$

From this definition, it is clear that the scalar multiplication is associative $[(k_1 k_2)P = k_1(k_2 P)]$, distributive $[(k_1 + k_2)P = (k_1 P) + (k_2 P)]$, compatible with identity $(1 \times P = P)$ and hence satisfies the expected properties of a scalar multiplication.

Note that the multiplication can be computed efficiently by first decomposing the multiplier k in a binary form $k = \sum_i 2^i k_i$. From the distributive property, we have $kP = \sum_i 2^i k_i P$, that is the result can be obtained efficiently by computing the $2^i P$ terms through successive doubling ($2^{i+1}P = 2^i P + 2^i P$) and adding $2^i P$ into a register encoding the result when $k_i = 1$ only. We present in [App. C](#) a windowed version of this algorithm, in the context of quantum computing.

2. Diffie–Hellman key exchange

The Diffie–Hellman protocol is a method of securely exchanging cryptographic keys over a public channel. Prior to the algorithm, Alice and Bob agree on a specific curve, that is they agree on a given prime number p such that the coordinates are numbers of the field of integers modulo p , and on the parameters a and b of [Eq. \(A1\)](#). They also publicly agree on a point G and will work only into the cyclic sub-group generated by G . For the following, we note r the order of this group, and in cryptography applications, r is typically a prime number.

To establish the key, Alice and Bob choose independently and randomly each one a number between 1 and $r - 1$; we write them respectively k_a and k_b . Those numbers are kept secret. Then, they compute respectively $k_a G$ and $k_b G$. The coordinates of those points are exchanged via the public channel. Alice and Bob compute respectively $k_a(k_b G)$ and $k_b(k_a G)$, obtaining the same result due to the commutativity of the multiplication. The x coordinate of this point is the key (the other coordinate is redundant with it, as the curve is publicly known).

Note that we presented here the basic version of Diffie–Hellman algorithm. To have a full operational protocol, authentication is required and the resulting key is usually hashed. Also, several variants exist, for instance the cofactor Diffie–Hellman protocol helps to reduce the risk for Alice of partially revealing her private secret k_a in case of a malicious Bob [\[44\]](#).

3. Elliptic Curve Digital Signature Algorithm

Suppose Alice now wants to send a signed message to Bob. She first needs to create a pair of private and public keys. In the elliptic curve signature algorithm, the private key of Alice is an integer s_a ($< r$), while the public key is given by $P_a = s_a G$. The message to sign is hashed down to the same number of bits than in r , and we write z this hash. Only this z is relevant for the signing algorithm.

The signature protocol starts by randomly picking a number k , smaller than r , that must be kept secret. Then, the point $(i, j) = kG$ is computed, and we define $x = i \bmod r$. In the case $x = 0$, we choose another k and start again the protocol. Then, $y = k^{-1}(z + s_a x) \bmod r$ is computed, and if $y = 0$, another k is chosen and the protocol starts again. The signature is the couple (x, y) .

For verifying the signature, the point $(i, j) = (zy^{-1} \bmod r)G + (xy^{-1} \bmod r)P_a$ is computed. The signature is valid if $x = i \bmod r$, invalid otherwise. To prove the correctness of this verification, we can check that injecting the definition of y in the computed point gives $(i, j) = kG$, and the result follows.

Bitcoin's parameters

The bitcoin protocol uses the elliptic curve digital signature algorithm to ensure that no one can impersonate the issuer of a transaction. This protocol uses the **secp256k1** curve, defined in [\[45\]](#). It works on the field of integers modulo $p = 2^{256} - 2^{32} - 977$ and its equation is $y^2 = x^3 + 7$. The generator G of the cyclic subgroup has the coordinates:

$$\begin{aligned} x = & 55066263022277343669578718895168534326 \\ & 250603453777594175500187360389116729240 \end{aligned} \quad (\text{A4a})$$

$$\begin{aligned} y = & 32670510020758816978083085130507043184 \\ & 471273380659243275938904335757337482424. \end{aligned} \quad (\text{A4b})$$

Those choices result in a subgroup of order

$$\begin{aligned} r = & 11579208923731619542357098500868790785 \\ & 2837564279074904382605163141518161494337, \end{aligned} \quad (\text{A5})$$

which is a prime number.

4. Discrete logarithm problem

The key exchange and signature algorithm presented above are secured under the assumption that given G and kG for some $k < r$, finding k is not possible for the adversary. This is the discrete logarithm problem. The Pollard's rho algorithm is the best known for solving this problem with a classical computer, and a complexity $O(\sqrt{r})$, which is exponential in terms of the number of bits in r . The larger discrete logarithm problem solved so far on a classical computer is based on the curve `secp256k1` with a 114-bit private key [46].

The discrete logarithm problem is tackled by Shor's algorithm, which is seen as a threat for elliptic curve cryptographic protocols.

Appendix B: Shor's and Ekerå's algorithms for discrete logarithm

Shor's algorithm for solving the discrete logarithm problem has been presented in [18, 19]. It was initially designed for the multiplicative group of integers modulo p but actually applies to any finite cyclic group. Ekerå introduced a variation of this algorithm in [25]. In this appendix, these two algorithms are presented and our choice to use Shor's algorithm is justified.

We write G the generator of the cyclic subgroup of the elliptic curve we work with. Its order is denoted by r , and n is the number of bits of r ($r < 2^n \leq 2r$). r is assumed to be a prime number. We write l the logarithm to be determined and P the corresponding point, that is $P = lG$.

1. Shor's algorithm

As for Shor's algorithm for factorizing integers, the one for the discrete logarithm computation is based on the preparation of registers in a superposition of all possible integers between 0 and a large number, followed by the application of a specific function, and the use of quantum Fourier transforms to reveal the period of this function. We here consider the following function of two variables

$$f(x_1, x_2) = x_1G - x_2P. \quad (\text{B1})$$

Note the alternative expression $f(x_1, x_2) = (x_1 - x_2l)G$ holds because of the definition of the logarithm l . The function f is periodic in the following meaning

$$\forall k, f(x_1 + kl, x_2 + k) = f(x_1, x_2). \quad (\text{B2})$$

This periodic feature is in essence what the quantum Fourier transform reveals, which allows one to access to l .

The algorithm starts by preparing two registers in a superposition of all possible numbers between 0 and $r-1$

$$\frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} |x_1\rangle |x_2\rangle. \quad (\text{B3})$$

The function f is computed with those registers as input and the output stored in a new register

$$\frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} |x_1\rangle |x_2\rangle |f(x_1, x_2)\rangle. \quad (\text{B4})$$

An inverse quantum Fourier transform is then applied to the registers containing $|x_1\rangle$ and $|x_2\rangle$. This leads to

$$\frac{1}{r^2} \sum_{x_1, x_2, y_1, y_2=0}^{r-1} e^{2\pi i(x_1 y_1 + x_2 y_2)/r} |y_1\rangle |y_2\rangle |f(x_1, x_2)\rangle, \quad (\text{B5})$$

that we can rewrite as

$$\sum_{y_1, y_2=0}^{r-1} \sum_{k=0}^{r-1} \left[\frac{1}{r^2} \sum_{\substack{x_1, x_2=0 \\ f(x_1, x_2)=kG}}^{r-1} e^{2\pi i(x_1 y_1 + x_2 y_2)/r} \right] |y_1\rangle |y_2\rangle |kG\rangle. \quad (\text{B6})$$

The part between brackets is the probability amplitude associated to the component $|y_1\rangle |y_2\rangle |kG\rangle$. To simplify further the expression of those amplitudes, notice that the condition $f(x_1, x_2) = kG$ is equivalent to $(x_1 - x_2l)G = kG$. Hence $x_1 - x_2l = k \pmod{r}$, that is $x_1 = k + x_2l \pmod{r}$. Plugging the last equality into the argument of the exponential, we obtain the following expression for the probability amplitude associated to $|y_1\rangle |y_2\rangle |kG\rangle$

$$\frac{1}{r^2} \sum_{x_2=0}^{r-1} e^{2\pi i(k y_1 + (y_2 + l y_1) x_2)/r}. \quad (\text{B7})$$

The sum vanishes (destructive interferences) except when $y_2 + l y_1 = 0 \pmod{r}$. Hence, by measuring the registers encoding y_1 and y_2 , the discrete logarithm can be recovered using $l = -y_2 y_1^{-1} \pmod{r}$ (from the choice of cyclic group, we imposed that r is prime and hence y_1 is invertible modulo r). Note that there are r^2 possible measurement outputs (as y_2 and k can each take r different values), each being produced with a probability $1/r^2$. Hence, the probability to obtain the value of the discrete logarithm is 1, as expected due to the normalization.

Note that when implementing the algorithm, the initial superposition of all numbers is usually extended to the next power of two, so that the register can be prepared by separately setting each qubit in the $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ state. The Fourier transform also goes up to the same power of two.

2. Ekerå's algorithm

Ekerå's algorithm for computing general logarithm [25] is a variation of Shor's algorithm allowing to choose a trade-off between the number of operations per run of the algorithm and the number of runs to be executed to access the desired discrete logarithm. We introduce the trade-off parameter s which is a small integer larger or equal than 1. n_r denotes the number of bits needed to write r ($2^{n_r-1} \leq r < 2^{n_r}$) and $n' = \lceil \frac{n_r}{s} \rceil$. The quantum part of Ekerå's algorithm is similar to the one in Shor's algorithm (for discrete logarithm), with the difference that the two registers have the respective sizes $n_r + n'$ and n' . This quantum part is typically repeated s times and the outputs are fed to the classical post-processing detailed in [25].

In Shor's algorithm, $2n_r$ qubits are used for the two registers containing $|x_1\rangle$ and $|x_2\rangle$, and the number of elliptic curve point additions scales accordingly. For Ekerå's algorithm, $n_r + 2\lceil \frac{n_r}{s} \rceil$ qubits are used for the same purpose, giving for instance a number of $3n_r$ qubits when $s = 1$, and n_r qubits in the asymptotic limit $s \rightarrow +\infty$. We tested different values of s and in any case, Shor's algorithm appeared to be a better trade-off when taking into account the overall runtime and the number of qubits. Shor's algorithm requires a prior knowledge of the order r of the cyclic group, while Ekerå's algorithm doesn't need it, but can retrieve it from the measurements [25]. This has a cost, which partially explains the differences we observed. The results presented in this paper are all obtained with Shor's algorithm.

Appendix C: Arithmetic circuits

We here present the circuit to implement Shor's algorithm. More precisely, we show how to compute $f(x_1, x_2) = x_1G - x_2P$ (see Eq. (B1)), that is to compute elliptic curve multiplications. As we show in this appendix, an elliptic curve multiplication can be decomposed into a sequence of elliptic curve additions. As we choose to represent the points of the elliptic curve by their coordinates, each addition is a combination of modular additions, subtractions, multiplications and divisions, see Eq. (A2).

The algorithm we use is derived from the one presented in [27], where integers are in Montgomery's representation, and windowed arithmetic circuits [29] are used. The main differences with respect to [27] is that the circuits are adapted for a direct use of Toffoli gates. Moreover, sub-circuits including controlled adders and comparisons are more efficiently implemented.

1. Montgomery representation

Montgomery's representation allows one to replace a reduction modulo p (obtained by euclidean division) by a halving operation (a division by 2, that is a simple bit shift) during the multiplication step [32, 47, 48]. Here we present the Montgomery representation with parameters relevant for the computation of discrete logarithms in a cryptography context. For a more general definition of Montgomery representation, see [47].

We work with operations modulo p , with $p > 2$ a n -bit long prime number. The basic idea of the Montgomery representation is to represent a number $x \in \mathbb{Z}/p\mathbb{Z}$ by $x' = x2^n \bmod p$ (still in $\mathbb{Z}/p\mathbb{Z}$). Note that 2^n and p are coprime, hence 2^n has an inverse in $\mathbb{Z}/p\mathbb{Z}$, that we write 2^{-n} , and x can be recovered as $x = x'2^{-n} \bmod p$. Although the Montgomery representation is a bijection, we don't need to convert number back to the standard representation in Shor's algorithm.

2. Modular addition

Outline — First, note that the standard modular addition is compatible with the Montgomery transformation

$$\begin{aligned} [(x2^n \bmod p) + (y2^n \bmod p)] \bmod p \\ = (x + y)2^n \bmod p. \end{aligned}$$

The modular addition is the operation $|x\rangle|y\rangle \mapsto |x\rangle|y + x \bmod p\rangle$, where p is a classically known non-negative number and $0 \leq x, y < p$. As mentioned before, p is a n -bit long prime number (x and y have the same length), hence $p < 2^n$. The modular addition, shown in Fig. 2, is implemented in three steps:

1. a non-modular addition of x in the target register, with an additional qubit for the output ($0 \leq x + y < 2p < 2^{n+1}$);
2. a reduction modulo p of the result from first step, with creation of an ancillary qubit that indicates if the reduction happened;
3. the ancillary qubit is uncomputed by flipping it if and only if $x + y \bmod p < x$.

The equivalence mentioned in the third step is ensured because if the modular reduction happens, $x + y$

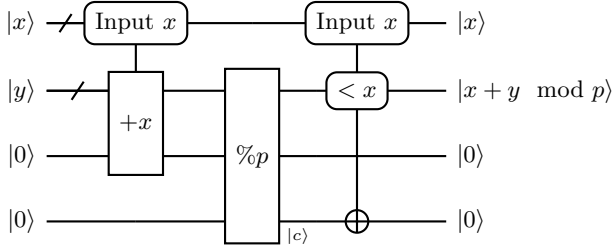


Figure 2. Addition modulo p : $|x\rangle |y\rangle \mapsto |x\rangle |x + y \bmod p\rangle$. It is obtained by a standard non-modular addition, a reduction modulo p that also creates an ancillary qubit $|c\rangle$ indicating if the reduction happened, and the uncomputation of the ancillary qubit through comparison between the result and x . Each of those three steps is achieved with a circuit detailed in following figures.

$\bmod p = x + y - p$ and as $y < p$ we have $x + y - p < x$, while if it doesn't happen, $x + y \bmod p = x + y$ and $y \geq 0$ implies that $x + y \geq x$.

We detail each of these three steps separately.

Non-modular addition — The first step is a non-modular addition: $|x\rangle |y\rangle \mapsto |x\rangle |x + y\rangle$ which is implemented by the circuit presented in Fig. 3, introduced in [31, Fig. 4, modified with the optimizations 4 and 5 proposed in this reference]. This circuit starts by computing successively the carry bits using repetitively the sub-circuit labeled as MAJ in Fig. 3 (each carry is temporarily stored in the qubit initially containing $|x_k\rangle$). The MAJ operations are then uncomputed while the bit encoding the result is set to its output value, with the sub-circuit labeled as UMA. First and last qubits are special cases with simplified and combined versions of MAJ and UMA operations. Note that for simplicity, we did not take into account the additional optimizations proposed in [31] which reduces the depth of the circuit (using time-optimal computation [49, 50] would give an even shallower circuit).

Modular reduction — The modular reduction consists in taking as input a register containing a number z such that $0 \leq z < 2p$, and outputting:

$$z \bmod p = \begin{cases} z & \text{if } z < p \\ z - p & \text{if } z \geq p \end{cases}.$$

To ensure reversibility, another output has to be generated: a bit c that indicates if the reduction occurred, and takes as value the quotient of the Euclidean division of z by p .

The modular reduction can be implemented with various circuits, three of them are presented in App. C 3. The most efficient is the third one and is the one we consider.

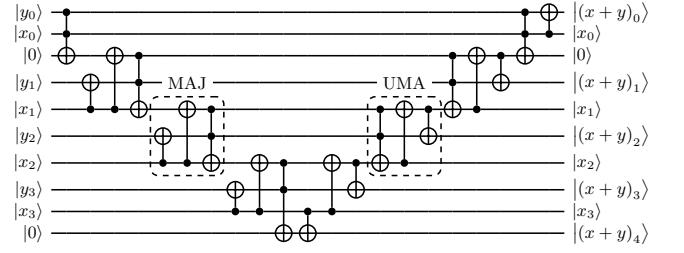


Figure 3. Adder with output carry. It implements the operation $|x\rangle |y\rangle \mapsto |x\rangle |y + x\rangle$, where the register y has one extra qubit at the output. Here the two inputs are represented on 4 bits. The MAJ sub-operation computes from the former carry and one bit from each input the following carry (set in the bottom qubit). The UMA sub-operation restores the x bit and the previous carry, and computes the current bit of the result. MAJ and UMA operations are used on every qubit pair, except the first and last for which we use a more efficient implementation.

Comparison — The last step is the uncomputation of the ancillary qubit generated by the reduction: $|x\rangle |z\rangle |z < x\rangle \mapsto |x\rangle |z\rangle |0\rangle$ ($|z < x\rangle$ is one qubit indicating if $z < x$ is true or false), which is done with a comparison between x and z . The corresponding circuit is presented in Fig. 4. As for the addition (Fig. 3), it consists in propagating carries, then the most significant bit is used, and the carries are uncomputed to restore the inputs. More precisely, the first half of the circuit is identical to the one for implementing a subtraction modulo 2^{n+1} : $|x\rangle |z\rangle \mapsto |x\rangle |z - x \bmod 2^{n+1}\rangle$, with n the number of bits of x and z . As $0 \leq x, z < 2^n$ and $0 \leq z - x \bmod 2^{n+1} < 2^{n+1}$, only two cases are possible:

$z - x \bmod 2^{n+1} = z - x$: as $z < 2^n$ and $x \geq 0$, $z - x < 2^n$ and we conclude that the most significant bit of the result takes value 0. On the other hand, $0 \leq z - x \bmod 2^{n+1} = z - x$ implies that $x \leq z$.

$z - x \bmod 2^{n+1} = z - x + 2^{n+1}$: as $x < 2^n$ and $z \geq 0$, $2^n < z - x + 2^{n+1}$ and we conclude that the most significant bit of the result takes value 1. On the other hand, $z - x \bmod 2^{n+1} = z - x + 2^{n+1} < 2^{n+1}$ implies that $z < x$.

From those two cases, we draw the conclusion that the most significant bit takes value 1 if and only if $z < x$. The uncomputation of the ancillary qubit can be achieved with a single CNOT controlled by the most significant bit and targeting the qubit to uncompute.

The circuit for achieving a subtraction modulo 2^{n+1} is the conjugate of the one for computing an addition modulo 2^{n+1} . It thus starts with UMA[†] operations, as defined in Fig. 3. In the comparison circuit, only the first half of the subtraction is used while the last half

uncomputes the carries, with UMA operations. In Fig. 4, we reduced the circuit size by directly uncomputing the target qubit instead of computing the most significant bit and then using it to control a CNOT.

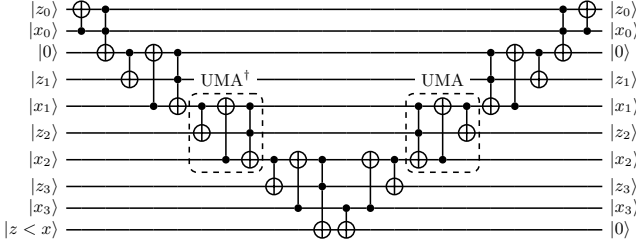


Figure 4. Comparison for uncomputing the ancillary bit: $|x\rangle|z\rangle|x < z\rangle \mapsto |x\rangle|z\rangle|0\rangle$. This first half of this circuit is based on a subtraction modulo 2^{n+1} (n being the number of bits of x and z), the conjugate of an addition. The most significant carry is used to perform the uncomputation, and then the inputs are restored to their original values. The boxed UMA^\dagger and UMA operations (same as in Fig. 3) compute and uncompute the carries, and are repeated for each qubit pair, except the first and last one where specific case circuits allow small optimization.

3. Modular reduction

A key sub-circuit for the modular addition (second step) and more broadly for the discrete logarithm computation, is the modular reduction. It consists in the following operation: $|z\rangle \mapsto |z \bmod p\rangle|c\rangle$ where p is a known integer, $0 \leq z < 2p$, and c indicates if the reduction happened (c is the quotient of the Euclidean division of z by p : $c = 0 \iff z \bmod p = z$; $c = 1 \iff z \bmod p = z - p$). The presence of $|c\rangle$ in the outputs ensures the reversibility of the modular reduction. We emphasize that n denotes the number of bits of p . z is initially coded on $n + 1$ qubits. We present here separately three different implementations of the modular reduction.

First implementation — The most common implementation [32, 51, 52] consists in subtracting p modulo 2^{n+1} , copying the most significant bit (that indicates the sign of the result $z - p$) and controlled by the copied bit, adding p . This algorithm is depicted in Fig. 5. The subtraction and the addition are detailed in the following sub-paragraphs.

Semi-classical subtraction We here consider the subtraction modulo 2^{n+1} of a classical value p from a quantum register encoding z , see the first operation in Fig. 5. The basic idea is to add $p' = 2^{n+1} - p$ modulo 2^{n+1} to the quantum register with the circuit presented

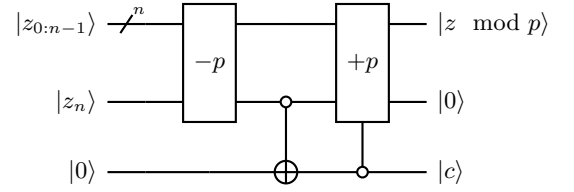


Figure 5. Modular reduction: first proposition. Apart from the reduction, it produces a qubit $|c\rangle$ indicating if the reduction happened, which is the quotient of the Euclidean division of z by p . The uncomputation of this qubit state depends on the context of the modular reduction. The addition and subtraction are here operations modulo 2^{n+1} .

in Fig. 6. As in Fig. 3, this circuit is ripple-carry based, with the main difference that one of its input is a classical number. The circuit has been adapted to take advantage of this classical input. It is inspired by [4, 31]. In the first half of the computation, the carry is computed at each step from the previous carry, the input qubit and the classical number. During the second half the carries are uncomputed while the result qubits are set to their desired values. First and last qubits are treated separately as special cases for which optimizations can be used.

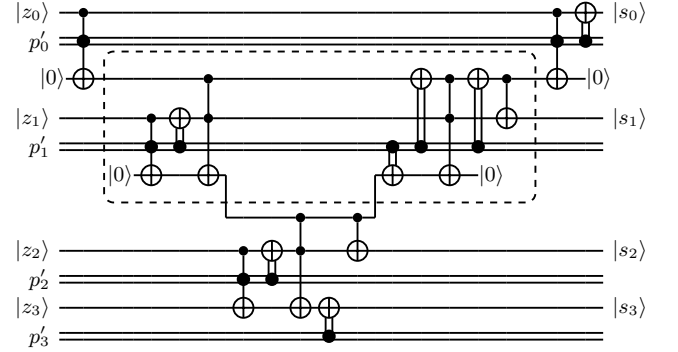


Figure 6. Semi-classical subtraction performing the operation: $|z\rangle \mapsto |z - p \bmod 2^{n+1}\rangle$, with n the number of bits in p . z has $n + 1$ qubits. Here we used $p' = 2^{n+1} - p$ and $s = z - p \bmod 2^{n+1}$. The boxed block is repeated for each qubit, except the first and last one that are handled with the depicted special cases.

Semi-classical controlled addition After copying the most significant bit of $z - p \bmod 2^{n+1}$, a controlled semi-classical addition is made in the modular reduction shown in Fig. 5. For simplicity, we write $z' = z - p \bmod 2^{n+1}$ the input of this addition. The sub-circuit of interest thus performs the addition of p modulo 2^{n+1} if the control qubit takes value 1: $|\text{ctrl}\rangle|z'\rangle \mapsto |\text{ctrl}\rangle|z' + \text{ctrl} \times p \bmod 2^{n+1}\rangle$. It is realized by the circuit presented in Fig. 7. As in Fig. 6, we consider a ripple-carry based adder. The boxed part of Fig. 7 conditionally

computes the next carry from the previous carry, input qubit and classical bit, and then uncomputes it while setting the result qubit. It is repeated for each qubit, with a special case for the first and last qubits, for which simplifications are possible.

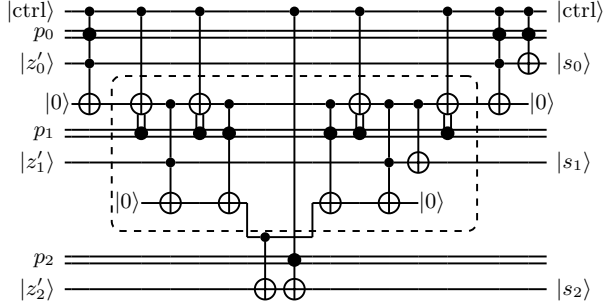


Figure 7. Semi-classical controlled adder. z' is the input number stored in a register of $n + 1$ qubits. p is known in the control software, and $s = z' + \text{ctrl}.p \bmod 2^{n+1}$. The boxed part takes as input the previous carry, the input qubit and classical bit, and conditioned on the control computes the following carry; it is then uncomputed and the output qubit is conditionally set. This boxed part is repeated for each input qubit, except the first and last ones, where optimizations are possible. Note that in the context of modular reduction, p has n bits and the most significant bit of s takes value 0. However, the presented circuit would work even if this is not the case.

Second implementation — A slightly simpler implementation of the modular reduction consists in comparing first z and p , and then subtracting p depending on the result of the comparison, see Fig. 8. We detail below the comparison and the controlled subtraction separately.

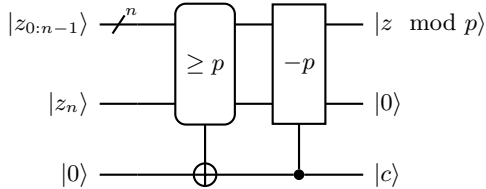


Figure 8. Modular reduction, second proposition.

Semi-classical comparison The first step compares the value z stored in the input quantum register with the number $p > 0$ (known in the control software): $|z\rangle |0\rangle \mapsto |z\rangle |z \geq p\rangle$. It is obtained with the circuit presented in Fig. 9, inspired by [4, Fig. 17]. Here z is written in a $n + 1$ qubit register and p uses n bits (but the circuit we present would work identically for a p with up to $n + 1$ bits). The principle is to compute the highest bit of $z + p'$ with $p' = 2^{n+1} - p$, which takes the value 1 if and only if $z + p' \geq 2^{n+1} \iff z \geq p$. It is obtained by computing all the carries with a semi-classical version of the MAJ

operation (see Fig. 3) and then uncomputing the carries with the conjugated circuit.

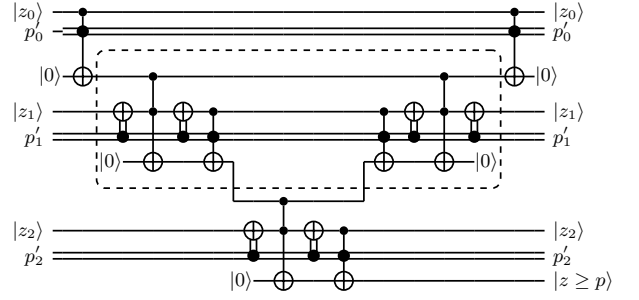


Figure 9. Semi-classical comparison circuit. z and p are compared, and the output bit takes value 1 if and only if $z \geq p$, while the quantum register containing z is restored to its initial value at the end. z is contained in a register of $n + 1$ qubits. p' is defined as $p' = 2^{n+1} - p$ with a n -bit long p . The basic principle of the circuit is to compute all carries of $z + p'$ successively, the last carry taking value 1 if and only if $z + p' \geq 2^{n+1} \iff z \geq p$. The boxed sub-circuit computes the carry with a semi-classical version of the MAJ operation (see Fig. 3) and then uncomputes it with the conjugated circuit; the boxed part is repeated for each bit. First and last bits are special cases and associated to sub-circuits represented outside the box.

Semi-classical controlled subtraction The semi-classical controlled subtraction is done using the circuit presented in Fig. 7 which implements a semi-classical controlled adder, but with a classical input $p' = 2^{n+1} - p$ (instead of p).

Third implementation — In the previous implementation of the modular reduction, the comparison is done by first computing the carries of $z + p'$ successively, then the last carry is copied and finally the carries are uncomputed. The subtraction is then realized by first computing again the carries of $z + p'$ (controlled on the copy qubit). The two operations can be merged in order to avoid the computation of the same carries twice. This requires to change the controlled semi-classical for a version where the control only applies to the UMA part. The resulting circuit is presented in Fig. 10.

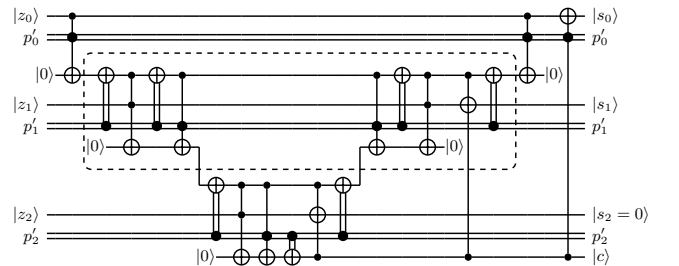


Figure 10. Modular reduction, producing a garbage qubit $|c\rangle$ that indicates if the reduction happened.

This circuit being the most efficient, it is the one we use for the resource estimation.

4. Multiplication

Multiplication algorithm

In Montgomery representation [47] with prime number p and radix 2^n , n being the number of bits in p , the multiplication of x and y consists in computing $xy2^{-n} \bmod p$. Note that x and y are here in the Montgomery representation. Here we adopt a version that interleaves the multiplication and division by 2^n in a windowed manner [27, 29]. More precisely, with w the size of each window, we use the decomposition:

$$\begin{aligned}
 & xy2^{-n} \bmod p \\
 &= \sum_{k=0}^{n-1} \sum_{j=0}^{w-1} x_{k+j} y 2^{j+k-n} \bmod p \\
 &= \sum_{k=0}^{n-1} \sum_{j=0}^{w-1} x_{k+j} y 2^j \left[2^{k-n} \bmod p \right] \\
 &= \left\{ \left[(x_0 y + x_1 2y + \dots + x_{w-1} 2^{w-1} y) 2^{-w} \right. \right. \\
 &\quad \left. \left. + x_w y + \dots + x_{2w-1} 2^{w-1} y \right] 2^{-w} \right. \\
 &\quad \left. + \dots \right\} 2^{-(n \bmod w)} \bmod p \\
 &= \left\{ \left[(x_{0:w} y) 2^{-w} + x_{w:2w} y \right] 2^{-w} \right. \\
 &\quad \left. + \dots \right\} 2^{-(n \bmod w)} \bmod p.
 \end{aligned}$$

with $x_{a:b} = \sum_{j=a}^{b-1} x_j 2^{j-a}$ (we emphasize that b is excluded) the number made from the slice of bits representing x (from bit a to bit $b-1$). As the two inputs x and y are in quantum registers, there is no obvious way to use windows to group the controlled additions, and only the modular reduction is done in a windowed way. Here we implement the multiplication in an out-of-place manner: $|x\rangle |y\rangle |0\rangle \mapsto |x\rangle |y\rangle |xy2^{-n} \bmod p\rangle$. This takes controlled (non-modular) additions, table lookups and additions (modulo 2^n), see Fig. 14 which is explained later. Before detailing the circuit implementing this multiplication algorithm, we first describe the sub-circuits it uses.

Sub-circuits

Controlled non-modular addition — The controlled non-modular addition between two quantum regis-

ters, corresponding to the operation $|\text{ctrl}\rangle |x\rangle |y\rangle \mapsto |\text{ctrl}\rangle |x\rangle |y + \text{ctrl}.x\rangle$, is obtained by using the circuit presented in Fig. 11. It works similarly to the adder circuit from Fig. 3, but where the UMA sub-circuit is modified to be controlled, that is, UMA is applied when the control qubit has value 1 while MAJ[†] is applied when the control qubit has value 0.

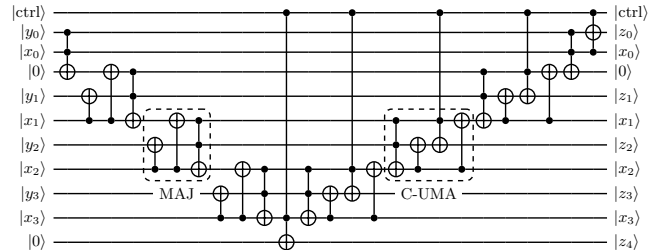


Figure 11. Controlled adder with output carry. It accomplishes the operation $|\text{ctrl}\rangle |x\rangle |y\rangle \mapsto |\text{ctrl}\rangle |x\rangle |z = y + \text{ctrl}.x\rangle$, with the register containing y and z having one extra qubit at the output. MAJ and UMA sub-operations have the same meaning as in Fig. 3. C-UMA applies UMA when the control qubit takes value 1 and MAJ[†] otherwise. MAJ and C-UMA are repeated as many times as required.

Table lookup — The table lookup operation, introduced in [28] and discussed in [29, Fig. 2], consists in loading into a quantum register some value from a table, known in the control software, according to an index given by a quantum register. For a table T , it performs the following operation: $|k\rangle |0\rangle \mapsto |k\rangle |T[k]\rangle$. Note in particular that if the address register (the one specifying the index value k) is in a superposition, the register loaded with $T[k]$ ends up entangled with the address one, that is $\sum_k \alpha_k |k\rangle |0\rangle \mapsto \sum_k \alpha_k |k\rangle |T[k]\rangle$.

The circuit for performing this operation is presented in Fig. 12. The part in the dashed box has an auxiliary qubit inside which is controlled by two inputs: the top one (initially in $|0\rangle$ and connected to the qubits $|k_1\rangle$ and $|k_2\rangle$) by a Toffoli gate in Fig. 12 acts as a control while the second one (in state $|k_0\rangle$ in Fig. 12) operates as a selector. When the control qubit is in state $|0\rangle$, the ancillary qubit always stays in $|0\rangle$. When the control qubit is in state $|1\rangle$ and the selector qubit is on state $|1\rangle$, the value of the ancillary qubit is first flipped to value $|1\rangle$ (with a first Toffoli) then back to $|0\rangle$ (with a CNOT), while if the selector qubit is on state $|0\rangle$, the ancillary qubit first takes value $|0\rangle$ and then $|1\rangle$. By recursively using the circuit in the box (with special case for the first qubit), a circuit is obtained such that for each possible value of k , the last ancillary qubit takes the value $|1\rangle$ at a given step at which the target register is encoded in $|T[k]\rangle$ and stays otherwise at value $|0\rangle$. Note that the second Toffoli gate of the boxed block can be replaced by a measurement-based uncomputing, see [28, Fig. 4] for details.

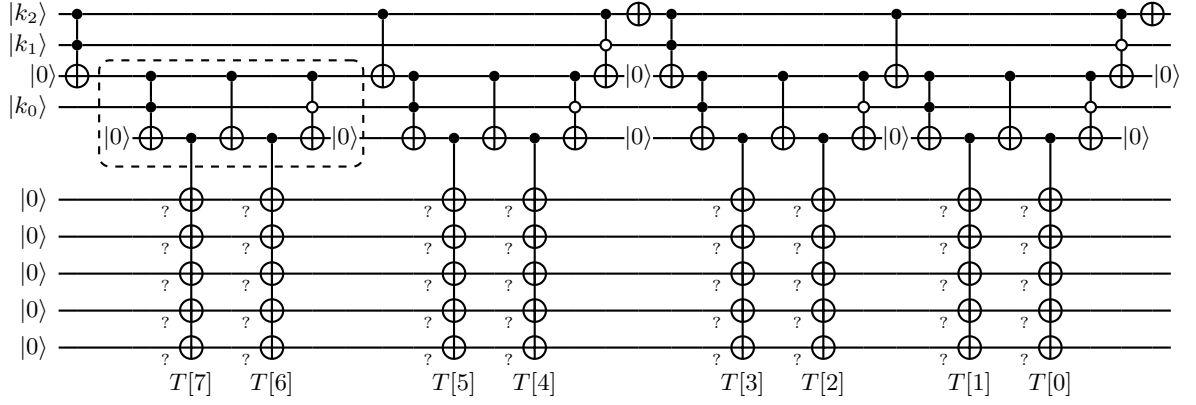


Figure 12. Lookup table circuit for an index composed of 3 qubits and a value register of 5 qubits. The elementary building block of the circuit is boxed; it is used recursively (by replacing the output controls by the same block acting on next qubit from k). The targets with question mark indicates that the CNOT is applied if the corresponding bit of $T[k]$ has value 1; otherwise the gate is skipped. Further description of this circuit is given in the text.

The preparation of the target registry in $|T[k]\rangle$ (see the lower part of Fig. 12) is obtained by applying NOT gates for each bit of $T[k]$ that has the value 1. These NOT gates are controlled by the upper part. Note that lattice surgery allows to merge all those NOT gates with a single control into one gate on all the involved logical qubits.

After use of $T[k]$, the register can be cleared by applying again the same circuit. However, we consider in our resource estimation a more efficient way based on measurements which has been introduced in [53, Appendix C] and improved in [29]. For more details on the measurement-based cleanup, see [42, Appendix D3].

Addition — The addition modulo 2^n with n the number of bits in the inputs is obtained with a circuit from [31] presented in Fig. 13. The repeated bloc is the same as in the non-modular addition (Fig. 3), and the circuits differ only for the most significant qubit.

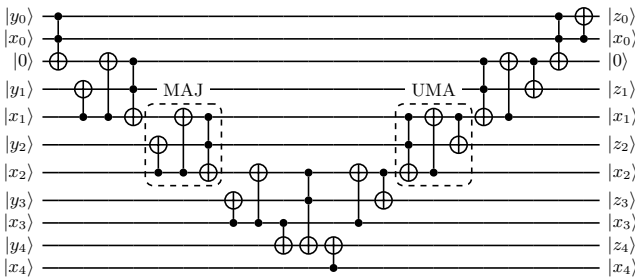


Figure 13. Adder modulo 2^n with n the number of bits of the inputs. It accomplishes the operation $|x\rangle|y\rangle \mapsto |x\rangle|z = y + x \bmod 2^n\rangle$. MAJ and UMA sub-operations, which are described in the caption of Fig. 3, are repeated for each pair of qubits except the first and two last qubits.

(Dirty) multiplication circuit

We emphasize that the goal is to compute $xy2^{-n} \bmod p$ out-of-place from the following sum of blocks $\left\{ \left[(x_{0:w}y)2^{-w} + x_{w:2w}y \right] 2^{-w} + \dots \right\} 2^{-(n \bmod w)} \bmod p$. This is done by repeatedly applying the circuit presented in Fig. 14 (taken from [27, Fig. 4]) for each block $x_{k:k+w}$, with $k \in \{0, w, 2w, \dots, \lfloor \frac{n}{w} \rfloor w\}$, of the windowed decomposition of the input x . In Fig. 14, we consider a labelling of windows according to $i \in \{0, 1, 2, \dots, \lfloor \frac{n}{w} \rfloor\}$ such that $k = iw$. Thus, the blocks of x are written $x_{iw:iw+w}$ (keep in mind that the last index $iw + w$ is excluded from the sum, i.e. $x_{iw:iw+w} = \sum_{j=iw}^{iw+w-1} x_j 2^{j-iw}$). The circuit starts by the non-modular addition of $x_{iw:iw+w}y$ to a target register (which includes the register $|z\rangle$ and w auxiliary qubits as shown in Fig. 14, all initialized to $|0\rangle$ for $i = 0$), by using w shifted additions. The division of $z_i + x_{iw:iw+w}y$ by 2^w modulo p is obtained by first adding to $z_i + x_{iw:iw+w}y$ the smallest multiple of p canceling its first w bits and by then performing a standard (non-modular) division by 2^w , by forgetting the first w bits with a bit re-labellization. This is done in five steps. First, the w less significant bits of the target register, which encode a number we call m_i is copied in a garbage register (second to last register in Fig. 14). Second, a table lookup is used to load $T[m_i] = (-m_i p^{-1} \bmod 2^w) \times p$ in an auxiliary register (last register in Fig. 14). $T[m_i]$ is the smallest multiple of p such that $m_i + T[m_i] = 0 \bmod 2^w$. Third, $T[m_i]$ is added to the target register, setting its w lowest bits to 0. Fourth, the division by 2^w is realized by forgetting the first w zeros of the target register and by relabelling the $w + 1$ th bit as the first bit, the $w + 2$ th bit as the second bit and so on up to the last bit. Fifth, the register containing $T[m_i]$ is cleaned. Once the circuit is applied on each block of the windowed

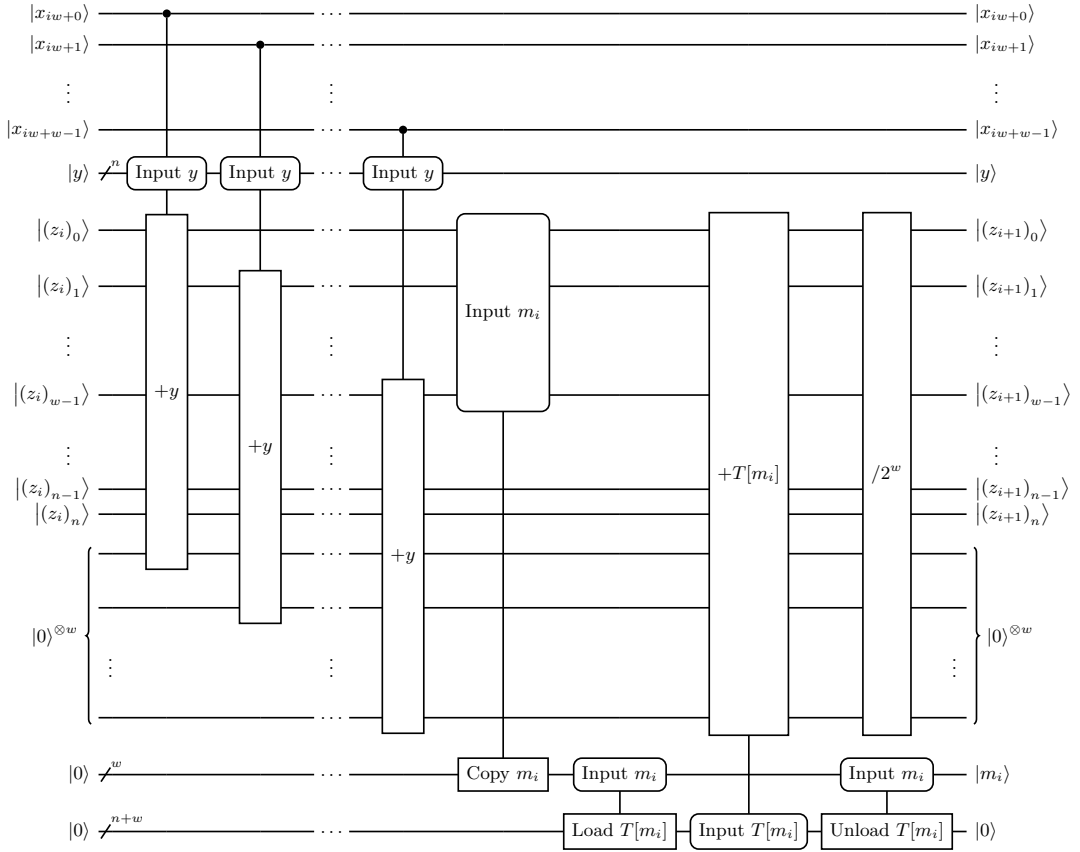


Figure 14. Circuit for one window of the Montgomery multiplication. The full multiplication is obtained by repeating it over all the blocks of the windowed representation of x , leading to the operation $|x\rangle |y\rangle |0\rangle \mapsto |x\rangle |y\rangle |xy2^{-n}\rangle$. w is the size of the window, n the number of qubits in x and y , and $T[m_i] = (-m_i p^{-1} \bmod 2^w) \times p$. At the first iteration, the register containing $|z_i\rangle$ starts at $|z_0 = 0\rangle$. After the last iteration, a modular reduction is applied to the register of z to obtain the result.

decomposition of x , the last step consists in realizing a modular reduction (see App. C 3 for its implementation). This creates an additional garbage qubit, which is stored in the same way as the $|m_i\rangle$. Note that for the last iteration, the size of the last window is reduced to the number of remaining qubits. Further note that the garbage qubits are entangled with the outputs of the circuit. They are typically cleared by latter applying the conjugate of the whole multiplication circuit, *cf.* next subsubsection for an example.

We now discuss the size of the different registers. By definition, we consider $0 \leq x, y < p$ and since $p < 2^n$, we have $0 \leq x, y < 2^n$. Let z be the initial value encoded in the target register, as in Fig. 14. Let us prove by induction that $0 \leq z < 2p$. For the first iteration $z = 0$ and the bound is satisfied. Let us assume that $z < 2p$ and prove the same bound after the circuit represented in Fig. 14. As $x_{iw:iw+w} \leq 2^w - 1$ and $y < p$, we have $x_{iw:iw+w}y < 2^w p - p$. We also have $-m_i p^{-1} \bmod 2^w \leq 2^w - 1$, hence $T[m_i] \leq 2^w p - p$. We can then conclude

$$z + x_{iw:iw+w}y + T[m_i] < 2p + p2^w - p + p2^w - p = p2^{w+1}.$$

After the division by 2^w , we are back to a number strictly smaller than $2p$. This concludes the proof that the value of the target register satisfies $0 \leq z < 2p$, *i.e.* $n+1$ qubits are sufficient.

Note that in our case, the multiplication circuit is used to compute $xy2^{-n} \bmod p$, *i.e.* a final modular reduction is required to go back to a number strictly smaller than p .

Further note that the advantage of the Montgomery representation with respect to a standard double-and-add method lies in the fact that it uses modular divisions by two instead of modular doubling. The former is less expensive to compute as long as we don't clean the ancillary qubits, because the need for a reduction can be assessed only by probing the less significant bit value, while the doubling requires a full comparison (which is costly, even when merged with the reduction as in Fig. 10).

Clean multiplication

In some situations, a multiplication circuit that does not create garbage qubits is required. The garbage register in the dirty multiplication circuit presented before can be reset to its initial value $|0\rangle^{\otimes w}$ by copying the result encoded in the target register into another register with CNOT gates, and then applying the conjugate of the multiplication circuit [54], that is

$$\begin{aligned} |x\rangle |y\rangle |0\rangle |0\rangle |0\rangle &\xrightarrow{\text{mul}} |x\rangle |y\rangle |0\rangle \quad |xy2^{-n}\rangle \left| \bigotimes_{\times}^{(x,y)} \right\rangle \\ &\xrightarrow{\text{copy}} |x\rangle |y\rangle |xy2^{-n}\rangle |xy2^{-n}\rangle \left| \bigotimes_{\times}^{(x,y)} \right\rangle \\ &\xrightarrow{\text{mul}^\dagger} |x\rangle |y\rangle |xy2^{-n}\rangle |0\rangle \quad |0\rangle \end{aligned}$$

Note that in some cases where the garbage qubits can be kept temporary, the dirty multiplication is enough (the copy is not needed).

Squaring

For implementing an out-of-place squaring operation, note that the circuit of Fig. 14 performs an out-of-place multiplication which does not modify y . Hence, the squaring is obtained by copying the bits of y into the register encoding x with CNOT gates, then applying the multiplication, and finally cleaning the x register with CNOT gates. This can be done window by window in order to limit the size of the “ x ” register to w qubits. A clean version of this squaring operation is obtained using the strategy used to get the clean multiplication. To subtract the squaring result from another register, the copy sub-operation in the clean squaring is replaced by a subtraction, obtained by conjugation of the adder circuit from Fig. 13.

5. Modular inversion

During the elliptic curve group operation, the computation of a slope is necessary. This takes a modular division, which is presented in this section.

As we use the Montgomery representation to simplify the multiplications, we need to consider an implementation of the inversion which is compatible with this representation. Concretely, given a number y with a Montgomery representation $x = y2^n \bmod p$, an in-place version of the modular inversion operates as $|x\rangle \mapsto |x^{-1}2^{2n} \bmod p\rangle$. As in [27, 32], we consider an implementation of the modular inversion in Montgomery representation using Kaliski’s algorithm [34].

Kaliski Algorithm — A python “pseudo-code” of the algorithm is given by

Algorithm 1 Kalisky algorithm [55]

```
def kaliski(x: int, p: int, n: int):
    u, v, r, s = p, x, 0, 1
    for i in range(0, 2*n):
        # Note: u and v even impossible
        if v == 0:
            r = 2*r elif u v = v//2
            r = 2*r
        elif u u = u//2
            s = 2*s
        # From here, u and v both odd
        elif u > v:
            u = u - v
            r = r + s
            u = u//2
            s = 2*s
        else:
            v = v - u
            s = s + r
            v = v//2
            r = 2*r
    assert u == 1
    assert v == 0
    assert s == p
    if r >= p:
        r = r - p
    return p - r
```

This algorithm runs on u, v, r and s . They are initialized as $u = p, v = x, r = 0$ and $s = 1$, with $x < p$. At the end of the algorithm $u = 1, v = 0, s = p$ and r is such that $p - r = x^{-1}2^{2n} \bmod p$ is the desired result, as we show below. The number of iterations k which is required to reach $v = 0$ is in between n and $2n$ depending on the input values. Stopping the algorithm after $2n$ iterations is thus sufficient (note that on a classical computer, we would stop right after $v = 0$ and group the remaining modular doublings of r).

We now present the main ideas of how to bound the size of registers, compute the number of iterations for the convergence of the algorithm and prove the values taken by the outputs. More detailed proofs can be found in [34]. In this paragraph, we consider the k first iterations of the algorithm, which lead to $v = 0$ (only modular doubling of r happens from the $(k + 1)$ th iteration, see the first if of the for loop in Algorithm 1). First note that the equality

$$p = us + vr \tag{C1}$$

is initially satisfied and we can easily check that it holds at each iteration. We can also prove by induction that $1 \leq s, 1 \leq u, 0 \leq v \leq x, \gcd(u, v) = \gcd(x, p) = 1$ and

that after i iterations of the loop (while the condition $v = 0$ is not yet reached):

$$xr \equiv -u2^i \pmod{p} \quad (\text{C2a})$$

$$xs \equiv v2^i \pmod{p}. \quad (\text{C2b})$$

Due to the non-negativity of all integers involved in Eq. (C1), it is clear that for all iterations $i < k$, we have $0 \leq u, v, r, s \leq p$, the upper bound being even strict for v and r (because $1 \leq us$ and v is decreasing). After the k th iteration resulting in $v = 0$, we have $0 < r < 2p$. Those bounds allow us to correctly size the registers containing the different variables.

Next, we can check that the product uv is at least divided by 2 at each step. This implies that after i iterations, $uv \leq \frac{px}{2^i} < 2^{2n-i}$. We can conclude that after $2n$ steps, $uv = 0$ hence $v = 0$. On the other hand, $u + v$ is at most divided by 2 at each step, hence after i iterations, $u + v \geq \frac{x+p}{2^i} > \frac{p}{2^i} \geq \frac{2^{n-1}}{2^i}$. Since at the penultimate $(k-1)$ iteration $u = v = 1$, we can conclude that the number of iterations before reaching $v = 0$ is at least n .

To prove the terminal values, first note that at the end, $v = 0$. Using $\gcd(u, v) = 1$, we conclude that at the end $u = 1$. Given Eq. (C2b) and $1 \leq s \leq p$, we get $s = p$ when $v = 0$. Finally, for the k such that $v = 0$ we deduce from Eq. (C2a) and $u = 1$ that $r \equiv -x^{-1}2^k \pmod{p}$. The $2n - k$ following loop executions consist in modular doubling, and result in $r = -x^{-1}2^{2n} \pmod{p}$.

Note that numerical tests we performed suggest that the maximum possible value of k could be equal to $2n - 1$ instead of $2n$, as presented above. We did not investigate this further, as this would insignificantly change the cost of the overall algorithm.

Note that in Algorithm 1, the two operations performed in the first two **else if** are identical. They are applied on v and r for the first **else if** and on u and s for the second **else if**. Similarly, the four operations in the last two **else if** are the same and are applied on u, v, r, s and v, u, s, r respectively. Moreover, in each **else if**, one division and one multiplication by 2 are applied. Instead of performing these operations in a conditional way, we can apply them systematically and make use of controlled swap operations to apply them on the proper register, as proposed in [27, Fig. 7]. This reduces the number of operations and make their implementation easier as they are not controlled anymore. The resulting classical formulation of the algorithm is:

Algorithm 2 Kaliski algorithm with swaps [55]

```
def kaliski_swaps(x: int, p: int, n: int):
    u, v, r, s = p, x, 0, 1
    for i in range(0, 2*n):
        if v == 0:
            r = r*2 continue
        swap = False
        if (u or (u and u > v)):
            u, v = v, u
            r, s = s, r
            swap = True
        if u > v:
            s = s + r
        v = v//2
        r = 2*r
        if swap:
            u, v = v, u
            r, s = s, r
    return u, v, r, s
```

Quantum circuit — The quantum circuit corresponding to one iteration of Algorithm 2 is given in Fig. 15, which is largely inspired by [27, Fig. 6b].

Note that u, v, r and s have the same meaning that in Algorithm 1 and must be initialized accordingly. The last qubit, in state $|f\rangle$, indicates when the “stop” condition $v = 0$ is reached. It starts with the value 1 and is switched to 0 at the beginning of the first round for which $v = 0$, see the first two gates, before step 1. Once it is set to 0, only the modular doubling is applied.

Qubits $|a\rangle$, $|b\rangle$ and $|m_i\rangle$ are used to decide which branch of the algorithm is run. More precisely, as long as $f = 1$, those qubits take the values $a = (u \text{ is even})$, $b = (u \text{ even or } v \text{ even})$ and $m_i = (u \text{ odd and } v \text{ even})$ before the comparison, see step 2. Note that the control by a register corresponds to a control by the least significant qubit of the register (control through the parity of the integer encoded in the register). After the comparison, the values become $a = (u \text{ even or } [u \text{ and } v \text{ odd and } u > v])$, $b = (u \text{ even or } v \text{ even})$ and $m_i = ([u \text{ odd and } v \text{ even}] \text{ or } [u \text{ and } v \text{ odd and } u > v])$, see step 3. Since u and v can’t be simultaneously even (Eq. (C1) tells us that if u and v are both even, p is even meaning that it is not a prime integer), a corresponds exactly to the condition for applying the swaps in Algorithm 2 (second **if**). The logical complement of b is the condition for applying the subtraction and addition, see the gates between step 4 and step 5.

b is uncomputed right after the subtraction and addition by means of the two CNOT gates with a and m_i as controls and b as target. Note that the contributions to a and m_i from the comparison (between steps 2 and 3) cancel each other when clearing b . The uncomputation

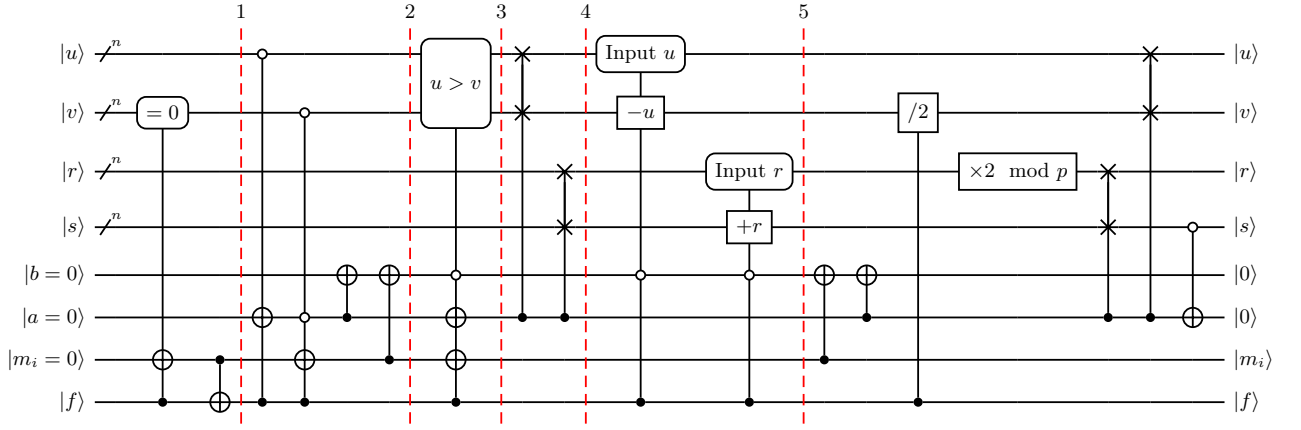


Figure 15. One iteration of Kaliski algorithm for modular inversion, with swaps. This figure is inspired from [27, Fig.6b]. Controls on a register indicate a control by its least significant bit. At the first step, $f = 1$. The different $|m_i\rangle$ are kept as garbage qubits, and are cleared by applying the conjugate of this circuit. See the text for the description of the algorithm and circuit.

of a relies on the swap operations that $|a = 1\rangle$ generates. More precisely, the register r and s are swapped before the subtraction and after the modular multiplication by 2. Note that the bound $0 \leq s < p$ has been proven with non-modular multiplication by 2, hence the modular reduction never happens. In addition, r and s can't be simultaneously even (see Eq. (C1)). This guarantees that if and only if the swap happened s is even right before the very last NOT operation on a conditioned on $s = 0$, hence, cleaning $|a\rangle$.

In Fig. 15, the first operation is a check of equality with 0, that is a multiple-controlled-NOT gate. It can be implemented by applying successively AND gates: a Toffoli gate targeting a clean ancillary qubit which is later uncomputed with another Toffoli gate (or via a measurement and correction as in [28, Fig.4]), as depicted in Fig. 16. Alternatively, it is possible to use borrowed qubits (ancillary qubits which don't need to be initialized and are restored into their original state) as described in [56, Lemma 7.2]. Further intuition on how to build multiple-controlled-NOT gates can be found in [57]. As ancillary qubits are available at that point of the algorithm, we consider the successive Toffoli method presented in Fig. 16 for the resource evaluation.

The comparison operation between steps 2 and 3 (Fig. 15) is done with the circuit already presented in Fig. 4.

The controlled addition between steps 4 and 5 is performed according to Fig. 17, while the subtraction is obtained through the conjugation of this circuit. It is similar to Fig. 11 except that in Fig. 17, the controlled addition is performed modulo 2^n with n the number of qubits of the inputs. The desired addition between s and r is not modular, but we have proven by induction that at

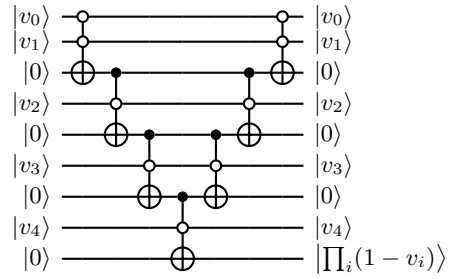


Figure 16. Multiple-controlled-NOT, with negative control. The small white circles designate controls on state $|0\rangle$.

the end of any iteration $s, r \leq p$ (except for r after the k th iteration, but the corresponding branch does not apply the addition to r). Given that s or r at the iteration i take the value of the sum $s + r$ at round $i - 1$, we conclude that $s + r \leq p < 2^n$. Although in Fig. 17 the addition and subtraction are performed modulo 2^n , we deduce that the properties of Algorithm 2 ensure that no overflow can occur.

The modular doubling applied to r once $v = 0$ in Fig. 15 is implemented with the scheme presented in Fig. 18.

After the circuit presented in Fig. 15 is repeated $2n$ times, the transformation $|r\rangle \mapsto |p - r\rangle$ is applied. The negation $r \mapsto -r$ is obtained by flipping each qubit and adding $+1$ (which is merged with the addition of p), as for a negation in two's complement. Given that p is a known integer, the addition is obtained by the semi-classical addition circuit presented in Fig. 19.

The $2n$ repetition of the circuit presented in Fig. 15 together with the transformation $|r\rangle \mapsto |p - r\rangle$ clarifies

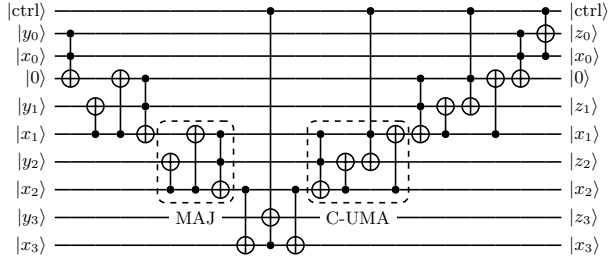


Figure 17. Controlled addition modulo 2^n . The output is $z = x + \text{ctrl}.y \bmod 2^n$, with n the number of bits in x and y ($n = 4$ here). MAJ and C-UMA operation are described in Fig. 11. MAJ and C-UMA are repeated as many times as required. Note that the controlled addition modulo 2^n is simplified compared with the controlled addition presented in Fig. 11 as it does not take an additional qubit for the output (the result of the desired sum is strictly smaller than 2^n) and the number of operations is reduced.

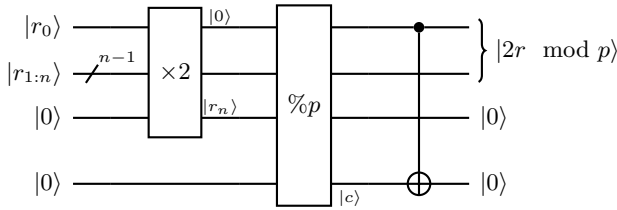


Figure 18. Doubling modulo p , with p odd. The multiplication by two is obtained by a simple register shift. The modular reduction, represented by $\%p$ operator is done according to Fig. 10, while the parity of the result is sufficient to uncompute the qubit $|c\rangle$ indicating if a reduction has been applied.

how to perform the inversion presented in [27, Fig. 6b]. Note that here we don't need to keep track of the current number of iterations i with a counter as together with f the values m_i are sufficient to ensure reversibility (to indicate if the iteration k has been reached) and the $2n$ repetition of the circuit in Fig. 15 ensures that the doubling is applied 2^{n-k} times. Further note that the modular multiplication by 2 is merged with the doubling required in the main branch (according to the proven bounds, the modular reduction can happen only once $v = 0$, thus the original algorithm is not disturbed). The comparison step is also simplified, as its result can be used before uncomputing the carries, by using a scheme similar with Fig. 4 (with use of the comparison result instead of using it for uncomputation).

6. Division

Following [27], a full out-of-place division $|x\rangle|y\rangle \mapsto |x\rangle|y\rangle|y/x \bmod p\rangle$ is obtained by combining the inver-

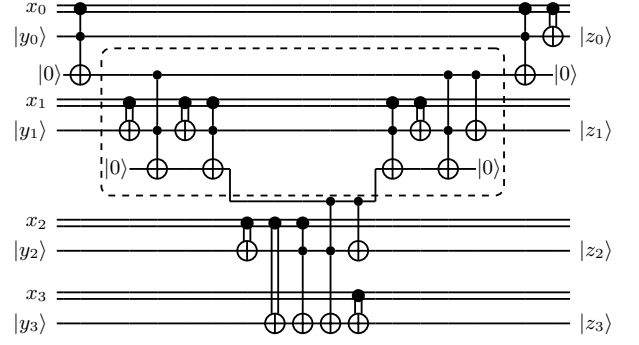


Figure 19. Semi-classical addition. The result is $z = x + y \bmod 2^n$ with n the number of bits in x and y . The boxed part computes the next carry, and then uncompute it while setting the result qubit to the appropriate value. It is repeated for each qubit, except the first and two last (special cases presented in the scheme).

sion and multiplication according to the following protocol

$$\begin{aligned}
 &|x\rangle|y\rangle|0\rangle|0\rangle|0\rangle|0\rangle \\
 &\xrightarrow{\text{inv}} |x^{-1}\rangle|y\rangle|0\rangle|0\rangle|0\rangle \left| \text{garbage}^{(x)} \right\rangle \\
 &\xrightarrow{\text{mul}} |x^{-1}\rangle|y\rangle|0\rangle|y/x\rangle \left| \text{garbage}^{(x^{-1},y)} \right\rangle \left| \text{garbage}^{(x)} \right\rangle \\
 &\xrightarrow{\text{copy}} |x^{-1}\rangle|y\rangle|y/x\rangle|y/x\rangle \left| \text{garbage}^{(x^{-1},y)} \right\rangle \left| \text{garbage}^{(x)} \right\rangle \\
 &\xrightarrow{\text{mul}^\dagger} |x^{-1}\rangle|y\rangle|y/x\rangle|0\rangle|0\rangle \left| \text{garbage}^{(x)} \right\rangle \\
 &\xrightarrow{\text{inv}^\dagger} |x\rangle|y\rangle|y/x\rangle|0\rangle|0\rangle|0\rangle
 \end{aligned}$$

where all the operations are modulo p , and all the numbers in Montgomery representation. Note that $|y/x\rangle$ is the step before the last one is the state of the copy register. $\left| \text{garbage}^{(x)} \right\rangle$ indicates garbage qubits created during the inversion of x (they depend on the value x), and $\left| \text{garbage}^{(x^{-1},y)} \right\rangle$ those generated by the multiplication of x^{-1} by y . The copy operation is done by applying for each qubit a CNOT gate targeting a qubit initialized in $|0\rangle$. At the end of the process, all ancillary qubits are restored to their initial state. A controlled version of the division is obtained by controlling the copy, hence changing the CNOT gates into Toffoli gates.

The reader might be interested to look at the circuit presented in [27, Fig. 8b] for an illustration of the division (note that the operation $\times 2^{2n-k}$ presented in [27, Fig. 8b] does not have to be applied since it is already included in the inversion).

7. Elliptic curve scalar multiplication

The elliptic curve scalar multiplication of an arbitrary integer k by an arbitrary point P is performed in a windowed manner, where k is stored in a quantum register and P is known in the classical control software. Writing n_e the number of bit in the multiplying factor k , we start with a decomposition of k into windows of w_e bits

$$k = \sum_{j \equiv 0 \pmod{w_e}}^{n_e} 2^j k_{j:j+w_e}.$$

where $k_{j:j+w_e}$ is the number composed of the w_e bits of k starting at index j (from least to most significant bits). Then we can decompose the multiplication operation into a sequence of additions

$$kP = \sum_{j \equiv 0 \pmod{w_e}}^{n_e} 2^j k_{j:j+w_e} P$$

hence the multiplication can be done with $\left\lceil \frac{n_e}{w_e} \right\rceil$ additions into an accumulation register of a point depending on $k_{j:j+w_e}$ loaded from the table associating $i \mapsto 2^j i P$, that contains 2^{w_e} different values. More precisely, $\left\lceil \frac{n_e}{w_e} \right\rceil$ additions from a table indexed by w_e qubits are required and eventually one addition from a smaller table indexed by $(n_e \bmod w_e)$ qubits.

An algorithm for performing elliptical curve addition between one point stored in a quantum register and one

point loaded from a table into another quantum register is required. The corresponding circuit is detailed in the following sub-section. Note that it is also possible to perform the elliptic curve scalar multiplication with controlled semi-classical elliptic curve additions, for details see [27, 32].

As the multiplication is performed with successive additions into an accumulation register, if the latter originally contains a point P_0 , the performed operation is $|k\rangle |P_0\rangle \mapsto |k\rangle |P_0 + kP\rangle$.

8. Elliptic curve addition

Here we detail how to add into a quantum register a point $P[i]$ loaded from a classical table $i \mapsto P[i]$, with an index i contained in a quantum register: $|i\rangle |Q\rangle \mapsto |i\rangle |Q + P[i]\rangle$, where Q is the point initially contained in the target register.

Following [32], we only implement the elliptic curve addition for the generic case, where the two points are distinct, not the inverse of each other and none is the neutral element. As detailed in [32], these exceptional cases happen in a negligible number unless the accumulation register is initialized in zero, which can be avoided by initializing the accumulation register with another point than the neutral element (which has no impact on the measurement statistics after the Fourier transform).

The addition $|i\rangle |Q\rangle \mapsto |i\rangle |Q + P[i]\rangle$ is realized with the following procedure

$$\begin{aligned}
& |i\rangle |x_Q\rangle |y_Q\rangle \xrightarrow{\text{lookup}} |i\rangle |x_Q\rangle |y_Q\rangle |x_{P[i]}\rangle |y_{P[i]}\rangle \\
& \xrightarrow{\text{substr}} |i\rangle |x_Q - x_{P[i]}\rangle |y_Q - y_{P[i]}\rangle |x_{P[i]}\rangle |y_{P[i]}\rangle \\
& \xrightarrow{\text{unlookup}} |i\rangle |x_Q - x_{P[i]}\rangle |y_Q - y_{P[i]}\rangle \\
& \xrightarrow{\text{div}} |i\rangle |x_Q - x_{P[i]}\rangle |y_Q - y_{P[i]}\rangle \left| \lambda = \frac{y_Q - y_{P[i]}}{x_Q - x_{P[i]}} \right\rangle \\
& \xrightarrow{\text{mul}^\dagger} |i\rangle |x_Q - x_{P[i]}\rangle |0 = (y_Q - y_{P[i]}) - \lambda \times (x_Q - x_{P[i]})\rangle |\lambda\rangle \\
& \xrightarrow{\text{lookup}} |i\rangle |x_Q - x_{P[i]}\rangle |0\rangle |\lambda\rangle |3x_{P[i]}\rangle \\
& \xrightarrow{\text{add}} |i\rangle |x_Q + 2x_{P[i]}\rangle |0\rangle |\lambda\rangle |3x_{P[i]}\rangle \\
& \xrightarrow{\text{unlookup}} |i\rangle |x_Q + 2x_{P[i]}\rangle |0\rangle |\lambda\rangle \\
& \xrightarrow{\text{square-}} |i\rangle |x_Q + 2x_{P[i]} - \lambda^2 = x_{P[i]} - x_{P[i]+Q}\rangle |0\rangle |\lambda\rangle \\
& \xrightarrow{\text{mul}} |i\rangle |x_{P[i]} - x_{P[i]+Q}\rangle |\lambda \times (x_{P[i]} - x_{P[i]+Q}) = y_{P[i]+Q} + y_{P[i]}\rangle |\lambda\rangle \\
& \xrightarrow{\text{div}^\dagger} |i\rangle |x_{P[i]} - x_{P[i]+Q}\rangle |y_{P[i]+Q} + y_{P[i]}\rangle \\
& \xrightarrow{\text{lookup}} |i\rangle |x_{P[i]} - x_{P[i]+Q}\rangle |y_{P[i]+Q} + y_{P[i]}\rangle |x_{P[i]}\rangle |y_{P[i]}\rangle \\
& \xrightarrow{\text{substr}} |i\rangle |-x_{P[i]+Q}\rangle |y_{P[i]+Q}\rangle |x_{P[i]}\rangle |y_{P[i]}\rangle \\
& \xrightarrow{\text{unlookup}} |i\rangle |-x_{P[i]+Q}\rangle |y_{P[i]+Q}\rangle \\
& \xrightarrow{\text{neg}} |i\rangle |x_{P[i]+Q}\rangle |y_{P[i]+Q}\rangle.
\end{aligned}$$

Each sub-operation has been previously described. Note that with the usage of the clean multiplication and division techniques previously presented (see [App. C 4](#) and [App. C 6](#)), no garbage qubits are created during the elliptic curve addition.

When used as a sub-operation of the elliptic curve scalar multiplication for the j th iteration, the specific choice $P[i] = iP2^j = iP'$ with $P' = 2^jP$ is made. This allows to use an additional improvement introduced in [27, Sec. 5.1]. The idea is to replace iP' by $(i - 2^{w_e-1})P'$, with the advantage of saving one bit for the control of each lookup, hence saving a factor 2 for the upper part of [Fig. 12](#). As this modification only subtracts the point $2^{w_e-1}P'$, independently of i , it introduces a bijection in the accumulation register that does not modify the interferences exploited by the quantum Fourier transforms. When $i \geq 2^{w_e-1}$, the most significant bit takes value 1 while the others encode the number $i - 2^{w_e-1}$, and using those qubits for controlling the table lookup operation allows loading the correct point. In the other case, $i < 2^{w_e-1}$ and the most significant bit takes value is 0. To prepare the correct point in this case, we start by applying the transformation $i \mapsto 2^{w_e-1} - i$, then use the same table lookup circuit as in the other case to load $(2^{w_e-1} - i)P'$, and change the sign of the y coordinate modulo p to negate the point and obtain $(i - 2^{w_e-1})P'$.

As i is stored in a quantum register, we distinguish the two cases by controlling the modular inversions by the most significant qubit (control on value $|0\rangle$). This improvement is taken into account in our resource estimation code [41].

9. Shor's algorithm

As detailed in [App. B](#), Shor's algorithm for computing the discrete logarithm of P in the cyclic group generated by G relies on the preparation of a superposition of all possible numbers in two registers, the computation of $f(x_1, x_2) = x_1G - x_2P$ (with x_1 and x_2 taken from the two registers) and a Fourier transform. The more expensive operation is the computation of $f(x_1, x_2)$, which is obtained according to the following procedure

$$\begin{aligned}
|x_1\rangle |x_2\rangle |P_0\rangle & \xrightarrow{\text{scal mult}} |x_1\rangle |x_2\rangle |P_0 + x_1G\rangle \\
& \xrightarrow{\text{scal mult}} |x_1\rangle |x_2\rangle |P_0 + x_1G + x_2(-P)\rangle
\end{aligned}$$

where the elliptic curve scalar multiplication implementation is detailed in [App. C 7](#).

Note that to correctly implement $f(x_1, x_2)$, P_0 should be chosen as the elliptic curve neutral element. However,

as detailed in App. C 8, it is preferable to take another value to avoid exceptional cases during the elliptic curve addition (as a translation as no influence on the outcome after the Fourier transform).

10. Gate count

In this subsection, we present an estimation of the number of CNOT and Toffoli gates in the implementation of elliptic curve discrete logarithm computation. To keep it simple, we show the dominant order in n (which is the number of bits in the prime p). Note, however, that the resource estimates given in the main text come from an exact resource estimation obtained via a numerical counting (the corresponding code is available at [41]).

Multiplication — The cost of Fig. 14 is asymptotically dominated by n controlled additions when the choice $w_m \sim \log_2(n)$ is made. Each addition implemented with Fig. 11 requires at the leading order $4n$ CNOT gates and $3n$ Toffoli. Hence, Montgomery multiplication uses essentially $4n^2$ CNOT gates and $3n^2$ Toffoli.

A clean multiplication is implemented by running the Montgomery multiplication, coping the result, and running the conjugate of Montgomery multiplication. Hence, it requires asymptotically $8n^2$ CNOT and $6n^2$ Toffoli. Note that the squaring operation (eventually including a subtraction) has the same asymptotic cost, *i.e.* it takes about $8n^2$ CNOT and $6n^2$ Toffoli.

Division — We start by evaluating the asymptotic number of gates involved in Fig. 15. The first step is a comparison with 0. When implemented according to Fig. 16, it uses $2n$ Toffoli gates. The comparison is implemented following Fig. 4 and uses $4n$ CNOT and $2n$ Toffoli. Each controlled swap (also known as Fredkin gate) can be implemented with 2 CNOT gates and 1 Toffoli [58]. Hence, a full register controlled swap involves $2n$ CNOT and n Toffoli. Each controlled addition or subtraction (Fig. 17) uses $4n$ CNOT and $3n$ Toffoli. The controlled division by two is obtained by repeating controlled swaps and costs $2n$ CNOT and n Toffoli. The modular multiplication by two (Fig. 18) is dominated by the modular reduction (Fig. 10), and uses asymptotically n CNOT and $3n$ Toffoli in average (we don't count the NOT gates). By summing those contributions, we conclude that Fig. 15 involves asymptotically $23n$ CNOT and $18n$ Toffoli gates.

The modular inversion is obtained by repeating $2n$ times the Fig. 15, hence it involves $46n^2$ CNOT and $36n^2$ Toffoli.

The division is obtained by running the inversion, a clean multiplication and the conjugate of the inversion. Hence, it involves $100n^2$ CNOT and $78n^2$ Toffoli gates.

Elliptic curve addition — In the elliptic curve addition protocol (with one point taken from a lookup circuit), only the two divisions, the two multiplications and the squaring contribute in the asymptotic cost (with the typical choice $w_e = \log_2(n)$ the table lookup does not contribute at the first order). Hence, it takes asymptotically $224n^2$ CNOT and $174n^2$ Toffoli gates. Note that the choice $w_e = \log_2(n)$ is illustrative, but not optimal (for instance $w_e = 2\log_2(n)$ is a better choice). In our analysis, the best value for w_e is automatically computed for a given n [41].

Discrete logarithm computation — As previously seen, the whole algorithm is dominated by the scalar multiplications on elliptic curve. For Shor's algorithm x_1 and x_2 have both typically $\approx n$ bits and the two elliptic curve multiplications are almost equivalent to a multiplication of a number containing $n_e \approx 2n$ bits, obtained from $\left\lceil \frac{n_e}{w_e} \right\rceil$ elliptic curve additions. Hence, the asymptotic number of gates for the whole algorithm is $448n^3/w_e$ CNOT and $348n^3/w_e$ Toffoli gates.

11. Qubit count

The maximum number of required logical qubits during the discrete logarithm computation is reached at the division step, and more exactly for the modular inversion.

w_e logical qubits are used for the current window of the scalar factor of the elliptic curve multiplication (written i in App. C 8). The two coordinates of the current point of the elliptic curve (x and y) each uses n logical qubits. The register associated to the slope (λ) also takes n logical qubits. To summarize, we need $3n + w_e$ logical qubits at this level.

In the modular inversion represented in Fig. 15 a , b and f use each one logical qubit, u , v , r and s are n qubits registers, and we need to store $2n$ different m_i values. At the first round the input is used as of v , so we don't count the corresponding qubits twice (it is an in-place inversion). Hence, the registers represented in Fig. 15 require $5n + 3$ additional qubits.

We also have to take into account the ancillary qubits used by the sub-operations of the inversion. The more demanding one is the modular multiplication by two, and more precisely the modular reduction. As shown in Fig. 18, the extension of r for the non-modular doubling

uses one qubit and another one is required for indicating if the reduction has been applied (c). The circuit shown in Fig. 10 uses by itself n ancillary qubits. Note that at this stage of the modular inversion, the register b is available and can be reused. Hence, the modular doubling adds $n + 1$ logical qubits to the count.

By summing up those numbers, we obtain that $9n + w_e + 4$ logical qubits are required for the elliptic curve logarithm computation. Note that by using a modular reduction based on the semi-classical adder involving only 2 ancillary qubits presented in [59], a reduction to $8n + w_e + 6$ logical qubits could be achieved.

Appendix D: Cat qubits, physical gates and noise models

1. Cat qubits

The cat qubit belongs to the family of bosonic qubits [60], for which quantum information is encoded in a subspace of the infinite dimensional Hilbert space of a quantum harmonic oscillator. The specific choice of the encoding is referred to as the bosonic code. The (two-component) cat code is defined by two coherent states of same amplitude and opposite phase $|\alpha\rangle$ and $|\alpha^*\rangle$ [14, 35], where α is assumed real without loss of generality. The amplitude of the cat is related to the average number of photons in the coherent state, $\langle \hat{a}^\dagger \hat{a} \rangle = \alpha^2$. An orthonormal basis for the computational subspace – the *codespace* – is the superpositions of these two states, the so-called Schrödinger cat states

$$\begin{aligned} |C_\alpha^+\rangle &= \frac{1}{\sqrt{2(1 + e^{-2\alpha^2})}}(|\alpha\rangle + |\alpha^*\rangle) \\ &= \frac{e^{-0.5\alpha^2}}{\sqrt{2(1 + e^{-2\alpha^2})}} \sum_n \frac{\alpha^{2n}}{\sqrt{(2n)!}} |2n\rangle \\ |C_\alpha^-\rangle &= \frac{1}{\sqrt{2(1 - e^{-2\alpha^2})}}(|\alpha\rangle - |\alpha^*\rangle) \\ &= \frac{e^{-0.5\alpha^2}}{\sqrt{2(1 - e^{-2\alpha^2})}} \sum_n \frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}} |2n+1\rangle, \end{aligned}$$

which are chosen to be the eigenstates of the Pauli X operator of the cat qubit with eigenvalues $+1$ and -1 , respectively (see Fig. 20). Note that the computational states $|0\rangle, |1\rangle$ are exponentially close (in α^2) to the coherent states $|\alpha\rangle, |\alpha^*\rangle$ as the normalization factor of the superpositions of coherent states are not exactly identical. To ensure the state of the quantum harmonic oscillator remains in the code space throughout the computation, a stabilization mechanism is required. In the case of cat

qubits, this stabilization is realized by implementing a two-photon dissipation [36, 37, 61, 62] modelled by the Lindblad master equation

$$\dot{\rho} = \kappa_2 \mathcal{D}[\hat{a}^2 - \alpha^2] \rho \quad (\text{D1})$$

where the superoperator \mathcal{D} is given by

$$\mathcal{D}[\hat{L}] \bullet = \hat{L} \bullet \hat{L}^\dagger - \frac{1}{2} \hat{L}^\dagger \hat{L} \bullet - \frac{1}{2} \bullet \hat{L}^\dagger \hat{L}$$

and κ_2 is the rate of the engineered two-photon dissipation.

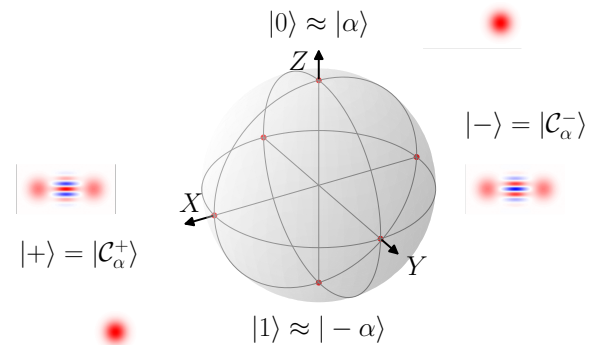


Figure 20. Bloch sphere representation of a cat qubit.

A major interest of cat qubits lies in the bias of the noise: when the stabilization rate is higher than that of typical errors, the bit-flip error rate induced by the errors of the quantum harmonic oscillator (single photon loss, thermal excitations, dephasing, *etc.*) is exponentially suppressed with the mean number of photon in the cat size $\gamma_X \propto \exp(-2\alpha^2)$, while the phase-flip error rate typically scales linearly $\gamma_Z \propto \alpha^2$ [36, 37]. As a result, even for moderate cat sizes, the noise bias γ_Z/γ_X of the cat qubit can be extremely large.

A large noise bias is a highly desirable feature for quantum error correction [13, 63, 64], lowering the requirements on the fault-tolerance threshold, and many recent works have been addressing how to best tailor the codes to leverage the noise bias [65–67]. In this work, we assume that the exponential suppression of bit-flips in the cat qubits will be sufficient to produce extremely low bit-flip error rate, such that the quantum error correcting code can be used to correct phase-flip errors only [17, 38]. In practice however, this assumption may not be realistic, as there could be error mechanisms causing the exponential suppression of bit-flips to saturate for some photon number, as has been typically observed experimentally [36, 37]. Thus, it may be required in practice to use a code that can correct for a certain amount of bit-flips, such as a thin rectangular surface code [38], but quantifying precisely the extra-overhead induced in this

case is beyond the scope of this work (we however provide a rough estimate of this overhead in App. F). In the two next paragraphs, we recall for self-completeness the physical implementations of operations on cat qubits. A thorough discussion of the code operation can be found in [17, 38].

2. Physical realization of cat qubits with superconducting circuits

The physical platform considered in this work for the realization of cat qubits is superconducting circuits in the context of circuit quantum electrodynamics (cQED) [68, 69]. The bosonic mode used to store quantum information is a mode of a superconducting co-planar waveguide microwave resonator or of a three-dimensional microwave cavity. The resonators are typically realized using a superconducting material like aluminium or niobium on a dielectric substrate, usually sapphire or silicon. To operate microwave resonators in the quantum regime, the chips are cooled at a temperature around 10 mK in dilution refrigerators.

Universal bosonic quantum information processing requires non-linear dynamics. In circuit QED, this non-linearity is inherited from the Josephson junction, a non-dissipative non-linear circuit element. The Hamiltonian of a Josephson junction is given by $\hat{H} = -E_J \cos(\hat{\varphi})$ where $\hat{\varphi}$ is the phase of the superconducting order parameter across the junction.

The non-linear dynamics required to stabilize cat qubits and process quantum information are realized using the mixing capabilities of the Josephson junction [70]. In practice, a cat qubit processor is made of many (linear) bosonic modes hosting the cat qubits; coupled together using non-linear circuit elements built from Josephson junctions. Quantum information processing is carried out using the non-linear wave-mixing capabilities of Josephson junctions, via the activation of parametric microwave drives and pumps at well-chosen frequencies.

We now briefly illustrate these principles by focusing on the realization of the two-photon dissipation $\mathcal{D}[\hat{a}^2]$, following closely the derivation given in [36]. The realization of this dissipation has been demonstrated experimentally in [36, 61, 62]. For detailed derivations of more complex operations (weak Hamiltonians required for the Zeno gates [62] and topological gates), we refer the reader to [17, 38].

To realize this dissipation on a high-Q mode \hat{a} , called the *memory mode*, a dissipative (low-Q) auxiliary mode \hat{b}

called the *buffer mode* is required. The memory and the buffer mode are coupled using a non-linear circuit element. In the first experimental realizations of cat qubits, this non-linear circuit element was a simple Josephson junction [61, 62]. Later, a more refined circuit containing more Josephson junctions called the Asymmetrically Threaded SQUID (ATS) [36] was used. The advantage of this more elaborate circuit is that it allows to engineer the desired two-to-one photon conversion without the creation of many spurious terms that spoil the cat qubit. The first experimental demonstration of the exponential suppression of bit-flips was realized using this circuit, which is why we illustrate the principles using this specific realization, as depicted in Fig. 21. An ATS is a SQUID shunted in its center by a large inductance, thus forming two loops with flux $\varphi_{\text{ext},1}$ and $\varphi_{\text{ext},2}$. Its potential energy is a function of the phase φ across the inductor

$$U(\varphi) = \frac{1}{2} E_{L,b} \varphi^2 - E_{J,1} \cos(\varphi + \varphi_{\text{ext},1}) - E_{J,2} \cos(\varphi + \varphi_{\text{ext},2}). \quad (\text{D2})$$

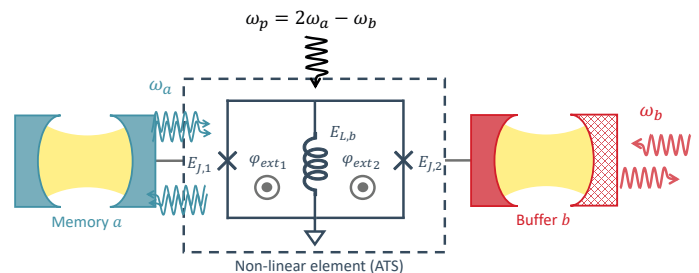


Figure 21. The cat qubit memory (blue) is coupled to the buffer (red). Pumping the ATS at frequency $\omega_p = 2\omega_a - \omega_b$ (black arrow), where ω_a and ω_b are the cat qubit and buffer frequencies, activates the conversion of two photons of the cat qubit (blue arrows) into one photon of the buffer (red arrows) and one photon of the pump, and vice-versa.

By writing the half-sum $\varphi_\Sigma = \frac{1}{2}(\varphi_{\text{ext},1} + \varphi_{\text{ext},2})$ and the half-difference $\varphi_\Delta = \frac{1}{2}(\varphi_{\text{ext},1} - \varphi_{\text{ext},2})$ and setting them such that $\varphi_\Delta = \pi/2 + \epsilon(t) = \pi/2 + \epsilon_0 \cos(\omega_p t)$ and $\varphi_\Sigma = \pi/2$ with ϵ_0 small, and assuming $E_{J,1} = E_{J,2} = E_J$, the time-dependent potential energy becomes

$$U(\varphi) = \frac{1}{2} E_{L,b} \varphi^2 - 2E_J \epsilon(t) \sin(\varphi). \quad (\text{D3})$$

The non-linear coupling of the memory mode \hat{a} to the buffer mode \hat{b} by an ATS is described by the Hamiltonian ($\hbar = 1$)

$$\hat{H} = \omega_{a,0} \hat{a}^\dagger \hat{a} + \omega_{b,0} \hat{b}^\dagger \hat{b} - 2E_J \epsilon(t) \sin(\hat{\varphi}_a + \hat{\varphi}_b)$$

where $\omega_{a/b,0}$ are the bare resonance frequencies of the modes, $\hat{\varphi}_a = \varphi_a(\hat{a} + \hat{a}^\dagger)$, $\hat{\varphi}_b = \varphi_b(\hat{b} + \hat{b}^\dagger)$ and $\varphi_{a,b}$ are

the zero point fluctuations of the modes across the ATS dipole, related to the geometry of the circuit.

Setting the pump frequency to be $\omega_p = 2\omega_a - \omega_b$, where $\omega_{a,b}$ are the renormalized (AC-Stark shifted) frequencies of the mode due to the presence of the pump, expanding the sine in Eq. (D2) up to third order, and neglecting the fast-oscillating terms (the so-called RWA approximation), one finds[36] that the above Hamiltonian reduces to

$$\hat{H} = g_2^* \hat{a}^2 \hat{b}^\dagger + g_2 \hat{a}^{\dagger 2} \hat{b}$$

where $g_2 = E_J \epsilon_0 \varphi_a^2 \varphi_b / 2$. Finally, the buffer mode \hat{b} being highly dissipative, its fast relaxation dynamics can be adiabatically eliminated to obtain an effective single-mode description of the slower dynamics induced on the memory mode, which takes the form of the effective two-photon dissipation $\mathcal{D}[\hat{a}^2]$.

These principles can be used to implement all the pieces of dynamics of the next subsection. By using resonant pumps at well-chosen frequencies, one can parametrically engineer more complex interaction Hamiltonians to perform gates on the cat qubits [17, 38].

3. Physical gates on cat qubits

The architecture relies by design on the noise bias of the cat qubit. It is thus of crucial importance to maintain this bias in the noise, even during the execution of the gates. Operations that preserve the noise bias are called bias-preserving, and only such operations may be used at the physical level.

State preparation and measurement — The eigenstates of the X operator having a well-defined photon-number parity, $(-1)^{\hat{a}^\dagger \hat{a}} |\mathcal{C}_\alpha^\pm\rangle = \pm |\mathcal{C}_\alpha^\pm\rangle$, the measurement of X can be realized with a photon-number parity measurement, routinely achieved in circuit QED [71]. The preparation of $|\mathcal{C}_\alpha^+\rangle$ may be simply realized by preparing the oscillator in the vacuum state and by turning on the cat qubit stabilization. Alternatively, a faster state preparation can be realized using optimal control. The Z measurement distinguishes the coherent states $|\pm\alpha\rangle$, which can be done *e.g.* with a homodyne measurement. The eigenstates of the Z operator $|\pm\alpha\rangle$ can be reliably prepared by applying a strong resonant microwave pulse to the oscillator prepared in the vacuum state to displace the oscillator and by turning on the stabilization immediately after the displacement.

Single qubit gates — The implementation of the single qubit Z gate is realized using the quantum Zeno effect, by applying a weak resonant drive of complex amplitude ϵ_Z to the cat qubit in presence of the stabilization (at rate $\kappa_2 \gg |\epsilon_Z|$), as was first proposed in [14]. The dynamics implementing this gate is modelled by the master equation

$$\dot{\rho} = -i[\epsilon_Z \hat{a} + \epsilon_Z^* \hat{a}^\dagger, \rho] + \kappa_2 \mathcal{D}[\hat{a}^2 - \alpha^2] \rho. \quad (\text{D4})$$

A π -rotation around the Z axis is realized in time $T = \pi/[4\alpha \text{Re}(\epsilon_Z)]$. Note that arbitrary rotations around the Z -axis $Z(\theta)$ can be realized using this implementation, giving access to interesting gates (S gate for $\theta = \pi/2$, T gate for $\pi/4$); but it is not clear how to use these gates at the logical level.

The implementation of the X gate is realized by making the two-photon stabilization time-dependent,

$$\kappa_2 \mathcal{D}[\hat{a}^2 - \alpha^2] \rightarrow \kappa_2 \mathcal{D}[\hat{a}^2 - (\alpha e^{i\pi t/T})^2] \quad (\text{D5})$$

such that the two states $|\pm\alpha\rangle$ are swapped adiabatically. Note that the fact that the X gate can be implemented in a bias-preserving manner may be counter-intuitive at first sight. Indeed, as noted in [12] in the case of regular qubits (two-level systems), it may be natural to assume that the imperfections of the physical process implementing the X will lead to an X component in the error model of the gate, *e.g.* if a slight over or under rotation is implemented, the corresponding error should have an X component. Indeed, in the case of regular two-level systems, it has been shown [17] that it is impossible to implement an X gate in a bias-preserving manner on two-level systems. In the case of cat qubits, the bias-preserving implementation is possible by exploiting the infinite dimensional Hilbert space of the underlying harmonic oscillator to implement a continuous code deformation.

The fully dissipative implementation of Eq. (D5) needs to be adiabatic with respect to the dissipative time-scale κ_2^{-1} . As a consequence, this may lead to low fidelity gates as the cat qubit suffers from decoherence during the execution of the gate. To accelerate the gate, a “feedforward” Hamiltonian $\hat{H}_X = -\pi/T \hat{a}^\dagger \hat{a}$ can be added. The role of this Hamiltonian is to ensure that the state of the quantum harmonic oscillator remains in the code space during the gate, instead of relying only on the dissipative stabilization. Loosely speaking, in presence of this Hamiltonian, the role of the dissipative stabilization is no longer to “drag” the quantum state to implement the gate but merely to ensure that the errors do not distort the state, while the actual dynamics implementing the gate is realized by the Hamiltonian part of the dynamics.

CNOT gate — Combining the ideas of the X gate and the Z gate, the CNOT gate is realized by making the rotation of the pumping of the target qubit implementing the X gate that depends on the state of the control qubit, by modifying the dissipative stabilization channels of the control cat qubit $\mathcal{L}_{\hat{a}} = \kappa_2 \mathcal{D}[L_{\hat{a}}]$ and target cat qubit $\mathcal{L}_{\hat{b}} = \kappa_2 \mathcal{D}[L_{\hat{b}}(t)]$ respectively as

$$\hat{L}_{\hat{a}} = \hat{a}^2 - \alpha^2 \quad (\text{D6a})$$

$$\hat{L}_{\hat{b}}(t) = \hat{b}^2 - \frac{1}{2}\alpha(\hat{a} + \alpha) + \frac{1}{2}\alpha e^{2i\frac{\pi}{T}t}(\hat{a} - \alpha) \quad (\text{D6b})$$

where \hat{a} and \hat{b} denote the annihilation operators of the control and target cat qubit respectively, and T denotes the CNOT gate time. Similarly to the case of the X gate, the gate speed can be dramatically increased, thus leading to higher gate fidelity, by adding a “longitudinal coupling” Hamiltonian $\hat{H}_{CX} = \frac{\pi}{4\alpha T}(\hat{a} + \hat{a}^\dagger - 2\alpha)(\hat{b}^\dagger \hat{b} - \alpha^2)$ to the gate dynamics.

Toffoli gate — Finally, the CNOT gate can be generalized to a Toffoli gate by adding another control cat qubit. The dynamics implementing the adiabatic Toffoli gate is realized with the stabilization channels $\mathcal{L}_{\hat{a}} = \kappa_2 \mathcal{D}[L_{\hat{a}}]$, $\mathcal{L}_{\hat{b}} = \kappa_2 \mathcal{D}[L_{\hat{b}}]$, $\mathcal{L}_{\hat{c}} = \kappa_2 \mathcal{D}[L_{\hat{c}}(t)]$ (respectively the first control, the second control and the target)

$$\hat{L}_{\hat{a}} = \hat{a}^2 - \alpha^2 \quad (\text{D7a})$$

$$\hat{L}_{\hat{b}} = \hat{b}^2 - \alpha^2 \quad (\text{D7b})$$

$$\begin{aligned} \hat{L}_{\hat{c}}(t) = & \hat{c}^2 - \frac{1}{4}(\hat{a} + \alpha)(\hat{b} + \alpha) + \frac{1}{4}(\hat{a} + \alpha)(\hat{b} - \alpha) \\ & + \frac{1}{4}(\hat{a} - \alpha)(\hat{b} + \alpha) - \frac{1}{4}e^{2i\frac{\pi}{T}t}(\hat{a} - \alpha)(\hat{b} - \alpha), \end{aligned} \quad (\text{D7c})$$

together with the Hamiltonian $\hat{H}_{CCX} = \frac{\pi}{16\alpha^2 T}(\hat{a} + \hat{a}^\dagger - 2\alpha)(\hat{b} + \hat{b}^\dagger - 2\alpha)(\hat{c}^\dagger \hat{c} - \alpha^2)$.

4. Physical noise model

We now detail the error models associated with the physical implementations of the gates described above, with errors coming from two different sources: the single photon loss of the quantum harmonic oscillator at a rate κ_1 , and the non-adiabaticity of the gates.

Physical phase-flip errors — Using the “shifted Fock basis”, a subsystem decomposition of the quantum harmonic oscillator well suited to the cat qubit encoding [38], the (dominant) phase-flip error probabilities of the single and multi-qubit gates can be obtained analytically. The corresponding Pauli error model is summarized in [Table I](#). Because the phase-flip errors induced by the natural losses of the quantum harmonic oscillator increase with the gate time, while the phase-flip errors induced by

$\alpha^2 = 19, \kappa_1/\kappa_2 = 10^{-5}$		
$\mathcal{P}_{ +\rangle}$		$T_{\text{prep}} = 1/\kappa_2$
$1 - \mathcal{F}$	$\alpha^2 \kappa_1 T_{\text{prep}}$	1.9×10^{-4}
\mathcal{M}_X		$T_{\text{meas}} = 1/\kappa_2$
$1 - \mathcal{F}$	$\alpha^2 \kappa_1 T_{\text{meas}}$	1.9×10^{-4}
CX		$T_{CX} = 1/\kappa_2$
$1 - \mathcal{F}$		8.4×10^{-3}
Z_1	$\alpha^2 \kappa_1 T_{CX} + \frac{\pi^2}{64\alpha^2 \kappa_2 T_{CX}}$	8.3×10^{-3}
$Z_2 = Z_1 Z_2$	$\frac{1}{2}\alpha^2 \kappa_1 T_{CX}$	9.5×10^{-5}

Table I. Pauli phase-flip error models used in this section. For the dissipative implementations considered in this work, we summarize the analytical errors models derived in [38]. The equalities in the left column, *e.g.* $Z_2 = Z_1 Z_2$, means that these errors occur with equal probability.

non-adiabaticity decrease with the gate time, the combination of these two sources of errors gives rise to an optimal finite gate time that minimizes the phase-flip errors.

As previously discussed [17, 38], the timescale $1/\kappa_2$ sets the typical time of quantum operations on a cat qubit, and hence the clock cycle time of the architecture, and the ratio κ_1/κ_2 sets the typical fidelity of quantum operations. For the specific value of $\kappa_1/\kappa_2 = 10^{-5}$ considered here, and an average number of photons $\alpha^2 = 19$, we obtain a total state preparation and measurement error probability of $p_{\text{SPAM}} = p_{\text{prep}} + p_{\text{meas}} = 3.8 \times 10^{-4}$ and a CNOT gate infidelity of 8.4×10^{-3} . The noise model associated to the Toffoli gate is later described in [Table II](#).

Note that the CNOT gate time $T_{CX} = 1/\kappa_2$ is sub-optimal for the gate fidelity, but nonetheless achieves a lower repetition code cycle error rate. This somewhat counter-intuitive fact is detailed in the recent work [40].

Physical bit-flip errors — In order to estimate the (exponentially suppressed) physical bit-flip error probability, we perform numerical process tomography of all the gates described in [App. D](#), at the exception of the CCX gate. Indeed, resolving accurately the bit-flip error probability requires to simulate the gate over a typical range of photon number $\alpha^2 = 2 - 10$ photons, and to use an appropriate truncation in the Fock basis. The current simulation method does not allow to perform a sufficiently accurate simulation of the 3-mode CCX gate due to the size of the Hilbert space required for the simulation to converge. We thus assume that the bit-flip error rate of the CCX gate to be similar to that of the CNOT gate.

We find that, while all operations have a bit-flip error probability scaling as $e^{-2\alpha^2}$, the operation that dominates the physical bit-flip error probability is the CNOT

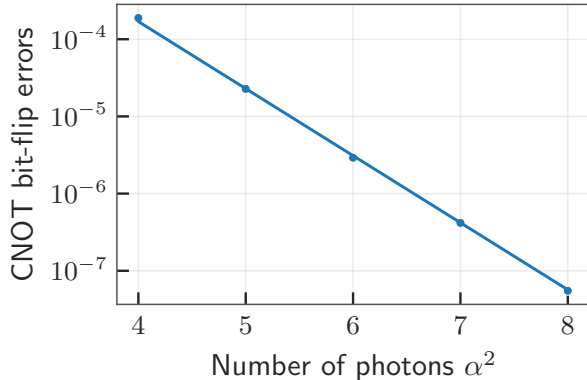


Figure 22. Total bit-flip error probability induced during the implementation of a CNOT gate versus the average photon number of the cat qubit, obtained through a numerical process tomography of Eq. (D6).

gate. Due to the fast implementation of this gate, we find that the dominant bit-flips are those induced by non-adiabaticity. We numerically estimate the value of the bit-flips errors by performing a full process tomography [58] of the dynamics implementing a CNOT gate. The sum of the probabilities of all the 12 bit-flip type errors (*e.g.* X_1 , $Z_1 \otimes Y_2$, *etc.*) is depicted in Fig. 22. To extrapolate to larger number of photons, we fit this curve and find

$$p_X^{CX} = 0.50e^{-2\alpha^2}. \quad (\text{D8})$$

Appendix E: Repetition code operation

In this appendix, we detail the architecture of our cat qubit quantum computer at the logical (repetition code) level.

1. Architecture

With currently available technology, cat qubits can only be built with planar connections. However, it is convenient to benefit from an all-to-all connectivity between the logical qubits, as it prevents proliferation of logical swaps. This is achieved by laying the physical qubits as presented in Fig. 24. The proposed architecture consists in organizing data busses for applying 2-qubit gates through lattice surgery. Each logical qubit corresponds

to a horizontal line of data qubits, and ancillary qubits between them allow the measurements of the code stabilizers. To apply CNOT gates between far away logical qubits with lattice surgery, the logical qubits are accessed through the routing qubits either on their extremity or with each of its physical qubits involved. Toffoli gate is realized by preparation of a magical state in a dedicated factory (yellow) and by a teleportation, that requires only 2-qubit gates as detailed in App. E 4.

For a code distance d , each logical qubit requires d physical qubits for the data and $d - 1$ for the ancillary qubits that allow measurements of the stabilizers. Each magical state factory involves 4 logical qubits; we adjust the number of magical state factory to deliver the states at a similar speed at which they can be consumed (we do not consider any parallelization, but ensure to have in average one magical state ready for each time interval corresponding to a gate teleportation). With nb_{log} and $\text{nb}_{\text{factory}}$ respectively the numbers of logical qubits and factories, we count $\text{nb}_{\text{rout}} = \lceil (\text{nb}_{\text{log}} + \text{nb}_{\text{factory}})/2 \rceil + 1$ horizontal lines of routing qubits. On each side, there is $3(\text{nb}_{\text{log}} + \text{nb}_{\text{rout}} + 4\text{nb}_{\text{factory}}) - 1$ additional routing qubits, including the corresponding ancillaries. Those numbers are added in the code used to evaluate the resources [41].

Note that with the proposed architecture only up to two CNOT gates can be realized in parallel. Large parallelization would require modifications, for instance by placing the logical qubits on several columns, as considered for surface codes [72–74].

2. Repetition code performance

In this work, we follow [17, 38] and assume that the bit-flip error rate can be made sufficiently low to run large-scale algorithms while relying only on a simple repetition code against phase-flip to produce a logical qubit. The logical $|+\rangle_L$ and $|-\rangle_L$ states of a distance- d repetition code are $|\pm\rangle_L := |\pm\rangle^{\otimes d} = |\mathcal{C}_\alpha^\pm\rangle^{\otimes d}$. Note that the logical $|0/1\rangle_L = \frac{1}{\sqrt{2}}(|+\rangle_L \pm |-\rangle_L)$ state corresponds to the equal superposition of all the 2^{d-1} states that have an even/odd number of $|1\rangle$ states. The $d - 1$ stabilizers of the code $S_i = X_i X_{i+1}$ can be measured using bias-preserving operations $\mathcal{P}_{|+\rangle}$, CNOT, \mathcal{M}_X .

We now detail how logical error models (at the level of the repetition code) can be obtained from the physical error models described in App. D 4, beginning this subsection with the repetition code error rates (memory). Here, we follow the recent proposal [40] that optimizes the repetition code performance. We proceed in two-steps: as

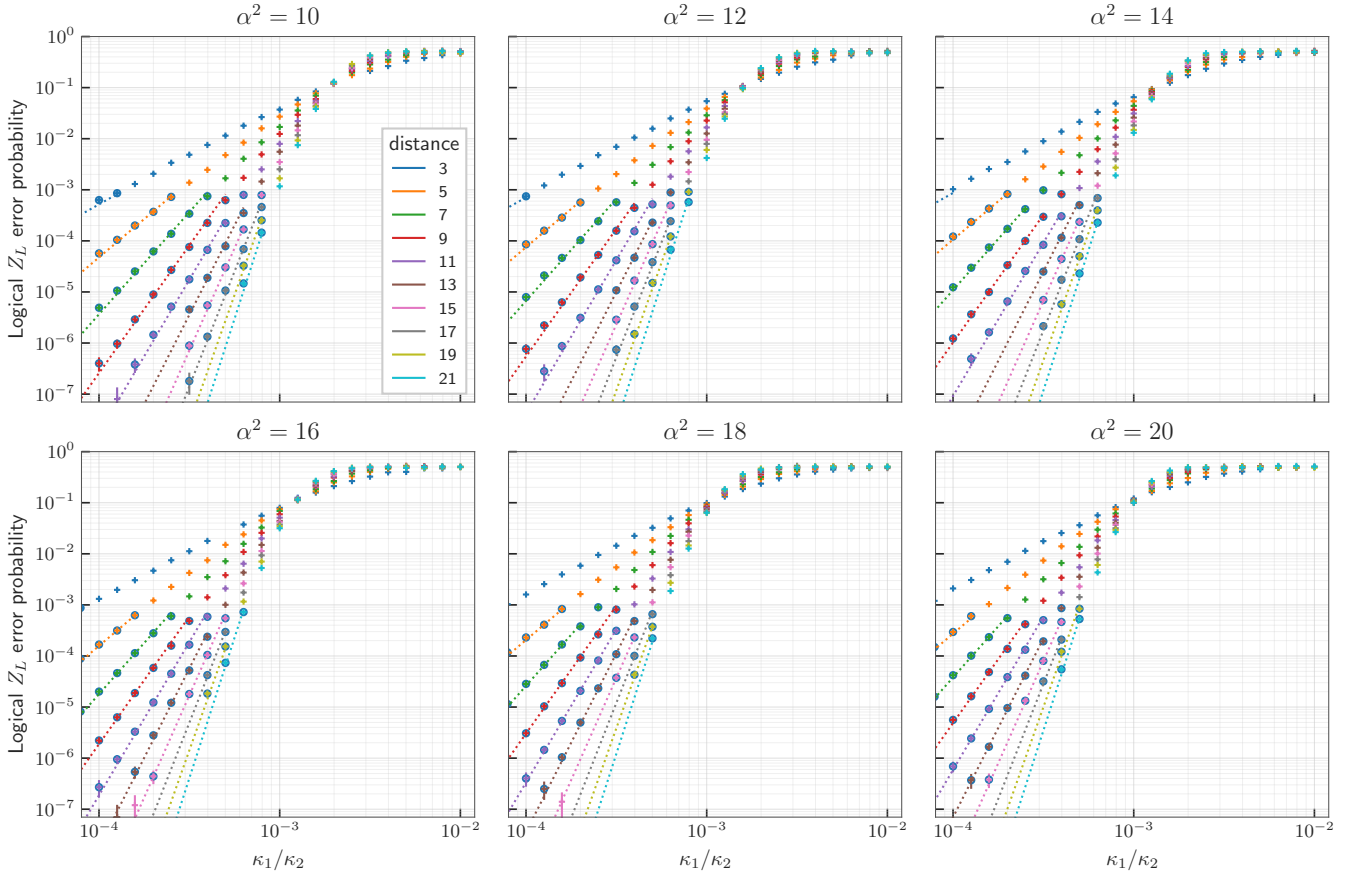


Figure 23. Logical phase-flip error probability for various values of the average photon number α^2 , calculated using Monte Carlo sampling of the repetition code circuit under circuit-level noise. The error bars display the statistical error. The dotted lines correspond to a leading order fit in the regime where errors are sparse, $\kappa_1/\kappa_2 \ll 1$, the data points used in the fit are circled.

the repetition code only corrects for phase-flip, we estimate the logical phase-flip error probability p_{Z_L} and the logical bit-flip error probability p_{X_L} separately, and the logical error rate is then estimated as $\epsilon_L = p_{Z_L} + p_{X_L}$.

Logical phase-flip — The logical phase-flip error probability is numerically estimated using circuit-level noise simulations of the repetition code circuit, where every operation in the circuit (including idle locations) is noisy. More precisely, every noisy operation is modelled as a perfect operation followed by the stochastic application of a Pauli phase-flip noise model, given in Table I. For the value of $\kappa_1/\kappa_2 = 10^{-5}$ and $\alpha^2 = 19$ considered in the main text, this translates to a preparation and measurement infidelity of $p_{\text{prep}} = p_{\text{prep}} = 1.9 \times 10^{-4}$, and a CNOT gate infidelity of $p_{\text{CX}} = 8.4 \times 10^{-3}$. To estimate the per cycle logical phase-flip error rate, the state of the circuit is initialized in $|+\rangle_L$, and the stabilizers are measured d times, followed by a final perfect round of stabilizer measurements. This final perfect round of stabilizer measurements emulates the fact that, in prac-

tice, the measurement of the stabilizers continues. This ensures the convergence of the decoding algorithm as if the data were buried under additional data as the processor keeps running. The estimate of the per cycle logical error rate is accurate as long as the temporal window used in the simulation (here, d code cycles) is sufficiently long [75]. Note that, at the end of the quantum algorithm, the data qubits are measured, and the finale value of the stabilizers may be inferred from this measurement. The history of syndrome outcomes is decoded using the open source minimum-weight perfect matching decoder pyMatching [76]. Decoding the syndromes yields the correction to apply to the state. If the state after (perfect correction) is $|+\rangle_L$, the quantum error correction circuit correctly interpreted the errors that occurred, while if the state after correction is $|-\rangle_L$, a logical phase-flip error Z_L occurred.

The probability of such a failure is then estimated by repeating the above procedure, and is depicted in Fig. 23 for various values of κ_1/κ_2 , average photon number α^2

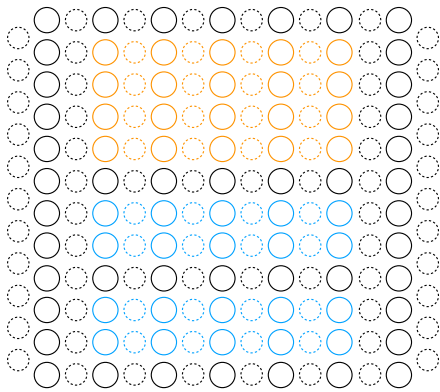


Figure 24. Architecture for a quantum processor using cat qubits, with 4 logical qubits and a code distance of 5. The data qubits are in plain line, the ancilla qubits are dashed, the qubits used to perform the computation are in blue, the qubits used in the magic state factory are orange, and the routing qubits are black.

and code distance d . In the regime where errors are rare, $\kappa_1/\kappa_2 \ll 1$, we expect the logical error rate to be dominated by the contributions of trajectories where exactly $(d+1)/2$ errors occurred (as any combination of less than $(d+1)/2$ errors cannot lead to a logical error, and combinations of more than $(d+1)/2$ errors are unlikely to occur in this regime). Thus, we fit the logical error probability after d rounds of stabilizer measurements to the ansatz

$$p_{Z_L} = A(\alpha^2) d \left(\frac{\kappa_1/\kappa_2}{(\kappa_1/\kappa_2)_{\text{th}}(\alpha^2)} \right)^{\frac{d+1}{2}}. \quad (\text{E1})$$

We find numerically (see Fig. 25) that $A(\alpha^2)$ is independent of α^2 , $A(\alpha^2) \approx 5.6 \times 10^{-2}$, and $(\kappa_1/\kappa_2)_{\text{th}}(\alpha^2)$ is well approximated by

$$(\kappa_1/\kappa_2)_{\text{th}}(\alpha^2) = \frac{1.3 \times 10^{-2}}{(\alpha^2)^{0.86}}.$$

We interpret the fact that $(\kappa_1/\kappa_2)_{\text{th}}(\alpha^2)$ is not exactly inversely proportional to α^2 as the effect of non-adiabatic (measurement) errors on the control. Indeed, in the absence of such errors, the only source of errors considered in our model is the single-photon loss which scales linearly with α^2 , which would produce a threshold inversely proportional to α^2 .

Logical bit-flip — From the characterization of the physical bit-flip error probabilities in App. D 4, dominated by the bit-flip errors induced by the CNOT gate, we estimate the probability of logical bit-flip error per repetition code cycle to be $p_{X_L} = n_{\text{CX}} \times p_X^{\text{CX}} = 2(d-1) \times 0.50e^{-2\alpha^2}$, where n_{CX} is the number of CNOT gates in a repetition code cycle.

Repetition code performance — Taking into account both errors, the per cycle error probability of the repetition code is given by (presented as Eq. (3) in main text)

$$\epsilon_L = 5.6 \times 10^{-2} \left(\frac{(\alpha^2)^{0.86} \kappa_1/\kappa_2}{(\kappa_1/\kappa_2)_{\text{th}}} \right)^{\frac{d+1}{2}} + 2(d-1) \times 0.50e^{-2\alpha^2}$$

with $(\kappa_1/\kappa_2)_{\text{th}} = 1.3 \times 10^{-2}$.

Note that this architecture does not have a threshold, as for any finite value of the noise κ_1/κ_2 , there is an optimal value for the mean number of photons α^2 and the repetition code distance d that minimizes the logical error rate. However, in this work we argue that the absence of a threshold may not be problematic as long as the minimal error rate that can be achieved is sufficiently low for the targeted algorithm.

3. Transversal logical gates implementation

We now show how the logical operations of the set $\{\mathcal{P}_{|+\rangle_L}, \mathcal{P}_{|0\rangle_L}, \mathcal{M}_{Z_L}, \mathcal{M}_{X_L}, Z_L, X_L, CX_L^k\}$ can be implemented on the repetition code, postponing the more involved implementation of the CCX_L gate to the next subsection.

Note that the logical gate CX_L^k is not required for universality as it can be synthesized from CX_L gates, but here we show how it can be directly implemented as it is widely used in the table lookup circuit (Fig. 12).

All of the operations in $\mathcal{S}_L = \{\mathcal{P}_{|+\rangle_L}, \mathcal{P}_{|0\rangle_L}, \mathcal{M}_{Z_L}, \mathcal{M}_{X_L}, Z_L, X_L, CX_L^k, CCX_L\}$ can be implemented transversally on the repetition code, except for the CCX_L gate, the implementation of the latter being discussed in the next subsection.

State preparation, measurement, and Pauli gates — The fault-tolerant preparation of $|+\rangle_L$ and $|0\rangle_L$ are realized by preparing the product states $|+\rangle^{\otimes d}$ and $|0\rangle^{\otimes d}$, respectively, followed by d rounds of stabilizer measurements, decoding and correction. This logical state preparation scheme is standard for stabilizer codes (see e.g. [10, 77]). The fault-tolerant measurement of X_L , denoted \mathcal{M}_{X_L} , is realized by measuring all the data qubits of the code in the X basis, followed by a majority vote on the measurement outcomes. Note that in principle, the value of the logical operator X_L can be read out on any data qubit of the code, but this is not fault-tolerant. The measurement of the logical Z_L operator, denoted \mathcal{M}_{Z_L} , is realized by measuring all the data qubits in the Z basis and by taking the product of all the measurement outcomes. The logical X_L gate is implemented by

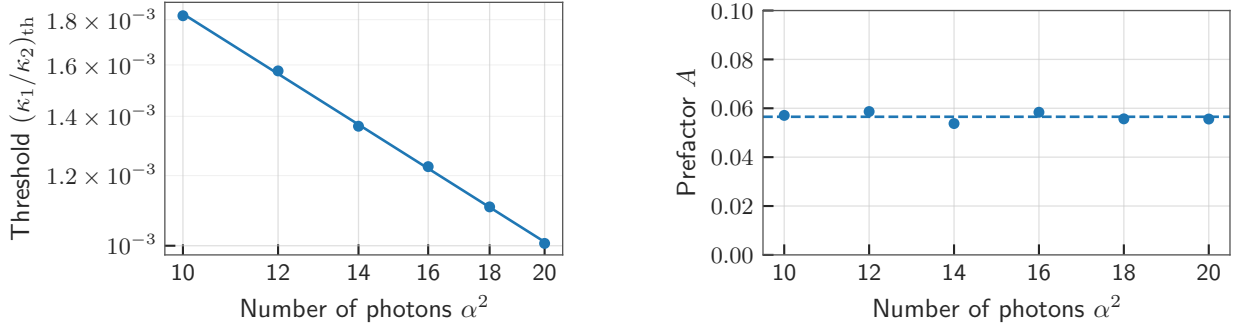


Figure 25. Numerical fit of the prefactor and value of the threshold in Eq. (E1). We find that the prefactor is independent of α^2 , while the threshold decreases almost linearly with α^2 , as one expects from the fact that the photon-loss induced phase-flips increase linearly with α^2 .

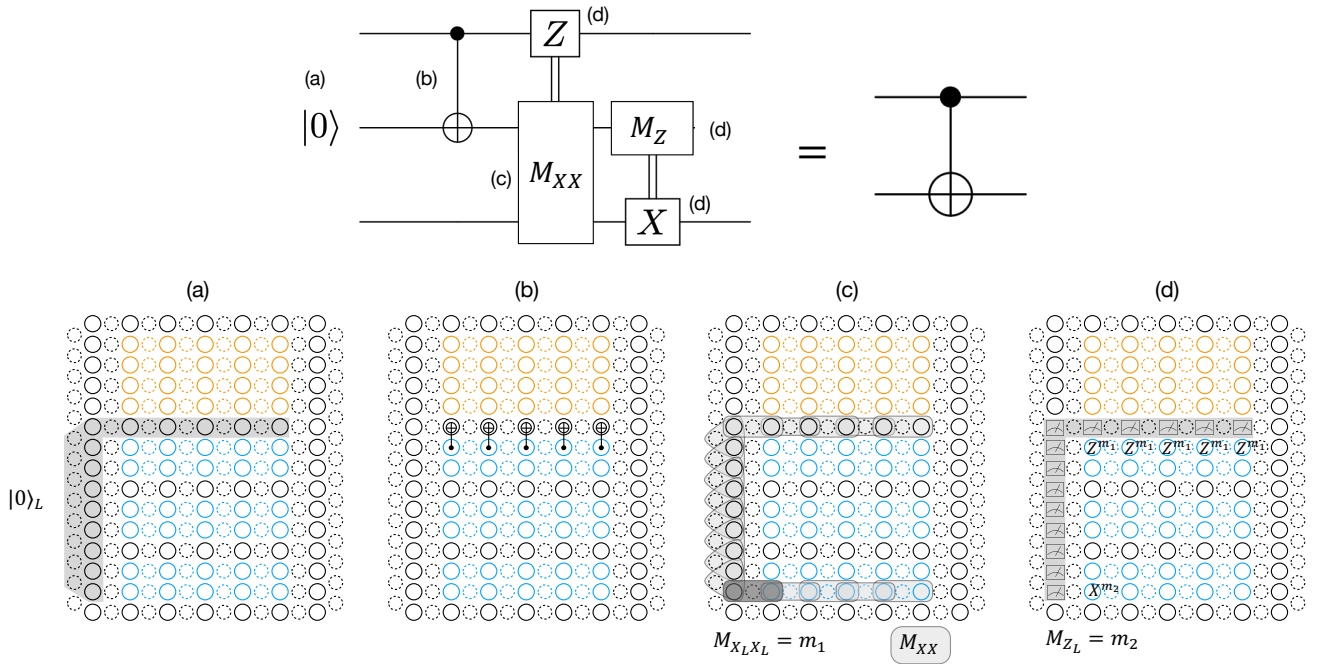


Figure 26. (Top) Circuit identity used to teleport a logical CNOT gate in the processor. (Bottom) Physical mapping of the top circuit onto the processor. It proceeds in four steps: (a) Preparation of a logical ancilla in the $|0\rangle_L$ state. This is achieved by preparing all data qubits in the $|0\rangle$ state, followed by d rounds of stabilizer measurements, decoding and correction. (b) A logical CNOT gate is realized using a local, transversal implementation. (c) A logical $X_L X_L$ measurement is realized by measuring d times the XX operator of the two physical qubits at the border between the logical qubits (in dark grey), as well as the stabilizers of the code (to ensure fault-tolerance). In terms of lattice surgery, this operation corresponds to a merge of the two logical qubits. The logical measurement outcome m_1 is obtained after decoding and subsequent correction. (d) To complete the gate teleportation, the logical Z_L operator is measured on the logical ancilla qubit. This is achieved by measuring the value of all the Z operators of the data qubits and the logical measurement outcome m_2 is obtained by taking the product of all measurement outcomes. Logical Pauli corrections, $Z_L^{m_1}$ on the control and $X_L^{m_2}$ may then be applied, or tracked in classical software to change the sign of subsequent logical measurement outcomes on these qubits.

performing a single physical X gate on any of the data qubits, and the logical Z_L gate is implemented transversally by applying a Z gate to all of the data qubits. Note that this is a consequence of the fact that we use a repetition code that corrects against phase-flip errors only,

which in turn comes from the fact that cat qubits have exponentially rare bit-flip errors.

CX_L gate — The logical CX_L gate can be implemented transversally on the repetition code. However,

implementing a logical CNOT gate in such a way between an arbitrary pair of logical qubits in the processor requires long distance interactions between the physical qubits of the processor, which is not a realistic feature of a superconducting quantum processor.

Instead, the logical CNOT gate can be realized using a circuit based on lattice surgery involving only nearest-neighbour interactions [78]. Here, we only provide a superficial overview of how lattice surgery works to illustrate how it may be adapted to the case of a repetition code (instead of the more standard case of a surface code). A detailed analysis of lattice surgery protocols may be found in [72, 79, 80]. The implementation proceeds in four (logical) steps, as shown in Fig. 26.

First, physical ancillary routing qubits are used to prepare a logical ancilla qubit in the $|0\rangle_L$ state that extends from the logical control qubit to the logical target qubit. Note that, to implement a CNOT gate, which is a ‘ $Z-X$ type’ interaction, the value of the logical Z_L operator on the control and of the logical X_L operator on the target needs to be accessed. For our QEC scheme, the Z_L operator has support on all of the physical qubits while the X_L operator can in principle be accessed on any of the data qubits, *e.g.* at the edge of the repetition code. For this reason, the logical ancilla prepared in the $|0\rangle_L$ state has an L shape, as depicted in Fig. 26(a).

Second, a (transversal) CNOT gate is performed between the logical control qubit and the logical ancilla, mapping the state of the control qubit $|\psi\rangle_L = \alpha|0\rangle_L + \beta|1\rangle_L$ to $\alpha|00\rangle_L + \beta|11\rangle_L$. Here, transversal means that physical CNOT gates are realized between pairs of physical qubits of the logical control qubit and the data qubits of the adjacent logical ancilla in the bus, as depicted in Fig. 26(b). Note however that the two logical qubits (control and ancilla) do not have the same distance, as the logical ancilla extends into the side bus. Because the logical X_L operator can be accessed on any of the physical qubits, however, a logical CNOT can be implemented using only physical CNOT gates on the part of the logical qubit that is in the horizontal bus (in terms of lattice surgery on the surface code, this corresponds to a ‘smooth split’ operation). However, in the case of a repetition code, one needs to use an additional ancillary logical qubit to implement this smooth split [81].

Then, the multi-qubit Pauli $X_L \otimes X_L$ operator of the logical ancilla and the logical target is measured using a local XX measurement between the edges of the two logical qubits, as depicted in dark grey in Fig. 26(c) (in terms of lattice surgery, one could also interpret this operation as a ‘rough merge’). For fault-tolerance, the measurement is repeated d times and the outcome is interpreted after decoding the full syndrome history.

The final step consists in disentangling the logical ancilla qubit from the logical control and logical target qubits using a logical Z_L measurement (Fig. 26(d)). To complete the teleportation, a (transversal) logical Z_L operation is applied to the control qubit if the logical $X_L \otimes X_L$ measurement produces the outcome -1 (with probability 0.5), and a logical X_L operation is applied to the logical target qubit if the logical Z_L measurement on the ancilla qubit produces the value -1 (with probability 0.5). In practice, these operations do not need to be performed but may be tracked in software (which is why we do not consider here that it is an additional time step).

As noted previously (*e.g.* [73, 79]), an attractive feature of using lattice surgery to implement logical multi-qubit measurements is that decoding algorithms used to interpret the error syndromes extend naturally over these protocols [38, 74, 82]. In its most general form, one may use lattice surgery to implement all the (single-qubit) Clifford gates using a classical tracking algorithm [80], by tracking the so-called edges operators (the correspondence between the physical qubits operators and the logical qubit operators). While this strategy is arguably most efficient in general, it also requires the ability to measure arbitrary logical Pauli operators, such as $X_L Y_L$, for instance. Lattice surgery protocols that achieve these measurements are more involved, *e.g.* using twist defects [72, 80] and the analysis of the associated logical failure rates under circuit-level noise has only been recently realized [74, 82]. In the context of Shor’s algorithm however, the overhead of the algorithm is widely dominated by the fault-tolerant implementation of the modular arithmetic circuits and table-lookup, composed of Toffoli and (sometimes multi-target) CNOT gates. Lattice surgery implementations of these gates only require $X_L X_L$ type measurements, which may be realized using regular stabilizer measurements only. Thus, we do not attempt to perform circuit-level simulations of lattice surgery protocols to derive the exact error models of these gates. Rather, we assume the same logical error rate per code cycle ϵ_L as in the case of the memory Eq. (3), and take into account the fact that the logical gates take $O(d)$ code cycles to complete.

CX_L^k gate — A major advantage of lattice surgery protocols is that they can be straightforwardly extended to multi-qubit Pauli measurements [72, 80]. As an example, we illustrate in Fig. 27 how the logical multi-target CX_L^k may be implemented on our processor. The only non-trivial difference with the case of the CX_L gate is the measurement of the multi-qubit Pauli operator $X_L X_L \dots X_L$. This may be achieved as depicted in Fig. 27(c) using physical weight-3 measurements of the XXX operator between three cat qubits.

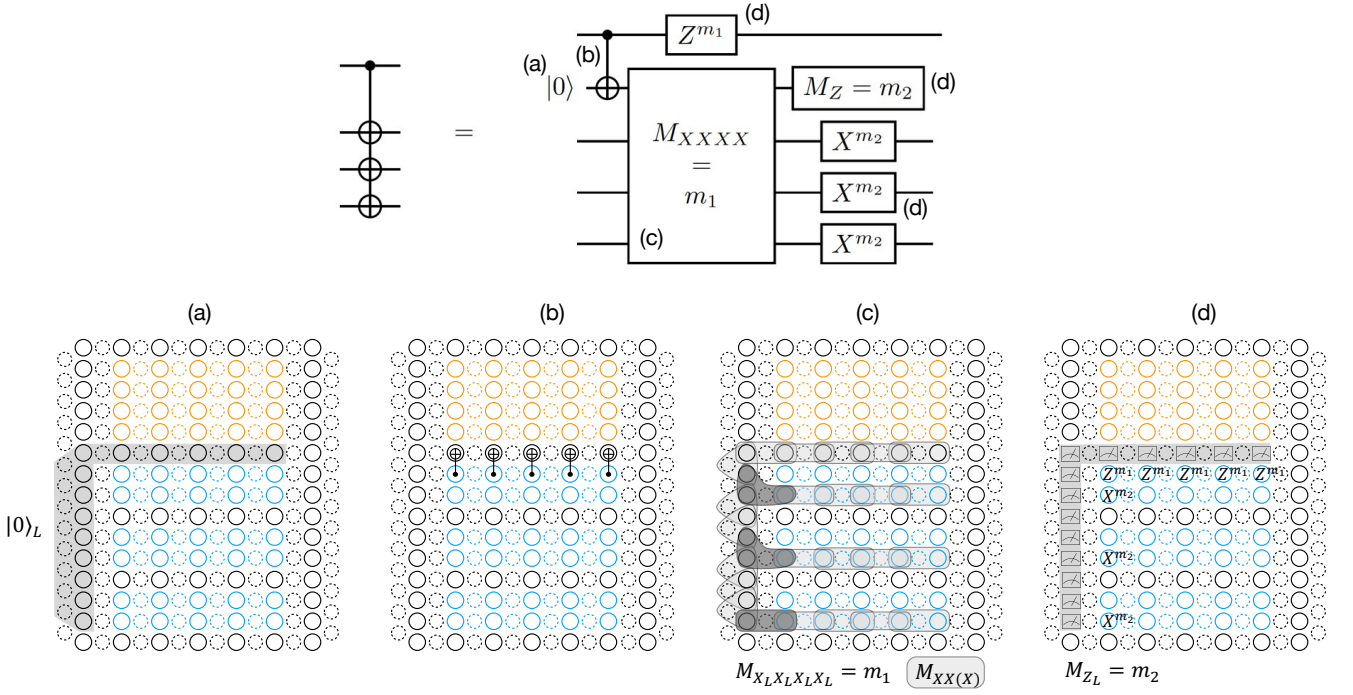


Figure 27. (Top) Circuit identity used to teleport a logical CX^k_L gate in the processor, with $k = 3$. (Bottom) Physical mapping of the top circuit onto the processor. The four steps are identical to that of Fig. 26, at the exception of the step (c) that consists in merging the logical qubits. This is achieved using weight-3 physical measurement of the XXX operator between two data qubits of the logical ancilla and the last data qubit of the logical target qubit. The logical measurement outcome m_1 is obtained by taking the product of the operators in dark grey (interpreted after subsequent decoding).

4. Logical Toffoli

We conclude this Appendix by detailing the implementation of the last logical gate, the Toffoli gate. In this work, we consider the teleportation based implementation [38, 83]. Note that other proposals to implement a logical Toffoli gate directly on repetition cat codes using pieceable fault-tolerance or code concatenation have been proposed [84], but the teleportation implementation leads to a lower overhead and is compatible with the physical layout of the processor we consider here.

Measurement based magic state preparation

The teleportation of a Toffoli gate consumes the (logical) magic state $|\text{CCX}\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$ [85]. Labelling the three logical qubits A, B, C, note that $|\text{CCX}\rangle$ is the +1 eigenstate of $X_A \text{CNOT}_{B,C}$, $X_B \text{CNOT}_{A,C}$ and $Z_C Z_{A,B}$ and can thus be obtained by starting from the logical state $|000\rangle_L$ and by performing a QND measurement of these operators. However, starting from a well-chosen state which can be both prepared easily and is already a +1 eigenstate of two of the

stabilizers, *e.g.* $|0+0\rangle_L$, it is sufficient to measure only the remaining stabilizer, here $X_A \text{CNOT}_{B,C}$ to achieve the preparation of $|\text{CCX}\rangle$. This stabilizer may be measured using the circuit depicted in Fig. 28(a). In this circuit, the Toffoli gates are used to measure $\text{CNOT}_{B,C}$ and a CNOT gate to measure X_A . In principle, a single physical ancilla qubit could be used to perform the measurement. However, for connectivity issues, it is convenient to use instead a block of ancilla qubits prepared in the $|\text{GHZ}\rangle = (|0\rangle^{\otimes d} + |1\rangle^{\otimes d})/\sqrt{2}$ state, in order to apply transversal Toffoli gates. The block of ancilla is then measured in the X basis and the $X_A \text{CNOT}_{B,C}$ stabilizer measurement result is given by the product of the X measurements. This state is prepared with a circuit of depth $(d+3)/2$ as shown in Fig. 28(a). Following [38], Fig. 28(b) shows the 2D layout to perform the QND measurement. If the measurement outcome is -1 , the prepared state is $Z_A |\text{CCX}\rangle$ and a correction needs to be applied (or tracked in the software). If the QND measurement is only performed once, a single physical Z error on the $|\text{GHZ}\rangle$ state would lead to a logical Z_A error. To make this circuit fault-tolerant, the measurement needs to be repeated. In the absence of errors, all measurement outcomes should be identical. However, when it is repeated, a single Z error on block A flips the results of all the following measurements and an error on block C randomly

flips all the following measurements as well. To prevent this, error detection or correction needs to be performed between each round of measurement by measuring the XX stabilizers. Below, we discuss two different fault-tolerant schemes to perform this magic state preparation.

Heralded scheme

Following the magic state preparation described in [38], the circuit of the logical Toffoli magic state preparation may be made fault-tolerant by post-selecting on the measurement outcomes. After the first QND measurement, a Z correction is applied to the qubit A if the measurement outcome is -1 . The following QND measurements are followed by a single round of error detection and the number of repetitions of the block ‘QND measurement + error detection’ is denoted d_m . The state preparation is rejected if the d_m QND measurements do not give the same result $+1$. If any error is detected during the error detection rounds, the state preparation is also rejected. The success probability is called the acceptance probability. The corresponding circuit is represented on Fig. 29. Note that a slightly different error model, described in Table II, is used compared to one described above for error correction. Indeed, in the case of error correction, we considered the recent proposed scheme [40] where the fast, noisy CNOT gates are used to measure the stabilizers of the repetition code. Here, in the context of a post-selected scheme, we consider the case where the CNOT gates are performed slower, in order to maximize the CNOT gate fidelity, so as not to lower the acceptance probability. The CNOT gate is now performed in a time $89/(\alpha^2\kappa_2)$ which depends on the number of photons, and the associated bit-flip error is given by $0.02e^{-2\alpha^2}$ [38]. Two scenarii can cause a logical error in this circuit: either all QND measurements are flipped, or a logical error happens on the blocks A, B or C without being detected by the error detection rounds. When d_m increases, the probability that each QND measurement fails decreases exponentially, while the probability of a logical error on the blocks A, B or C increases linearly, thus an optimal number of measurement repetitions d_m that minimized the logical error can be found.

However, when d_m increases, the acceptance probability of the magic state preparation decreases exponentially. To optimize these parameters, the space-time overhead, *i.e.* the number of qubits multiply by the depth of the circuit to generate one magic state, must be minimized. The space-time overhead to generate one magic state is evaluated as

$$\text{space-time overhead} = \frac{\text{number of qubits} \times \text{circuit depth}}{\text{acceptance probability}}. \quad (\text{E2})$$

$\kappa_1/\kappa_2 = 10^{-5}$		
CX		$T_{CX} = 89/(\kappa_2\alpha^2)$
$1 - \mathcal{F}$		3.5×10^{-3}
Z_1	$\alpha^2\kappa_1 T_{CX} + \frac{\pi^2}{64\alpha^2\kappa_2 T_{CX}}$	2.6×10^{-3}
$Z_2 = Z_1 Z_2$	$\frac{1}{2}\alpha^2\kappa_1 T_{CX}$	4.4×10^{-4}
CCX		$T_{CCX} = 89/(\kappa_2\alpha^2)$
$1 - \mathcal{F}$		4.6×10^{-3}
$Z_1 = Z_2$	$\alpha^2\kappa_1 T^* + \frac{\pi^2}{128\alpha^2\kappa_2 T^*}$	1.8×10^{-3}
Z_3	$\frac{5}{8}\alpha^2\kappa_1 T^*$	1.1×10^{-4}
$Z_1 Z_2$	$\frac{\pi^2}{128\alpha^2\kappa_2 T^*}$	8.8×10^{-4}
$Z_1 Z_3 = Z_2 Z_3$	$\frac{1}{8}\alpha^2\kappa_1 T^*$	2.3×10^{-5}
$= Z_1 Z_2 Z_3$		

Table II. Pauli phase-flip error models used for the magic state preparation. For the dissipative implementations considered in this work, we summarize the analytical errors models derived in [38]. The equalities in the left column, *e.g.* $Z_2 = Z_1 Z_2$, means that these errors occur with equal probability.

To ensure that at least $(d+1)/2$ physical errors are needed to create a logical error, the QND measurement has to be repeated at least $d_m = (d-1)/2$ times. However at this parameter value, the magical state preparation errors are dominated by the $|\text{GHZ}\rangle$ measurement errors by several orders of magnitude as noticed in [38, Fig. 15c]. By increasing d_m , these measurement errors diminish and even if the acceptance rate also diminishes, it is beneficial for achieving a lower space-time overhead for the same logical phase-flip error.

Fig. 30 presents the space-time overhead needed as a function of the logical error targeted. The space-time overhead shown for a certain logical error is optimized in terms of distance d and number of repeated QND measurement d_m (in red). The proposition in [38] where $d_m = (d-1)/2$ is also represented (in blue).

Deterministic scheme

This section presents a deterministic scheme (with acceptance probability equals to one). This scheme is similar to the one before but now includes a fault-tolerant error correction between each round of measurement (and not only error detection), and a majority vote between the d_m outcomes of the stabilizer measurements (*c.f.* Fig. 31). Note that error correction is needed at each round because in case a Z error is not corrected on the block C before the next stabilizer measurement, its outcome is random. Further note that d rounds of error correction are needed to make it fault-tolerant. Here again, we neglect the classical processing time of the decoding

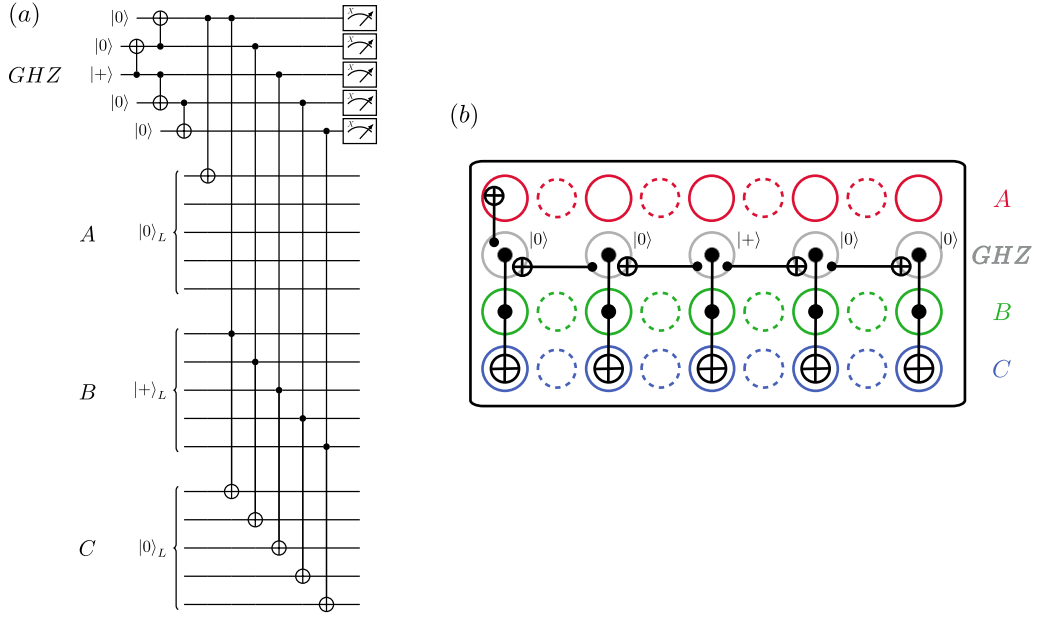


Figure 28. (a) $X_A \text{CNOT}_{B,C}$ measurement circuit for a distance $d = 5$ code. An auxiliary $|\text{GHZ}\rangle$ state is prepared on the first block and is connected to the qubit A by a CNOT gate to perform the X_A stabilizer measurement, and to qubit B and C by transversal Toffoli gates to implement the $\text{CNOT}_{B,C}$ stabilizer measurement. The stabilizer measurement result is given by computing the parity of the X measurements of the $|\text{GHZ}\rangle$ state. Starting from the state $|0+0\rangle$, this achieves the preparation of $|\text{CCX}\rangle$ or $Z_A |\text{CCX}\rangle$ if the measurement outcome is $+1$ or -1 respectively. (b) Mapping of the circuit on the physical layout of the processor. Note that all interactions are local [38].

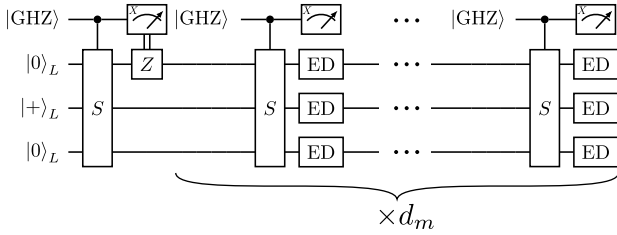


Figure 29. Heralded scheme of the magic state preparation. The first QND measurement ($S = X_A \text{CNOT}_{B,C}$) is followed by a Z correction if the measurement outcome is -1 . Then, the block ‘QND measurement + error detection (ED)’ is repeated d_m times and the preparation is rejected if the measurements do not all give $+1$. The error detection round is performed between the rounds of QND measurements to prevent errors from propagating to the GHZ measurement. d_m is optimized to minimize the space-time overhead.

of the syndrome and assume that the correction on the data qubits is perfect and instantaneous. As in the previous case, when d_m increases, the probability that the majority vote between the QND measurements fails decreases exponentially, while the probability of a logical error on the blocks A, B or C increases, such that there exists a finite optimal number of repetitions.

Fig. 30 (yellow curve) shows the space-time overhead needed as a function of the logical error targeted for the

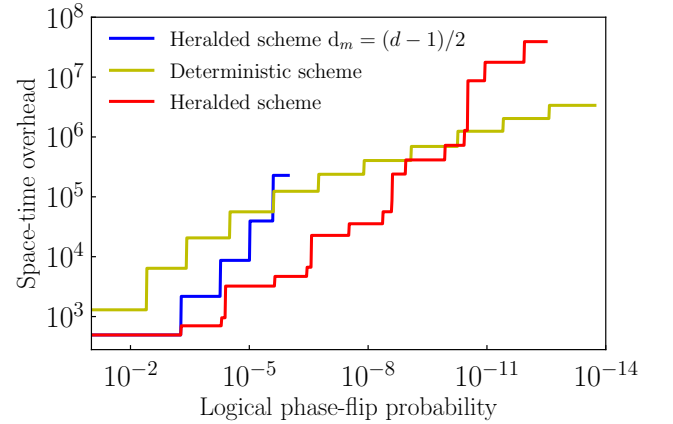


Figure 30. Space-time overhead as a function of the logical error probability needed for the Toffoli magic state prepared. The space-time overhead is calculated with $\text{space-time overhead} = \text{number of qubits} \times \text{circuit depth/acceptance probability}$. For the heralded and deterministic scheme, the distance of the code and d_m are chosen to minimize the space-time overhead. For comparison, the proposition in [38] where $d_m = (d-1)/2$ is represented (in blue).

deterministic scheme. Like for the heralded scheme, the space-time overhead shown for a certain logical error is optimized in terms of distance d and number of repeated

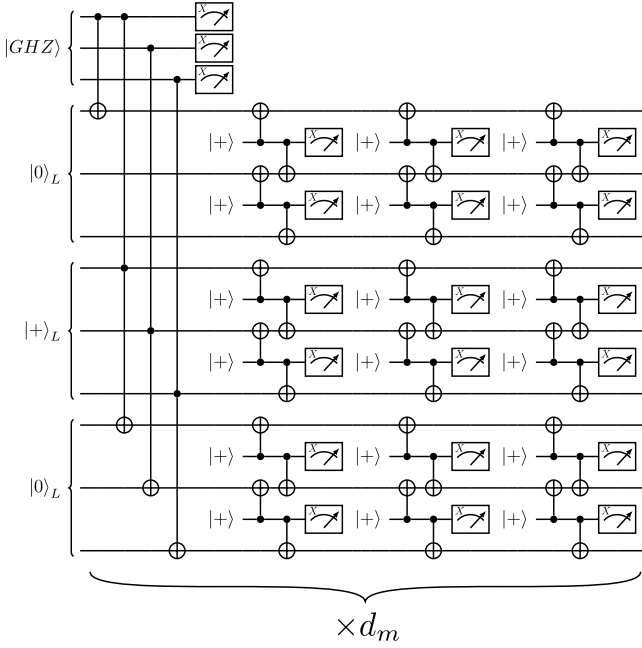


Figure 31. Deterministic scheme of the magic state preparation for $d = 3$. For simplicity, only one block is shown, however this circuit is repeated d_m times. d rounds of error correction are performed between the rounds of QND measurements to correct errors before the next GHZ measurement. A majority vote between the QND measurements then determines the result of the measurement. The number of repetitions d_m is optimized to minimize the space-time overhead.

QND measurement d_m . This scheme needs a larger default overhead because of its very large depth, but has a better scaling as a function of the logical error targeted and thus become better than the heralded scheme if the phase-flip logical error targeted is below approximately 10^{-10} .

Magic state preparation total logical error

As for the logical memory error, the bit-flip is calculated independently of the logical phase-flip error. The former is calculated with the CNOT and Toffoli gates physical bit-flip which are dominant. The number of photon is chosen so that the logical bit-flip equals the logical phase-flip and the results are shown in Table III.

i	d_1	α^2	error prob.	steps	time	accept. prob. (%)
0	3	3.75	1.05×10^{-3}	23	54.7 μ s	84
1	3	3.93	1.02×10^{-4}	29	65.8 μ s	74.5
2	3	5.32	8.14×10^{-5}	35	58.7 μ s	66
3	5	7.15	4.62×10^{-6}	46	57.4 μ s	45.6
4	5	8.18	7.00×10^{-7}	53	57.8 μ s	36.2
5	5	8.38	5.36×10^{-7}	60	63.9 μ s	28.8
6	7	9.71	6.14×10^{-8}	73	67.1 μ s	14.8
7	7	10.76	8.40×10^{-9}	81	67.2 μ s	10.5
8	7	11.06	5.16×10^{-9}	89	71.8 μ s	7.27
9	9	11.64	2.28×10^{-9}	104	79.7 μ s	2.62
10	9	12.83	2.30×10^{-10}	113	78.6 μ s	1.54
11	9	13.44	7.36×10^{-11}	122	81 μ s	0.975
12	19	17.35	7.90×10^{-12}	9576	4.92 ms	100
13	21	18.94	5.40×10^{-13}	14112	6.65 ms	100
14	23	20.53	3.74×10^{-14}	21344	9.27 ms	100

Table III. Parameters for the preparation of the Toffoli states. i is an index identifying each parameter set, the one used in Table IV. d and α^2 are respectively the code distance and the average number of photons used during the preparation of the magical state. The fourth column describes the error probability during the process. Fifth column counts the depth of the magical state preparation, in number of physical gates. Last column is the acceptance probability. The heralded scheme is used for $i \leq 11$ while for $i \geq 12$ the deterministic scheme is favored.

Heralded scheme simulation technique

In order to evaluate the logical failure of a circuit from the physical errors, the circuit-level error model is used, which includes every possible location for an error to occur. Monte Carlo simulations are generally used to sample the logical failure rate. However, sampling a logical failure probability of 10^{-10} with an acceptance probability of 10^{-2} would require thousands of years of CPU runtime to reach a relative standard deviation of the order of the percent. We will now present two methods which have been used in order to reach reasonable computational time.

Stratified sampling consists in partitioning the population to sample in distinct subgroups, which are sampled independently. Partitioning the population according to the number of errors happening in the circuit is an efficient way to reduce the time required for the Monte Carlo simulations.

$$\mathbb{P}(\text{failure}) = \sum_{n=0}^{n=N} \mathbb{P}(\text{failure} \mid n \text{ errors in the circuit}) \times \mathbb{P}(n \text{ errors in the circuit}) \quad (\text{E3})$$

where N denotes the number of possible locations for an error to occur in the circuit. $\mathbb{P}(n \text{ errors in the circuit})$ is a binomial law and becomes negligible for large n . Due to the fault-tolerant construction of the scheme,

$\mathbb{P}(\text{failure} \mid n \text{ errors in the circuit} < n_{FT}) = 0$ where $n_{FT} = \min(\frac{d+1}{2}, d_m + 1)$. Thus, only a handful of n contributes to the logical error probability. $\mathbb{P}(n \text{ errors in the circuit})$ can be calculated analytically and the only remaining terms to simulate with Monte Carlo simulations are $\mathbb{P}(\text{failure} \mid n \text{ errors in the circuit})$ for a few relevant values of n .

However, this method alone cannot reduce sufficiently the computational time for large d_m . We introduce a second type of stratified sampling, which combined with the first one, is sufficient to reach tractable computations. Because the scheme uses post-selection, most of the trajectories which could cause a logical failure because they contain more Z errors than $(d+1)/2$ are rejected because these errors are detected by the error detection rounds. But we can finely choose the trajectories which can both cause a logical error while being undetected by syndrome measurements, *i.e.* a stratified sampling on the location where errors can happen. If \mathcal{C} designates the set of restricted locations where errors need to happen in order to create a logical failure without being detected, the logical failure is then given by

$$\mathbb{P}(\text{failure}) = \mathbb{P}(\text{failure} \mid n \text{ errors} \in \mathcal{C}) \times \mathbb{P}(n \text{ errors} \in \mathcal{C}) \quad (\text{E4})$$

Deterministic scheme simulation technique

The circuit-level error model is here intractable due to the depth of the circuit considered. Once again, two logical error sources can be distinguished. Either the majority vote of the repeated measurements fails, or a logical error happens on the logical qubits A, B or C . The latter has the same logical error as the memory. After each correction applied to the logical qubits A, B or C , residual errors can propagate to the QND measurement. In order to perform a circuit level simulation of the failure probability of the QND measurement, the residual errors from the logical qubits A, B or C were sampled with circuit-level simulation, and added as input of the QND measurement simulation. Because d rounds of error correction are performed between each round of QND measurement, the failure probability of the different QND measurements are independent and can be added in order to calculate the failure probability of the majority vote.

Teleportation

The teleportation of Toffoli gate, from the magical state $|\text{CCX}\rangle$, is done using the circuit represented in

Fig. 32. Note that an auto-corrected Toffoli state would allow to also perform the corrections offline, such as in [50].

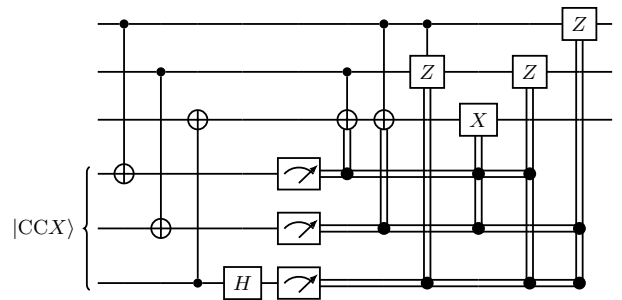


Figure 32. Teleportation of a Toffoli gate. From top, the two first qubits are the controls and the third is the target. $|\text{CCX}\rangle$ is the magical state for the Toffoli gate, defined as the result of applying a Toffoli gate on $|+\rangle|+\rangle|0\rangle$, and obtained via the magical state preparation described in the text.

Appendix F: Resources for different key sizes

Estimation of resources required for solving elliptic curve discrete logarithm problem for different sizes are reported in Table IV. The optimal parameters that we found are also given. A description of symbols can be found in the caption of Table IV. The optimization is run by an exhaustive search on the different parameters to minimize the product $\alpha^2 n_{\text{qubits}} t_{\text{exp}}$.

Similarly, the optimal parameters and resources for factoring RSA integers are detailed in Table V. The implementation of Shor's algorithm for factorization used to evaluate the resources is detailed in [42], and the code producing the table is available at [41].

As stated in the main text, we find that computing a discrete logarithm on a 256-bit elliptic curve requires 126 133 cat qubits, which corresponds to a distance-13 repetition code and cat qubits of size $\alpha^2 = 19$ photons. This number was obtained under the assumption that the exponential suppression of bit-flip errors holds up until cat sizes of 19 photons, an assumption that will be crucial to demonstrate experimentally. Note that recent theoretical works [86–88] have shown that, due to the better scaling of exponential suppression of bit-flips in squeezed cats, the extremely low bit-flip error rates required to run large-scale algorithms on repetition cat codes could be attained with much fewer photons. Alternatively, under similar assumptions than those used in this work, we estimate that a $(d_X, d_Z) = (3, 37)$ rectangular (rotated) surface code built on cat qubits of size $\alpha^2 = 10$ photons yields the same logical error rate as a

n	n_e	w_e	w_m	α^2	d	i	#factories	factories qubits	n_{qubits}	t	t_{exp}	logical qubits
8	16	9	2	12	7	4	5	388	2817	1 s	1 s	85
16	32	11	4	14	9	5	6	463	5961	9 s	10 s	159
32	64	13	4	15	9	7	16	1537	12050	55 s	1 min	305
64	128	15	4	17	11	7	13	1252	25346	8 min	9 min	595
128	256	17	5	18	13	10	87	10026	64543	1 hours	1 hours	1173
256	512	18	6	19	13	12	84	18101	126133	7 hours	9 hours	2326
512	1024	20	7	21	15	12	73	15736	258739	3 days	3 days	4632

Table IV. Resources and parameters for discrete logarithm computation. n is the number of qubits to represent the coordinates of an elliptic curve point. n_e is the number of qubits dedicated for the two registers containing the factors of the elliptic curve multiplication; $n_e = 2n$ with Shor's algorithm assuming the order of the cyclic group being of the same order of magnitude as p . w_e and w_m are the windows size for respectively the elliptic curve multiplication and the integer multiplication. α^2 is the average number of photons used for each cat qubit. d is the code distance and i the index of the parameters of magical states factory, which are presented in Table III. Next detailed parameters are the number of magical states factories (#factories) and number of qubits used in all of them. n_{qubits} is the total number of (physical) cat qubits. t and t_{exp} are respectively the time for one run and the average time to successfully compute the discrete logarithm. Last parameter is the number of logical qubits involved in the computation.

n	n_e	m	w_e	w_m	α^2	d	i	#factories	factories qubits	n_{qubits}	t	t_{exp}	logical qubits
6	6	5	2	2	10	5	2	4	229	986	62 ms	243 ms	33
8	9	8	2	2	11	5	3	6	463	1476	159 ms	331 ms	45
16	21	10	3	3	12	7	4	5	388	2551	992 ms	1 s	76
128	189	18	4	3	16	11	7	13	1252	18650	3 min	3 min	430
256	381	20	4	4	17	11	8	20	1917	35083	15 min	19 min	819
512	765	23	4	4	19	13	10	87	10026	84073	2 hours	2 hours	1593
829	1242	24	5	4	19	13	12	84	18101	136456	6 hours	8 hours	2548
1024	1493	26	5	4	20	15	12	73	15736	180269	12 hours	13 hours	3137
2048	3029	28	5	5	21	15	13	98	23075	349133	3 days	4 days	6214

Table V. Resources and parameters for integer factorization. The corresponding algorithm is detailed in [42] and the code generating this table is available at [41]. n is the number of qubits to represent the coordinates of an elliptic curve point. n_e is the number of qubits dedicated for the two registers containing the factors of the elliptic curve multiplication; $n_e = 2n$ with Shor's algorithm assuming the order of the cyclic group being of the same order of magnitude as p . m is the number of qubits added for the coset representation of integers. w_e and w_m are the windows size for respectively the exponentiation and the multiplications. α^2 is the average number of photons used for each cat qubit. d is the code distance and i the index of the parameters of magical states factory, which are presented in Table III. Next detailed parameters are the number of magical states factories (#factories) and number of qubits used in all of them. n_{qubits} is the total number of (physical) cat qubits. t and t_{exp} are respectively the time for one run and the average time to successfully compute the discrete logarithm. Last parameter is the number of logical qubits involved in the computation.

distance-13 repetition code on $\alpha^2 = 19$ photons, which corresponds roughly to a $\approx \times 10$ overhead.

* elie.gouzien@cea.fr

† <https://quantum.paris>

- [1] A. Montanaro, Quantum algorithms: an overview, *npj Quantum Information* **2**, 15023 (2016), 1511.04206.
- [2] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, Elucidating reaction mechanisms on quantum computers, *Proceedings of the National Academy of Sciences* **114**, 7555 (2017), 1605.03590.
- [3] C. Gidney and M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, *Quantum* **5**, 433 (2021), 1905.09749.
- [4] Y. R. Sanders, D. W. Berry, P. C. S. Costa, L. W. Tessler, N. Wiebe, C. Gidney, H. Neven, and R. Babbush, Compilation of Fault-Tolerant Quantum Heuristics for Combinatorial Optimization, *PRX Quantum* **1**, 020312 (2020), 2007.07391.

- [5] E. T. Campbell, B. M. Terhal, and C. Vuillot, Roads towards fault-tolerant universal quantum computation, *Nature* **549**, 172 (2017), 1612.07330.
- [6] D. Aharonov and M. Ben-Or, Fault-Tolerant Quantum Computation with Constant Error Rate, *SIAM Journal on Computing* **38**, 1207 (2008), quant-ph/9906129.
- [7] A. Y. Kitaev, Quantum computations: algorithms and error correction, *Russian Mathematical Surveys* **52**, 1191 (1997).
- [8] E. Knill, R. Laflamme, and W. H. Zurek, Resilient quantum computation: error models and thresholds, *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **454**, 365 (1998), quant-ph/9702058.
- [9] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, *Physical Review A* **71**, 022316 (2005), quant-ph/0403025.
- [10] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation, *Physical Review A* **86**, 032324 (2012), 1208.4088.

- (2012), 1208.0928.
- [11] L. Childress and R. Hanson, Diamond NV centers for quantum computing and quantum networks, *MRS Bulletin* **38**, 134 (2013).
 - [12] P. Aliferis and J. Preskill, Fault-tolerant quantum computation against biased noise, *Physical Review A* **78**, 052331 (2008), 0710.1301.
 - [13] D. K. Tuckett, S. D. Bartlett, and S. T. Flammia, Ultrahigh Error Threshold for Surface Codes with Biased Noise, *Physical Review Letters* **120**, 050505 (2018), 1708.08474.
 - [14] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, Dynamically protected cat-qubits: a new paradigm for universal quantum computation, *New Journal of Physics* **16**, 045014 (2014), 1312.2017.
 - [15] V. V. Albert, C. Shu, S. Krastanov, C. Shen, R.-B. Liu, Z.-B. Yang, R. J. Schoelkopf, M. Mirrahimi, M. H. Devoret, and L. Jiang, Holonomic Quantum Control with Continuous Variable Systems, *Physical Review Letters* **116**, 140502 (2016), 1503.00194.
 - [16] S. Puri, S. Boutin, and A. Blais, Engineering the quantum states of light in a Kerr-nonlinear resonator by two-photon driving, *npj Quantum Information* **3**, 18 (2017), 1605.09408.
 - [17] J. Guillaud and M. Mirrahimi, Repetition Cat Qubits for Fault-Tolerant Quantum Computation, *Physical Review X* **9**, 041053 (2019), 1904.09474.
 - [18] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994) pp. 124–134.
 - [19] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing* **26**, 1484 (1997), quant-ph/9508027.
 - [20] E. Barker, *Guideline for using cryptographic standards in the federal government: cryptographic mechanisms* (2020).
 - [21] Information Technology Laboratory, *Digital Signature Standard (DSS)* (2013).
 - [22] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, Quantum Attacks on Bitcoin, and How to Protect Against Them, *Ledger* **3**, 10.5195/ledger.2018.127 (2018), 1710.10377.
 - [23] The following description of point addition, as well as Eq. (1), are valid when P and Q are distinct and different from the neutral element. If $P = Q$, the tangent of the curve on this point is used. If Q is the neutral element, the line to consider is the one parallel to the y -axis going through P , and the result is $P + Q = P$. If $Q = -P$, that is Q is symmetrical of P with respect to the x -axis, the line joining them is vertical and the result is the neutral element: $P + Q = 0$.
 - [24] D. P. DiVincenzo and P. W. Shor, Fault-Tolerant Error Correction with Efficient Quantum Codes, *Physical Review Letters* **77**, 3260 (1996), quant-ph/9605031.
 - [25] M. Ekerå, Quantum algorithms for computing general discrete logarithms and orders with tradeoffs (2018), <https://eprint.iacr.org/2018/797>.
 - [26] R. B. Griffiths and C.-S. Niu, Semiclassical Fourier Transform for Quantum Computation, *Physical Review Letters* **76**, 3228 (1996), quant-ph/9511007.
 - [27] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, and M. Soeken, Improved Quantum Circuits for Elliptic Curve Discrete Logarithms, in *Post-Quantum Cryptography*, Vol. 12100, edited by J. Ding and J.-P. Tillich (Springer International Publishing, 2020) pp. 425–444, series Title: Lecture Notes in Computer Science, 2001.09580.
 - [28] 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, *Physical Review X* **8**, 041015 (2018), 1805.03662.
 - [29] C. Gidney, Windowed quantum arithmetic, 1905.07682 (2019).
 - [30] Eq. (1) only describes the elliptic curve addition in the generic case when P and Q are distinct and different from the neutral element. Only the generic case is implemented as this saves resources at the cost of an approximate algorithm; the exact consequences are discussed in [32].
 - [31] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, A new quantum ripple-carry addition circuit, quant-ph/0410184 (2004).
 - [32] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms, in *Advances in Cryptology – ASIACRYPT 2017*, Vol. 10625, edited by T. Takagi and T. Peyrin (Springer International Publishing, 2017) pp. 241–270, series Title: Lecture Notes in Computer Science, 1706.06752.
 - [33] We allow the accumulation register to store a number up to $2p$ after each add and half cycle. The division by 2 ensure its value not to be amplified beyond this limit, after each cycle, even when using non-modular additions (what would not be the case when doubling). See App. C 4 for the details.
 - [34] B. S. Kaliski, The Montgomery inverse and its applications, *IEEE Transactions on Computers* **44**, 1064 (1995).
 - [35] P. T. Cochrane, G. J. Milburn, and W. J. Munro, Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping, *Physical Review A* **59**, 2631 (1999), quant-ph/9809037.
 - [36] R. Lescanne, M. Villiers, T. Peronnin, A. Sarlette, M. Delbecq, B. Huard, T. Kontos, M. Mirrahimi, and Z. Leghtas, Exponential suppression of bit-flips in a qubit encoded in an oscillator, *Nature Physics* **16**, 509 (2020), 1907.11729.
 - [37] C. Berdou, A. Murani, U. Reglade, W. C. Smith, M. Villiers, J. Palomo, M. Rosticher, A. Denis, P. Morfin, M. Delbecq, T. Kontos, N. Pankratova, F. Rautschke, T. Peronnin, L.-A. Sellem, P. Rouchon, A. Sarlette, M. Mirrahimi, P. Campagne-Ibarcq, S. Jezouin, R. Lescanne, and Z. Leghtas, One hundred second bit-flip time in a two-photon dissipative oscillator, 2204.09128 (2022).
 - [38] C. Chamberland, K. Noh, P. Arrangoiz-Arriola, E. T. Campbell, C. T. Hann, J. Iverson, H. Putterman, T. C. Bohdanowicz, S. T. Flammia, A. Keller, G. Refael, J. Preskill, L. Jiang, A. H. Safavi-Naeini, O. Painter, and F. G. S. L. Brandão, Building a Fault-Tolerant Quantum Computer Using Concatenated Cat Codes, *PRX Quantum* **3**, 010329 (2022), 2012.04108.
 - [39] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, *Nature* **402**, 390 (1999), quant-ph/9908010.
 - [40] F.-M. Le Régent, C. Berdou, Z. Leghtas, J. Guillaud, and M. Mirrahimi, High-performance repetition cat code

- using fast noisy operations, [2212.11927](#) (2022).
- [41] Code is available at https://github.com/ElieGouzien/elliptic_log_cat.
- [42] É. Gouzien and N. Sangouard, Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory, *Physical Review Letters* **127**, 140503 (2021), [2103.06159](#).
- [43] C. Gidney, Quantum block lookahead adders and the wait for magic states, [2012.01624](#) (2020).
- [44] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, *Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography* (2018).
- [45] D. R. L. Brown, Standards for Efficient Cryptography (2010).
- [46] A. Zieniewicz and J.-L. Pons, *Pollard's kangaroo for SECPK1* (2020).
- [47] P. L. Montgomery, Modular multiplication without trial division, *Mathematics of Computation* **44**, 519 (1985).
- [48] R. Rines and I. Chuang, High Performance Quantum Modular Multipliers, [1801.01081](#) (2018).
- [49] A. G. Fowler, Time-optimal quantum computation, [1210.4626](#) (2013).
- [50] C. Gidney and A. G. Fowler, Flexible layout of surface code computations using AutoCCZ states, [1905.08916](#) (2019).
- [51] V. Vedral, A. Barenco, and A. Ekert, Quantum networks for elementary arithmetic operations, *Physical Review A* **54**, 147 (1996), [quant-ph/9511018](#).
- [52] S. Beauregard, Circuit for Shor's algorithm using $2n+3$ qubits, *Quantum Information & Computation* **3**, 175–185 (2003), [quant-ph/0205095](#).
- [53] D. W. Berry, C. Gidney, M. Motta, J. R. McClean, and R. Babbush, Qubitization of Arbitrary Basis Quantum Chemistry Leveraging Sparsity and Low Rank Factorization, *Quantum* **3**, 208 (2019), [1902.02134](#).
- [54] C. H. Bennett, Logical Reversibility of Computation, *IBM Journal of Research and Development* **17**, 525 (1973).
- [55] “=” is the affectation operator, “==” check the equality, “//” is the integer division operator (quotient of Euclidean division) and “%” returns the rest of the Euclidean division.
- [56] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Physical Review A* **52**, 3457 (1995), [quant-ph/9503016](#).
- [57] C. Gidney, *Constructing Large Controlled Nots* (2015).
- [58] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
- [59] T. Häner, M. Roetteler, and K. M. Svore, Factoring using $2n+2$ qubits with Toffoli based modular multiplication, *Quantum Information & Computation* **17**, 673 (2017), [1611.07995](#).
- [60] A. Joshi, K. Noh, and Y. Y. Gao, Quantum information processing with bosonic qubits in circuit QED, *Quantum Science and Technology* **6**, 033001 (2021), [2008.13471](#).
- [61] Z. Leghtas, S. Touzard, I. M. Pop, A. Kou, B. Vlastakis, A. Petrenko, K. M. Sliwa, A. Narla, S. Shankar, M. J. Hatridge, M. J. Reagor, L. Frunzio, R. J. Schoelkopf, M. Mirrahimi, and M. H. Devoret, Confining the state of light to a quantum manifold by engineered two-photon loss, *Science* **347**, 853 (2015), [1412.4633](#).
- [62] S. Touzard, A. Grimm, Z. Leghtas, S. O. Mundhada, P. Reinhold, C. Axline, M. J. Reagor, K. S. Chou, J. Z. Blumoff, K. M. Sliwa, S. Shankar, L. Frunzio, R. J. Schoelkopf, M. Mirrahimi, and M. H. Devoret, Coherent Oscillations inside a Quantum Manifold Stabilized by Dissipation, *Physical Review X* **8**, 021005 (2018), [1705.02401](#).
- [63] D. K. Tuckett, A. S. Darmawan, C. T. Chubb, S. Bravyi, S. D. Bartlett, and S. T. Flammia, Tailoring Surface Codes for Highly Biased Noise, *Physical Review X* **9**, 041031 (2019), [1812.08186](#).
- [64] D. K. Tuckett, S. D. Bartlett, S. T. Flammia, and B. J. Brown, Fault-Tolerant Thresholds for the Surface Code in Excess of 5 % Under Biased Noise, *Physical Review Letters* **124**, 130501 (2020), [1907.02554](#).
- [65] Q. Xu, N. Mannucci, A. Seif, A. Kubica, S. T. Flammia, and L. Jiang, Tailored XZZX codes for biased noise, [2203.16486](#) (2022).
- [66] J. P. Bonilla Ataides, D. K. Tuckett, S. D. Bartlett, S. T. Flammia, and B. J. Brown, The XZZX surface code, *Nature Communications* **12**, 2172 (2021), [2009.07851](#).
- [67] J. Roffe, L. Z. Cohen, A. O. Quintavalle, D. Chandra, and E. T. Campbell, Bias-tailored quantum LDPC codes, [2202.01702](#) (2022).
- [68] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S. M. Girvin, and R. J. Schoelkopf, Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics, *Nature* **431**, 162 (2004), [cond-mat/0407325](#).
- [69] A. Blais, A. L. Grimsom, S. Girvin, and A. Wallraff, Circuit quantum electrodynamics, *Reviews of Modern Physics* **93**, 025005 (2021), [2005.12667](#).
- [70] J. Clarke, A. N. Cleland, M. H. Devoret, D. Esteve, and J. M. Martinis, Quantum Mechanics of a Macroscopic Variable: The Phase Difference of a Josephson Junction, *Science* **239**, 992 (1988).
- [71] P. Bertet, A. Auffeves, P. Maioli, S. Osnaghi, T. Meunier, M. Brune, J.-M. Raimond, and S. Haroche, Direct Measurement of the Wigner Function of a One-Photon Fock State in a Cavity, *Physical Review Letters* **89**, 200402 (2002).
- [72] A. G. Fowler and C. Gidney, Low overhead quantum computation using lattice surgery, [1808.06709](#) (2019).
- [73] D. Litinski, A Game of Surface Codes: Large-Scale Quantum Computing with Lattice Surgery, *Quantum* **3**, 128 (2019), [1808.02892](#).
- [74] C. Chamberland and E. T. Campbell, Universal Quantum Computing with Twist-Free and Temporally Encoded Lattice Surgery, *PRX Quantum* **3**, 010331 (2022), [2109.02746](#).
- [75] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, Topological quantum memory, *Journal of Mathematical Physics* **43**, 4452 (2002), [quant-ph/0110143](#).
- [76] O. Higgott, PyMatching: A Python Package for Decoding Quantum Codes with Minimum-Weight Perfect Matching, *ACM Transactions on Quantum Computing* **3**, 1 (2022), [2105.13082](#).
- [77] P. Brooks and J. Preskill, Fault-tolerant quantum computation with asymmetric Bacon-Shor codes, *Physical Review A* **87**, 032310 (2013), [1211.1400](#).
- [78] D. Gottesman, Fault-Tolerant Quantum Computation with Higher-Dimensional Systems, *Chaos, Solitons and*

- Fractals* **10**, 1749 (1999), [quant-ph/9802007](#).
- [79] C. Horsman, A. G. Fowler, S. Devitt, and R. Van Meter, Surface code quantum computing by lattice surgery, *New Journal of Physics* **14**, 123011 (2012), [1111.4022](#).
 - [80] D. Litinski and F. v. Oppen, Lattice Surgery with a Twist: Simplifying Clifford Gates of Surface Codes, *Quantum* **2**, 62 (2018), [1709.02318](#).
 - [81] Indeed, on a surface code, the smooth split operation consists in splitting the logical qubit in two logical qubits in the ‘logical X_L ’ direction, *i.e.* the X -distance d_X of the two children logical qubits is half that of the parent qubit and (after correction) the new logical X_L^i operators are related to the old one as $X_L^1 \otimes X_L^2 = X_L^{\text{old}}$. For repetition cat codes, the role of the X -distance d_X is played by the average photon number in the cat qubits, and the support of the logical X_L operator is a single physical qubit. Therefore, unlike in the surface code case, one cannot ‘split’ a string of physical X operators to produce two new logical qubits. Rather, preparing a logical ancilla qubit in the $|0\rangle_L$ state and applying a logical CNOT gate has the same effect.
 - [82] C. Chamberland and E. T. Campbell, Circuit-level protocol and analysis for twist-based lattice surgery, *Physical Review Research* **4**, 023090 (2022), [2201.05678](#).
 - [83] X. Zhou, D. W. Leung, and I. L. Chuang, Methodology for quantum logic gate construction, *Physical Review A* **62**, 052316 (2000), [quant-ph/0002039](#).
 - [84] J. Guillaud and M. Mirrahimi, Error rates and resource overheads of repetition cat qubits, *Physical Review A* **103**, 042413 (2021), [2009.10756](#).
 - [85] P. W. Shor, Fault-tolerant quantum computation, in *Proceedings of 37th Conference on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1996) pp. 56–65, [quant-ph/9605011](#).
 - [86] D. S. Schlegel, F. Minganti, and V. Savona, Quantum error correction using squeezed Schrödinger cat states, *Physical Review A* **106**, 022431 (2022), [2201.02570](#).
 - [87] T. Hillmann and F. Quijandría, Quantum error correction with dissipatively stabilized squeezed cat qubits, [2210.13359](#) (2022).
 - [88] Q. Xu, G. Zheng, Y.-X. Wang, P. Zoller, A. A. Clerk, and L. Jiang, Autonomous quantum error correction and fault-tolerant quantum computation with squeezed cat qubits, [2210.13406](#) (2022).