

[CC BY 4.0 DEED Attribution 4.0 International](#)

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

**Please provide feedback**

Please support the ScholarWorks@UMBC repository by emailing [scholarworks-group@umbc.edu](mailto:scholarworks-group@umbc.edu) and telling us what having access to this work means to you and why it's important to you. Thank you.

# Elliptic Curves in Continuous-Variable Quantum Systems

Maxwell Aifer and Evan Sheldon

Department of Physics, University of Maryland, Baltimore County, Baltimore, MD 21250, USA

(Dated: January 24, 2024)

Elliptic curves are planar curves which can be used to define an abelian group. The efficient computation of discrete logarithms over this group is a longstanding problem relevant to cryptography. It may be possible to efficiently compute these logarithms using a quantum computer, assuming that the group addition operation can be computed efficiently on a quantum device. Currently, however, thousands of logical qubits are required for elliptic curve group addition, putting this application out of reach for near-term quantum hardware. Here we give an algorithm for computing elliptic curve group addition using a single continuous-variable mode, based on weak measurements of a system with a cubic potential energy. This result could lead to improvements in the efficiency of elliptic curve discrete logarithms using a quantum device.

*Introduction.*—Elliptic curves have a prominent role in number theory, and are of great practical importance in modern cryptography, as they provide an alternative to the RSA algorithm [1–3]. This makes the efficient computation of the elliptic curve group operation (and the discrete logarithm over this group) a question of great importance. As alternative computing paradigms can in some cases provide speed-ups over classical digital computers, it is of interest to explore the computation of elliptic curve group operations in different paradigms.

Previous work has explored the use of discrete-variable and quantum computers to evaluate the elliptic curve group operation and take discrete logarithms over this group; however, to use these results in practical scenarios requires thousands of logical qubits [4], placing it beyond NISQ-era capabilities. Continuous-variable quantum information is seen as a promising approach to realizing cryptographic protocols like quantum key distribution [5, 6], as continuous-variable states are compatible with existing telecom infrastructure; however, to our knowledge, no attempt has been made to evaluate the elliptic curve group using continuous variable quantum systems. There has also been significant effort to design classical computing hardware for elliptic curve group addition [7].

In this work, we propose a method for evaluating the group operation of an elliptic curve (over the reals) using a continuous-variable quantum system. As is well known, the elliptic curve group addition operation can be cast as a geometric relationship between points in the plane, in particular by identifying points of intersection between a straight line and an elliptic curve [2, 3]. We show that a continuous-variable quantum system can be designed whose energy eigenstates have Wigner functions resembling elliptic curves, by implementing a Hamiltonian with a cubic potential energy function. Moreover, weak quantum measurements of quadrature operators can effectively project this Wigner function onto a straight line in the plane, resulting in a method for elliptic curve point addition.

Interestingly, this algorithm is entirely based on the geometric properties of a quantum system’s Wigner function, and those of the weak measurement operation. We note that existing algorithms of elliptic curve group ad-

dition work by operating on binary encodings of elliptic curves, and these encodings do not readily exhibit the geometry of the problem. In contrast, our algorithm operates directly on an object that geometrically embodies the elliptic curve, namely the Wigner function of a continuous-variable mode. We therefore consider this algorithm exemplary of a novel “geometric computing” paradigm, which may be applicable both in classical and quantum settings.

It is also shown that a superconducting nonlinear asymmetric inductive element (SNAIL) device [8, 9] can be used to realize the necessary cubic potential physically, suggesting a path to the experimental implementation of our algorithm.

*Elliptic Curves in a Continuous Variable Quantum System.*—A real elliptic curve is the set of points  $(x, y) \in \mathbb{R}^2$  defined by the equation [3]

$$y^2 = ax^3 + bx + c, \quad (1)$$

for some  $a, b, c \neq 0$ . A group can be defined over the points of an elliptic curve. Let  $A = (x_A, y_A)$  and  $B = (x_B, y_B)$  be two points belonging to an elliptic curve, as in Fig. 1a. We denote the slope of the line connecting  $A$  and  $B$  by  $s = (y_B - y_A)/(x_B - x_A)$ . We may compute a third point  $C = (x_C, y_C)$  from  $A$  and  $B$  as follows

$$x_C = s^2 - x_A - x_B, \quad (2)$$

$$y_C = -y_A + s(x_A - x_B). \quad (3)$$

Then we may define a binary operation  $(+)$  acting on points of the curve by

$$A + B = -C \quad (4)$$

where  $-C = (x_C, -y_C)$  is the reflection of  $C$  over the  $x$  axis. It can be shown that the points of the curve form a group under the operation  $(+)$ . Graphically, we can interpret the group addition rule in the following way: to obtain the point  $C$ , take points  $A$  and  $B$ , draw a line that intersects the 2 points and also a third point  $-C$  on the curve (See Fig. 1a). Finally,  $-C$  is reflected over the  $x$  axis to obtain  $C$ . We also define coordinates  $r$  and  $\theta$

as an alternative way to specify the line between  $A$  and  $B$ . Namely,

$$\theta = \arctan(s), \quad r = (y_A - sx_A) \cos(\theta) \quad (5)$$

Elliptic curves appear naturally as the characteristic phase-space curves of a system with a cubic potential energy. Suppose that a classical system has a potential energy

$$V(x) = -ax^3 - bx, \quad (6)$$

with real constants  $a, b > 0$ . Then the classical Hamiltonian is given by

$$H(x, p) = -ax^3 - bx + \frac{1}{2m}p^2, \quad (7)$$

where  $m$  is the mass. Consider the constant energy set obtained by setting  $H(x, p) = E$ . If we make the identifications  $E = c$  and  $y = p/\sqrt{2m}$ , then Eq. (7) is equivalent to Eq. (1), so the equal-energy curves are elliptic curves as shown in Fig. 1(a). A corresponding quantum Hamiltonian can be defined by replacing the variables  $x$  and  $p$  with the dimensionless quadrature operators  $\hat{x} = (\hat{a}^\dagger + \hat{a})/\sqrt{2}$  and  $\hat{p} = i(\hat{a}^\dagger - \hat{a})/\sqrt{2}$ , where  $\hat{a}^\dagger$  and  $\hat{a}$  are respectively the creation and annihilation operators for a single bosonic mode [10, 11]. That is, we define

$$\hat{H} = -a\hat{X}^3 - b\hat{X} + \frac{1}{2m}\hat{P}^2. \quad (8)$$

A Hamiltonian of this form can be realized physically using a SNAIL device [8] with the correct choice of parameters. Note that the SNAIL device can interpolate between quadratic and cubic Hamiltonians; therefore one can begin with an eigenstate of the harmonic oscillator Hamiltonian, and then adiabatically deform the Hamiltonian into the form of Eq. (8), which will result in an energy eigenstate of the latter [12]. We now consider an eigenstate of the elliptic curve Hamiltonian, that is a wavefunction  $|\Psi\rangle$  satisfying the time-independent Schrödinger equation

$$\hat{H}|\Psi\rangle = E|\Psi\rangle, \quad (9)$$

where we have set  $\hbar = 1$ . In particular, we consider the Wigner function of such an energy eigenstate, defined as [11]

$$W(x, p) = \int_{-\infty}^{\infty} dy e^{ipy} \left\langle x - \frac{y}{2} \right| \Psi \rangle \left\langle \Psi \right| x + \frac{y}{2} \rangle. \quad (10)$$

The Wigner function is a quasiprobability distribution which shares certain features with classical phase space probability density function, notably that integrating it in any direction results in a valid marginal probability density function. We therefore intuitively expect that the Wigner function  $W(x, p)$  of the energy eigenstate  $|\Psi\rangle$  will be concentrated around the classical phase-space orbit corresponding to energy  $E$ . In Fig. 1, we see that this is

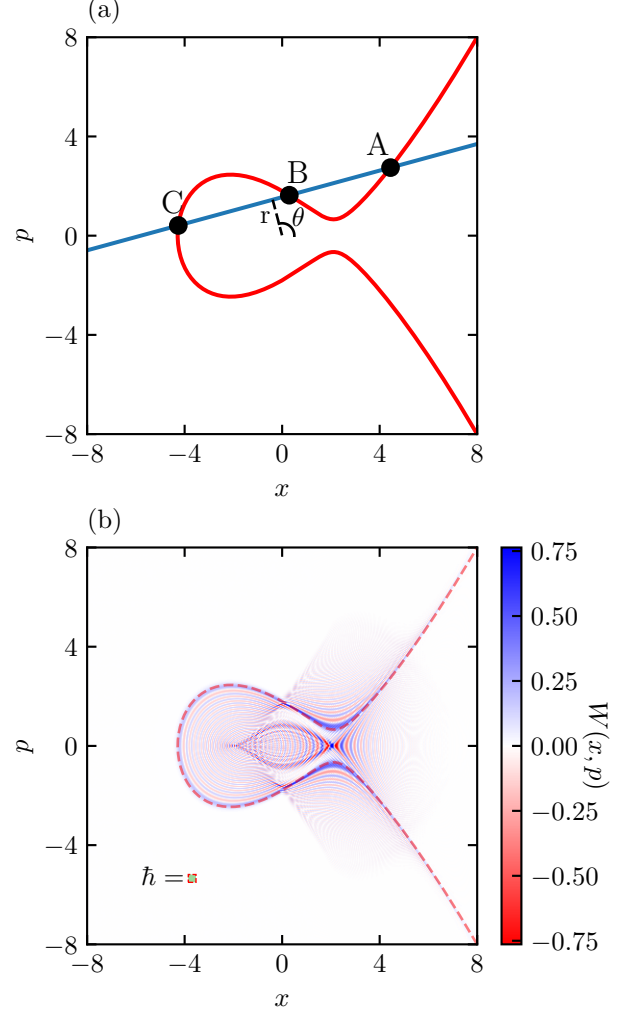


FIG. 1. (a) The elliptic curve corresponding to the classical Hamiltonian (7) with parameters  $a = 0.075$  and  $b = -1$ , and  $m = 1$ , and  $E = 1.62$  (arbitrary units). (b) The Wigner function derived from the Eigenvector of the quantum Hamiltonian (9) with the same parameters and  $\hbar = 0.1$ . In some places, there were values of the Wigner function as large as  $W = 1.53$ , but to make the form of the function easily visible, values of the Wigner function are cut off at  $\pm 0.75$ .

in fact the case; we have plotted both the classical phase space orbit in panel (a), and the Wigner function of the quantum Hamiltonian in panel (b), and remark that the Wigner function of the classical system shows high concentration around the classical phase space orbit. There are also regions where the Wigner function has support that are distant from the classical phase space orbit. However, one notices that in these regions the Wigner function oscillates rapidly, meaning that they will often be eliminated from the marginal distributions due to destructive interference. The Wigner function was obtained

in two steps. First, the eigenstate  $|\Psi\rangle$  was constructed in the position basis by discretizing the Hamiltonian operator and then numerically performing an eigendecomposition. Then the Wigner function was evaluated on a grid via straightforward numerical integration of Eq. (10) using methods similar to those described in [13]. We also adapted code from [13] for generating plots of the Wigner function.

Having found a way to realize quantum states that are representative of elliptic curves, we next will turn to the problem of approximately evaluating the elliptic curve group addition operation using this state.

*Evaluation of the Elliptic Curve Group Operation.*—

The problem we would like to solve is as follows: given two points  $A = (x_A, y_A)$  and  $B = (x_B, y_B)$ , evaluate the coordinates of the point  $C = A + B$ , where addition is understood as defined in equations (2) and (3). Graphically, the addition operation can be carried out by drawing a line through the points  $A$  and  $B$ , then finding the third point where this line intersects the elliptic curve, and finally reflecting the point thus obtained over the  $x$  axis. After a measurement of a quadrature operator (that is, a linear combination of the  $\hat{X}$  and  $\hat{P}$  operators), the Wigner function will “collapse” so that its support is a line in the phase space. However, performing such a measurement on the elliptic curve state described earlier would leave none of the structure of that state, making it impossible to extract the result of the group addition operation. Alternatively, we can consider weak measurements of a quadrature operator on an elliptic curve state [14, 15]. Such a weak measurement can be seen as a kind of interpolation between the identity operation (leaving the elliptic curve state unchanged) and a projective quadrature measurement (completely collapsing the wavefunction). This can be accomplished using weak measurements of a quantum system with the cubic potential energy in Eq. (6). Specifically, define a basis of quadrature states  $|\psi_\theta\rangle$  as the eigenvectors of the quadrature operator  $x_\theta$

$$\hat{X}_\theta |x_\theta\rangle = x_\theta |x_\theta\rangle, \quad (11)$$

where

$$\hat{X}_\theta = \cos(\theta)\hat{X} + \sin(\theta)\hat{P}. \quad (12)$$

To define a weak measurement of quadrature  $\hat{X}_\theta$  having outcome  $\mu$  and width parameter  $w$ , we define the Krauss operator

$$K_\theta = \frac{2^{1/4}}{(\pi w^2)^{1/4}} \int_{-\infty}^{\infty} dx_\theta e^{-(x_\theta - \mu)^2/w^2} |x_\theta\rangle \langle x_\theta| \quad (13)$$

For a system initialized in the state  $|\psi_0\rangle$ , the Krauss operator can be used to determine the post-measurement state  $|\psi_{\text{pm}}\rangle$  as follows

$$|\psi_{\text{pm}}\rangle = \frac{K_\theta |\psi_0\rangle}{\sqrt{\langle \psi_0 | K_\theta^\dagger K_\theta | \psi_0 \rangle}}. \quad (14)$$

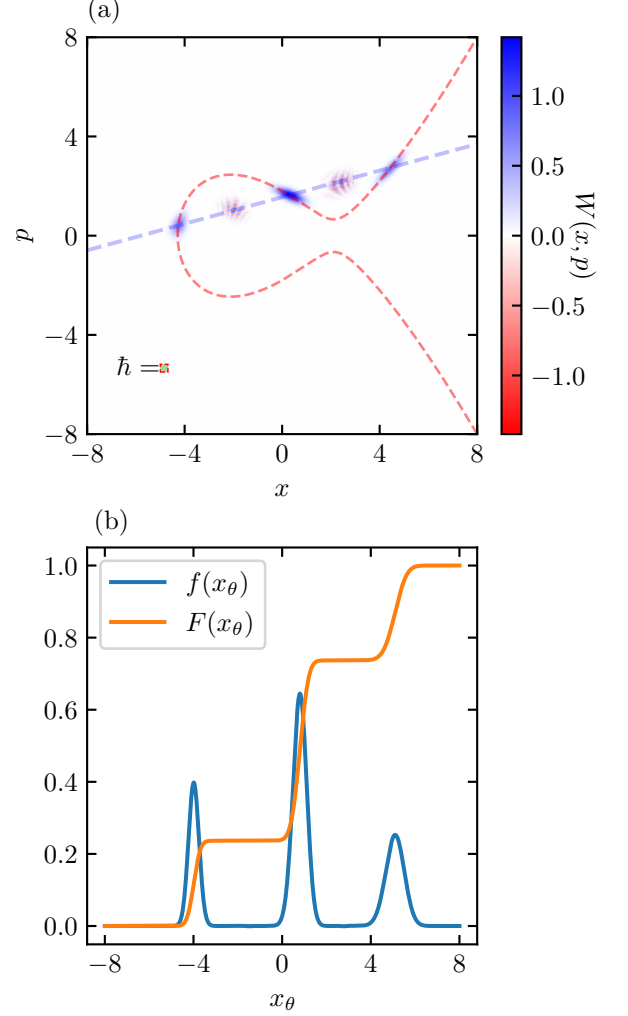


FIG. 2. (a) The post-measurement state after a weak measurement of a quadrature operator  $\hat{X}_\theta$ , with  $\theta = \pi/12$  and  $r = 1.5$ . Similarly to Fig.1, the range of values for the Wigner function has been restricted, in this case to the interval  $\pm 1.42$ . In some places, there were values of the Wigner function as large as  $W = 2.84$ . (b) Marginal distribution for the second quadrature measurement (of the operator  $\hat{X}_{\theta+\pi/2}$ ). The blue curve  $f(x)$  is the probability density function for the marginal distribution, and the orange curve  $F(x)$  is the cumulative distribution function, where the three peaks correspond to the three blue regions of concentration in phase space of the Wigner function in Fig. 2a. In Fig. 2a we also see two regions of concentration with wavelike patterns in between these, which are not present in the marginal due to destructive interference.

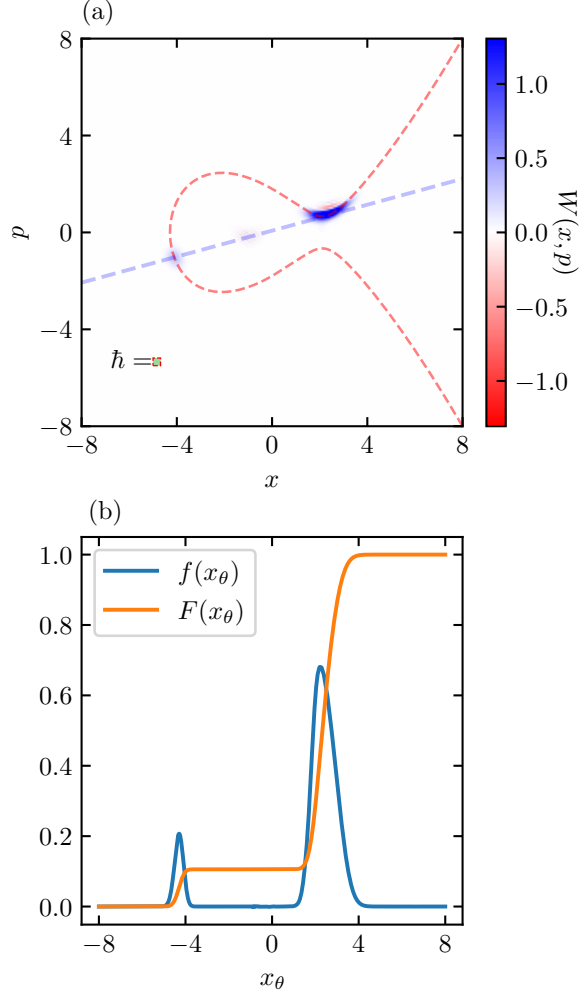


FIG. 3. (a) The post-measurement state after a weak measurement of a quadrature operator  $\hat{X}_\theta$ , with  $\theta = \pi/12$  and  $r = 0.07$ . Similarly to Fig.1, the range of values for the Wigner function has been restricted, in this case to the interval  $\pm 1.31$ . In some places, there were values of the Wigner function as large as  $W = 2.61$ . (b) Marginal distribution for the second quadrature measurement (of the operator  $\hat{X}_{\theta+\pi/2}$ ). The blue curve  $f(x)$  is the probability density function for the marginal distribution, and the orange curve  $F(x)$  is the cumulative distribution function, where the peaks correspond to the blue regions of concentration in phase space of the Wigner function in Fig. 3a.

In Figs. 2 and 3 we see the effect of a weak quadrature measurement on the Wigner function of our system, initially prepared in an eigenstate of the Hamiltonian (8).

1. Prepare an energy eigenstate  $|\psi_n\rangle$  of the cubic Hamiltonian.
2. Compute the polar coordinates  $r, \theta$  from Eq. (5), and make a weak measurement of the quadrature  $x_\theta$ .
3. Choose some tolerance  $\delta_r$ . If  $|x_\theta - r| > \delta_r$ , repeat steps 1 and 2 until  $|x_\theta - r| \leq \delta_r$ . This will require  $O(1/\delta_r)$  trials on average.
4. Take a projective measurement of the quadrature  $x_{\theta+\pi/2}$ , and compute  $x$  and  $y$ .
5. Make sure that the computed  $x$  and  $y$  are not the points  $A$  or  $B$ , and if so, repeat steps 1-4

*Discussion.*— In summary, we have demonstrated the ability to perform the group addition operation over an elliptic curve group by performing weak measurements on elliptic curve-shaped Wigner functions, which could be realized experimentally using a quantum SNAIL device [8]. Once the validity of our method has been demonstrated through experiments, the algorithm can be modified and extended to accomplish more complex tasks. In particular, it is desirable to extend this method to perform elliptic curve exponentiation [16]; if an elliptic curve exponentiation can be performed that preserves a coherent superposition, then Shor's algorithm may be applied to achieve efficient computation of the discrete logarithm, which would have far-reaching impacts in cryptography.

Further investigations into this topic include implementing quantum error-correcting procedures for this continuous variable state. Given that this protocol will be affected by environmental decoherence, the experimental realization of this algorithm would require a protocol for continuous-variable error correction, which has been investigated to some extent [17–19].

It is also important to estimate the resource costs of our quantum algorithm, especially the time and energy needed to evaluate the elliptic curve group addition operation. Analyses of the time and energy costs of discrete-variable quantum computations have been carried out [20–23], and a similar method could be adapted to continuous-variable systems to address our algorithm.

---

[1] Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017.

[2] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

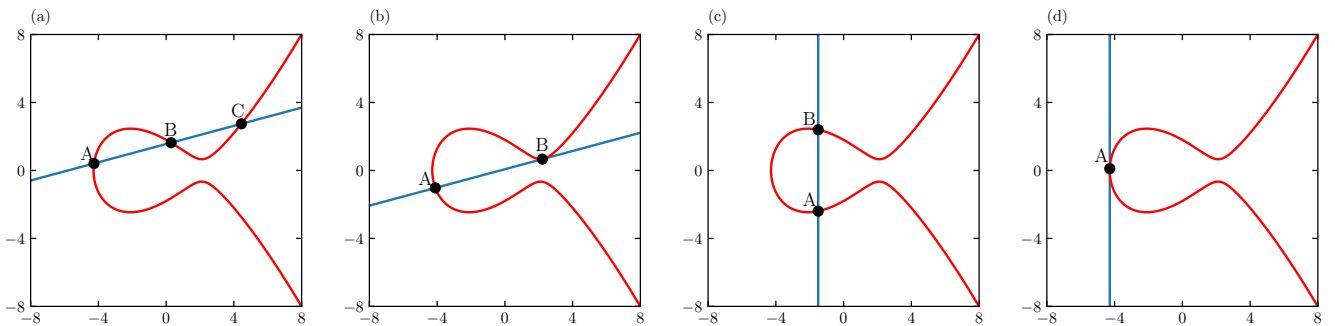
[3] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97. Springer Science & Business Media, 1993.

[4] Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken. Improved quantum circuits for elliptic curve discrete logarithms. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings*.

- ceedings 11*, pages 425–444. Springer, 2020.
- [5] Nitin Jain, Hou-Man Chin, Hossein Mani, Cosmo Lupo, Dino Solar Nikolic, Arne Kordts, Stefano Pirandola, Thomas Brochmann Pedersen, Matthias Kolb, Bernhard Ömer, et al. Practical continuous-variable quantum key distribution with composable security. *Nature communications*, 13(1):4740, 2022.
  - [6] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.
  - [7] Arielle Verri Lucca, Guilherme Augusto Mariano Sborz, Valderi Reis Quietinho Leithardt, Marko Beko, Cesar Albenes Zeferino, and Wemerson Delcio Parreira. A review of techniques for implementing elliptic curve point multiplication on hardware. *Journal of Sensor and Actuator Networks*, 10(1):3, 2020.
  - [8] Timo Hillmann, Fernando Quijandria, Göran Johansson, Alessandro Ferraro, Simone Gasparinetti, and Giulia Ferrini. Universal gate set for continuous-variable quantum computation with microwave circuits. *Phys. Rev. Lett.*, 125:160501, Oct 2020.
  - [9] NE Frattini, U Vool, S Shankar, A Narla, KM Sliwa, and MH Devoret. 3-wave mixing josephson dipole element. *Applied Physics Letters*, 110(22), 2017.
  - [10] Alessio Serafini. *Quantum continuous variables: a primer of theoretical methods*. CRC press, 2017.
  - [11] Wolfgang P Schleich. *Quantum optics in phase space*. John Wiley & Sons, 2011.
  - [12] Tosio Kato. On the adiabatic theorem of quantum mechanics. *Journal of the Physical Society of Japan*, 5(6):435–439, 1950.
  - [13] Nanite. Efficient numerical evaluation of wigner function. *Physics Stack Exchange*, Jul 2020.
  - [14] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
  - [15] Howard M Wiseman and Gerard J Milburn. *Quantum measurement and control*. Cambridge university press, 2009.
  - [16] Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery. Fast elliptic curve arithmetic and improved weil pairing evaluation. In Marc Joye, editor, *Topics in Cryptology — CT-RSA 2003*, pages 343–354, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
  - [17] Peter van Loock. A note on quantum error correction with continuous variables. *Journal of Modern Optics*, 57(19):1965–1971, 2010.
  - [18] Josephine Dias and Timothy C Ralph. Quantum error correction of continuous-variable states with realistic resources. *Physical Review A*, 97(3):032335, 2018.
  - [19] Richard L Barnes. Stabilizer codes for continuous-variable quantum error correction. *arXiv preprint quant-ph/0405064*, 2004.
  - [20] Joni Ikonen, Juha Salmilehto, and Mikko Möttönen. Energy-efficient quantum computing. *npj Quantum Information*, 3(1):17, 2017.
  - [21] Sebastian Deffner. Energetic cost of hamiltonian quantum gates. *Europhysics Letters*, 134(4):40002, 2021.
  - [22] Maxwell Aifer and Sebastian Deffner. From quantum speed limits to energy-efficient quantum gates. *New Journal of Physics*, 24(5):055002, 2022.
  - [23] Alexia Auffeves. Quantum technologies need a quantum energy initiative. *PRX Quantum*, 3(2):020101, 2022.

## Appendix A: Elliptic Curves

The material on elliptic curves here is taken from references [3] and [2].



An elliptic curve is a curve that is defined by the equation

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

If we want to represent the points on an elliptic curve as a group, we can take points A and B, draw a line that intersects the 2 points, and also a third point C on the curve; as displayed in (a). We can then define

$$A + B = -C \quad (\text{A2})$$

where  $-C$  is a reflection of  $C$  across the x-axis.

In the case of (b), the third intersection point  $C$  approaches  $B$ , and the line becomes tangent to the curve at  $B$ . As a result, the tangent point,  $B$  is also the intersection point so we can define

$$A + B = -B \quad (\text{A3})$$

In the case of  $B = -A$  as seen in (c), we encounter a vertical intersection line through the curve. An issue in this case is that we don't have a third point on the curve our line intersects. Our solution is to define an additional point  $\mathcal{O}$  at infinity. An important property is that  $\mathcal{O}$  exists on all vertical lines.

$$A + B = A + (-A) = \mathcal{O} \quad (\text{A4})$$

The last case (d) we will look over is a vertical line with one point of intersection on the curve,  $B = A$ . Since our intersection line is vertical, we can represent this case as

$$A + A = \mathcal{O} \quad (\text{A5})$$

## Appendix B: Phase Space Description

The material on the quantum phase space formalism is taken from references [10] and [11]. The state of a quantum system is, in general, represented by a density operator  $\hat{\rho}$ , which may be expanded in an eigenbasis of pure states as

$$\hat{\rho} = \sum_n p_n |\psi_n\rangle \langle \psi_n|. \quad (\text{B1})$$

Absent from this description is any concept of the phase space, which is prominent in the corresponding classical theory. However, quantum systems also admit a phase-space description, which can be found using the Weyl transformation. An operator  $\hat{A}$  acting on the quantum Hilbert space can be mapped to a phase-space function  $\tilde{A}(x, p)$  via

$$\tilde{A}(x, p) = \int_{-\infty}^{\infty} dy e^{ipy/\hbar} \left\langle x - \frac{y}{2} \left| \hat{A} \right| x + \frac{y}{2} \right\rangle \quad (\text{B2})$$

So, if we want to be able to map the action of the density matrix in phase space, we should perform a Weyl transformation on the density matrix, and in doing so we can derive the Wigner function.

$$W(x, p) = \tilde{\rho}/\hbar = \frac{1}{\hbar} \int_{-\infty}^{\infty} dy e^{ipy/\hbar} \left\langle x - \frac{y}{2} \left| \hat{\rho} \right| x + \frac{y}{2} \right\rangle \quad (\text{B3})$$

One of the key properties of the Wigner function is that we can calculate the probability distribution in space or momentum of the state by integrating along  $p$  or  $x$  respectively.

$$\int_{-\infty}^{\infty} W(x, p) dp = \langle x | \hat{\rho} | x \rangle = \rho(x, x) = P(x) \quad (\text{B4})$$

$$\int_{-\infty}^{\infty} W(x, p) dx = \langle p | \hat{\rho} | p \rangle = P(p) \quad (\text{B5})$$

In fact, the Wigner function can be marginalized over an arbitrary axis in the  $x$ - $p$  plane to yield a probability distribution for the perpendicular coordinate. That is, if we define the variables  $x_\theta$  and  $p_\theta$  (called quadratures)

$$x_\theta = \cos(\theta)x + \sin(\theta)p, \quad p_\theta = -\sin(\theta)x + \cos(\theta)p. \quad (\text{B6})$$

Integrating the Wigner function with respect to one of these quadratures gives the probability density function for the perpendicular one

$$\int_{-\infty}^{\infty} W(x_\theta, p_\theta) dp_\theta = \langle x | \hat{\rho} | x \rangle = P(x_\theta) \quad (\text{B7})$$

$$\int_{-\infty}^{\infty} W(x_\theta, p_\theta) dx = P(p_\theta). \quad (\text{B8})$$

Importantly, the Wigner function is not quite a probability distribution, as it can have negative values, and in fact the negativity of the Wigner function characterizes the quantum behavior of a system. For this reason the Wigner function is often referred to as a quasi-probability distribution.

Although typically a continuous-variable quantum state is expressed in the position or momentum basis, we may also use the basis corresponding to the quadrature variables  $x_\theta$  or  $p_\theta$ . To this end, we define a quadrature operator  $\hat{X}_\theta$

$$\hat{X}_\theta = \cos(\theta)\hat{x} + \sin(\theta)\hat{p}, \quad (\text{B9})$$

where we restrict the region of theta to  $0 \leq \theta \leq \pi$ . The basis associated with this operator is determined by the eigenvalue equation

$$\hat{X}_\theta |X_\theta\rangle = X_\theta |X_\theta\rangle. \quad (\text{B10})$$

Multiply both sides by  $\langle x|$  to achieve

$$\langle x|\hat{X}_\theta|X_\theta\rangle = \langle x|X_\theta|X_\theta\rangle \quad (\text{B11})$$

$$\rightarrow \hat{X}_\theta\psi(x) = X_\theta\psi(x) \quad (\text{B12})$$

where  $\psi(x) = \langle x|X_\theta\rangle$ .

$$\rightarrow (\cos(\theta)\hat{x} + \sin(\theta)\hat{p})\psi(x) = X_\theta\psi(x) \quad (\text{B13})$$

$$\rightarrow \cos(\theta)x\psi(x) - i\hbar\sin(\theta)\partial_x\psi(x) = X_\theta\psi(x) \quad (\text{B14})$$

The solution to this eigenvalue problem is

$$\psi(x) = C_\theta \exp\left[\frac{-ix(-2X_\theta + x\cos(\theta))}{2\hbar\sin(\theta)}\right] \quad (\text{B15})$$

Since this wavefunction is imaginary, we need to normalize it in reference to delta functions. By projecting onto the completeness relation and utilizing orthogonality, we yield the normalization constant

$$|C_\theta|^2 = \frac{1}{2\pi\hbar\sin(\theta)} \quad (\text{B16})$$

This gives our rotated quadrature eigenstate wavefunction of

$$\psi(x) = \sqrt{\frac{1}{2\pi\hbar\sin(\theta)}} \exp\left[\frac{-ix(-2X_\theta + x\cos(\theta))}{2\hbar\sin(\theta)}\right] \quad (\text{B17})$$

### Appendix C: Weak Measurements

This treatment of weak measurements is based on references [14] and [15]. If we want to take a weak measurement of a system, we must take the system's initial quantum state  $|\psi\rangle$ , and couple it with an ancilla state  $|\varphi\rangle$ . This gives us the combined initial system of  $|\Psi\rangle = |\psi\rangle \otimes |\varphi\rangle$ . The entire system evolves in time through the time evolution operator, represented by  $U(t)$ .

$$|\Psi_t\rangle = U(t)|\Psi_0\rangle \quad (\text{C1})$$

We can solve for  $U(t)$  by plugging it into the Schrodinger Equation.

$$\frac{dU(t)}{dt} = \frac{-i}{\hbar}HU(t) \quad (\text{C2})$$

$$U(t) = e^{\frac{-itH}{\hbar}} \quad (\text{C3})$$

$H = H_S \otimes H_A$  where  $H$  is the Hamiltonian of the whole system,  $H_S$  is the Hamiltonian of the quantum state, and  $H_A$  is the Hamiltonian of the ancilla state. We can also represent  $U(t)$  with a Taylor series expansion. Assume  $t$  is small such that  $t^3 \approx 0$

$$U(t) = I \otimes I - itH - \frac{1}{2}t^2H^2 + O(t^3) \quad (\text{C4})$$

$$\approx I \otimes I - itH_S \otimes H_A - \frac{1}{2}t^2H_S^2 \otimes H_A^2 \quad (\text{C5})$$



This allows us to rewrite the time evolved combined system as follows,

$$|\Psi_t\rangle = (I \otimes I - itH_S \otimes H_A - \frac{1}{2}t^2 H_S^2 \otimes H_A^2) |\Psi_0\rangle \quad (C6)$$

When evaluating the effects of taking a quantum measurement, it's important to remember these following properties:

1. Quantum measurements can be described by a set of quantum operators  $\{M_q\}$
2. If the initial state of a quantum system is  $|\psi\rangle$ , then the probability that result  $q$  occurs is:  $p(q) = \langle\psi|M_q^\dagger M_q|\psi\rangle$
3. the state of the system after the quantum measurement will become:  $\frac{M_q|\psi\rangle}{\sqrt{\langle\psi|M_q^\dagger M_q|\psi\rangle}}$

In order for us to properly take a weak measurement of the system, we want to take a specific projective measurement that only acts on the ancilla state. Such a measurement can be described by

$$E_q = I \otimes |q\rangle\langle q| \quad (C7)$$

Projective measurements have the property that when applied to a composite system  $|\psi\rangle$ :  $p(q) = \langle\psi|E_q|\psi\rangle$  and the post-measurement system becomes

$$\frac{E_q|\psi\rangle}{\sqrt{p(m)}} \quad (C8)$$

Applying this measurement operator to our time evolved state, the post measurement state becomes:

$$|\Psi_q\rangle = \frac{E_q|\Psi_t\rangle}{\sqrt{\langle\Psi_t|E_q|\Psi_t\rangle}} \quad (C9)$$

$$= \frac{I\langle\varphi|q\rangle - itH_S\langle q|H_A|\varphi\rangle - \frac{1}{2}t^2 H_S^2\langle q|H_A^2|\varphi\rangle}{\sqrt{\langle\Psi_t|E_q|\Psi_t\rangle}} |\psi\rangle \otimes |q\rangle \quad (C10)$$

What we can do now is set

$$M_q := I\langle\varphi|q\rangle - itH_S\langle q|H_A|\varphi\rangle - \frac{1}{2}t^2 H_S^2\langle q|H_A^2|\varphi\rangle \quad (C11)$$

where  $M_q$  is called a Kraus operator. Returning back to deriving the weak measurement, we can describe our time evolved state with our Kraus operator below

$$|\Psi_q\rangle = \frac{E_q|\Psi_t\rangle}{\sqrt{\langle\Psi_t|E_q|\Psi_t\rangle}} = \frac{M_k|\psi\rangle}{\sqrt{\langle\psi|M_k^\dagger M_k|\psi\rangle}} \otimes |\varphi\rangle \quad (C12)$$

Note that the above postmeasurement state is a tensor product state, and therefore we may consider the state of the system alone, which is

$$|\psi_q\rangle = \frac{M_k|\psi\rangle}{\sqrt{\langle\psi|M_k^\dagger M_k|\psi\rangle}}. \quad (C13)$$

By using the unitary evolution of the joint Hilbert space, we see that projective measurements can satisfy the properties of quantum measurements as we've previously established.

We use a Krauss operator of the form

$$K_\theta = k \int_{-\infty}^{\infty} dX_\theta e^{-(X_\theta - \mu)^2/w^2} |X_\theta\rangle\langle X_\theta|, \quad (C14)$$

where  $k$  is a normalization constant that will not appear in the postmeasurement state. We apply the resolution of identity,

$$\mathbb{I} = \int dx |x\rangle\langle x| \quad (C15)$$

To represent the Kraus operator in the position basis:

$$\langle x|K_\theta|x'\rangle = k \int_{-\infty}^{\infty} dX_\theta e^{-(X_\theta - \mu)^2/w^2} \langle x|X_\theta\rangle \langle X_\theta|x'\rangle. \quad (\text{C16})$$

From B17 we can express this as,

$$\langle x|K_\theta|x'\rangle = \frac{k}{2\pi\hbar\sin\theta} \int_{-\infty}^{\infty} dX_\theta e^{-(X_\theta - \mu)^2/w^2} \exp\left(-\frac{i}{2\hbar}(x^2 - x'^2)\cot(\theta) + \frac{i}{\hbar}(x - x')X_\theta\csc(\theta)\right) \quad (\text{C17})$$

$$= \frac{k}{2\pi\hbar\sin\theta} w\sqrt{\pi} \exp\left(\frac{1}{4\hbar^2}(x - x')\csc(\theta)[4i\mu\hbar - 2i(x + x')\hbar\cos(\theta) + w^2(x' - x)\csc(\theta)]\right) \quad (\text{C18})$$

Kraus operators are useful in scenarios such that if a coupled or joined system undergoes unitary evolution, we can use Kraus operators to describe how a specific subset of the system evolves in time. For example, if we take an initial system  $|\psi\rangle \otimes |\varphi\rangle$ , it will evolve as follows

$$|\psi\rangle \otimes |\varphi\rangle \rightarrow \frac{M_k |\psi\rangle}{\sqrt{\langle\psi|M_k^\dagger M_k|\psi\rangle}} \otimes |\varphi\rangle \quad (\text{C19})$$

If we now want to analyze just  $|\psi\rangle$ , we can represent the initial state through density matrices.

$$|\psi\rangle \langle\psi| \otimes |\varphi\rangle \langle\varphi| \rightarrow \sum_{k,l} M_k |\psi\rangle \langle\psi| M_l^\dagger \otimes |\varphi_k\rangle \langle\varphi_l| \quad (\text{C20})$$

By performing a partial trace with respect to  $\varphi$ ,

$$|\psi\rangle \langle\psi| \rightarrow \sum_{k,l} M_k |\psi\rangle \langle\psi| M_l^\dagger \langle\varphi_l|\varphi_k\rangle \quad (\text{C21})$$

$$= \sum_k M_k |\psi\rangle \langle\psi| M_k^\dagger \quad (\text{C22})$$

Unlike the combined system which evolves under unitary transformation, a subsystem evolution can be described as

$$\rho \rightarrow \sum_k M_k \rho M_k^\dagger \quad (\text{C23})$$