A quantum algorithm for semidirect product discrete logarithm on elliptic curves

Muhammad Imran
Institute of Mathematics, Department of Algebra,
Budapest University of Technology and Economics,
Műegyetem rkp. 3., Budapest, H-1111, Hungary.
E-mail: mimran@math.bme.hu

July 5, 2023

Abstract

Shor's algorithm solves the discrete logarithm problem (DLP) efficiently by taking advantage of the commutativity structure of the group underlying the problem. To counter Shor's algorithm, Horan *et al.* propose a DLP analogue in the semidirect product semigroup $G \rtimes \mathrm{End}(G)$, given a (semi)group G, to construct a quantum-resistant Diffie-Hellman key exchange based on it. For general (semi)groups, the semidirect product discrete logarithm problem (SPDLP) can be reduced to the hidden shift problem where Kuperberg's subexponential quantum algorithm is applicable. In this paper, we consider a specific case where G is an elliptic curve over a finite field and we show that SPDLP on elliptic curves can be solved efficiently using an adaptation of Shor's algorithm for the standard elliptic curve discrete logarithm problem (ECDLP). This result points out that one should not use elliptic curves as the platforms for the semidirect product key exchange.

Keywords: Quantum algorithm, Semidirect product discrete logarithm, Elliptic curves.

1 Introduction

The presumed difficulty of computing discrete logarithm problem (DLP) in certain groups is essential for the security of Diffie-Hellman key exchange which is the basis for a number of communication protocols deployed today. One of the modern choice is a group of rational points of an elliptic curve defined over a finite field, which is the centre of elliptic curve cryptography, one of the most popular public key cryptography today. However, since the invention of Shor's algorithm [Sho94], the problem of computing discrete logarithm can be solved efficiently in the domain of quantum computing.

A massive efforts has been done in order to construct a DLP analogue for constructing Diffie-Hellman key exchange in which Shor's algorithm is not applicable. Since Shor's algorithm takes advantage of the group structure underlying the problem, a DLP analoge in the framework of commutative group actions has been proposed. It is called the *vectorization problem.* The framework originally appears in [Cou06] and it becomes a centre of isogeny based cryptography, CSIDH [CLM$^+$18] for example.

Another natural approach which is worth consideration to escape from the quantum attack is a DLP analogue in non-commutative groups. It is natural in a sense that Shor's algorithm crucially depends on the commutativity of the underlying groups. A promising proposal for this direction is to use semidirect product groups which firstly appears in its full generality in [HKKS13].

Specifically, let G be a group and $\mathrm{Aut}(G)$ be the group of automorphisms of G. Then we have the holomorph of G as the semidirect product $G \rtimes \mathrm{Aut}(G)$ where the multiplication is defined by $(g, \phi)(h, \psi) = (g\phi(h), \phi\psi)$. Moreover, we have a formula for exponentiation

$$(g, \phi)^n = \left(\prod_{i=0}^{n-1} \phi^{n-(i+1)}(g), \phi^n \right).$$

This leads us to a discrete logarithm analogue in the semidirect product group defined as follows.

Problem 1 (Semidirect product discrete logarithm problem (SPDLP))**.** *Given $g \in G, \phi \in \mathrm{Aut}(G)$, and $A = \prod_{i=0}^{n-1} \phi^{n-(i+1)}(g)$ for some integer n. Find n.*

SPDLP is interesting as it allows us to perform a Diffie-Hellman key exchange procedure as follows. Suppose two parties, Alice and Bob, agree on a public group G, an element $g \in G$, and an automorphism $\phi \in \mathrm{Aut}(G)$. Then they can arrive at the same $G-$element:

1. Alice picks a random positive integer x and computes $(g, \phi)^x = (A, \phi^x)$. Then, Alice sends $A = \prod_{i=0}^{x-1} \phi^{x-(i+1)}(g)$ to Bob.

2. Bob also picks a random positive integer y, computes $(g, \phi)^y = (B, \phi^y)$ and sends $B = \prod_{i=0}^{y-1} \phi^{y-(i+1)}(g)$ to Alice.

3 Alice computes its shared key $K_A = \varphi^x(B)A$.

4 Bob computes its shared key $K_B = \varphi^y(A)B$.

Note that $K_A = K_B$ based on the following computations

$$\begin{aligned}
\varphi^x(B)A &= \prod_{i=0}^{y-1} \varphi^{x+y-i-1}(P) \prod_{i=0}^{x-1} \varphi^{x-i-1}(P) \\
&= \prod_{i=0}^{x-1} \varphi^{x+y-i-1}(P) \prod_{i=0}^{y-1} \varphi^{y-i-1}(P) \\
&= \varphi^y(A)B.
\end{aligned}$$

The problem above can even be generalized to a semigroup G by taking the semigroup of endomorphisms $\mathrm{End}(G)$ under the composition operation instead of $\mathrm{Aut}(G)$.

Battarbee *et al* [BKPS22] present a subexponential quantum attack for SPDLP by giving a reduction to the vectorization problem and hence use the fact that the vectorization problem reduces to the Abelian hidden shift problem in which Kuperbeg's subexponential time algorithm [Kup05] is available.

There are several proposed platforms for SPDLP including matrices over group rings $M_3(\mathbb{Z}_7[A_5])$ [HKKS13], free nilpotent p-group [KS16], tropical algebra [GS14, GS19], matrices over finite filed $\mathbb{Z}_p$ [RS22], and matrices over bit strings [RS21]. Some of the proposed platforms are vulnerable by some attacks using the structure of the platforms. See [BKS22] for more detailed survey on the semidirect product key exchange.

In this paper, we consider SPDLP on elliptic curves. Particularly, we consider the semidirect product $E \rtimes \mathrm{End}(E)$ where E is an elliptic curve. Moreover, we show that SPDLP on elliptic curves can be solved efficiently using an adaptation of the standard Shor's quantum algorithm for discrete logarithm problem.

2 Preliminaries

2.1 Elliptic curves

For standard notations and concepts of elliptic curves, we refer the reader to the textbooks, e.g., [Sil09]. Let $\mathbb{F}_p$ be a finite field of characteristic p and $\overline{\mathbb{F}}_p$ be the algebraic closed field of $\mathbb{F}_p$. In the following we assume $p > 3$ and therefore an elliptic curve E over $\mathbb{F}_p$ can be defined by its short Weierstrass form

$$E(\overline{\mathbb{F}}_p) = \{(x, y) \in \overline{\mathbb{F}}_p^2 \mid y^2 = x^3 + ax + b\} \cup \{O_E\}$$

where $a, b \in \mathbb{F}_p$ such that $4a^3 + 27b^2 \neq 0$ and O_E is the point $(X : Y : Z) = (0 : 1 : 0)$ on the associated projective curve. The set of points of an elliptic curve forms an abelian group with the chord and tangent rule: *three points of E on a line sum to zero, which is the point at infinity O_E.*

For any pair E_1 and E_2 of elliptic curves over $\mathbb{F}_p$, the group $\mathrm{Hom}(E_1, E_2)$ consists of all morphisms of curves $E_1 \to E_2$ that are also group homomorphisms of $E_1(\overline{\mathbb{F}}_p) \to E_2(\overline{\mathbb{F}}_p)$, such a curve morphism is also called *isogeny*. Given $\varphi \in \mathrm{Hom}(E_1, E_2)$, the degree of φ is the degree as a curve morphism and we have the dual of φ denoted by $\varphi \in \mathrm{Hom}(E_2, E_1)$ such that $\varphi \circ \widehat{\varphi} = \widehat{\varphi} \circ \varphi = \deg \varphi$.

The endomorphism ring of an elliptic curve E is defined as $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ with multiplication defined by composition $\alpha\beta = \alpha \circ \beta$. For any $\alpha \in \mathrm{End}(E)$, we have $\mathrm{tr}(\alpha) = \alpha + \widehat{\alpha} = 1 + \deg(\alpha) - \deg(1 - \alpha)$. This can be shown directly using the fact that $\widehat{(\alpha + \beta)} = \widehat{\alpha} + \widehat{\beta}$. Thus,

$$\deg(1 - \alpha) = (1 - \alpha)(\widehat{1} - \widehat{\alpha}) = 1 - (\alpha + \widehat{\alpha}) + \deg(\alpha).$$

Moreover, both of α and its dual $\widehat{\alpha}$ are the roots of the quadratic polynomial

$$\lambda^2 - \mathrm{tr}(\alpha)\lambda + \deg(\alpha).$$

Indeed, as $\alpha^2 - \mathrm{tr}(\alpha)\alpha + \deg(\alpha) = \alpha^2 - (\alpha + \widehat{\alpha})\alpha + \alpha\widehat{\alpha} = 0$.

The group $\mathrm{Aut}(E)$ of authomorphisms of E consists of all invertible endomorphisms α of E, i.e., there exists $\beta \in \mathrm{End}(E)$ such that $\alpha\beta = \beta\alpha = 1$. The group of automorphism of elliptic curves over a field K is well known and it has order dividing 24. It is classified based on the j-invarian of $E : y^2 = x^3 + ax + b$ which is defined as $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$ and the character of the underlying field. Particularly we have the following classifications.

$\lvert\mathrm{Aut}(E)\rvert$	$j(E)$	$\mathrm{char}(K)$
2	$j(E) \neq 0, 1728$	-
4	$j(E) = 1728$	$\mathrm{char}(K) \neq 2, 3$
6	$j(E) = 0$	$\mathrm{char}(K) \neq 2, 3$
12	$j(E) = 0, 1728$	$\mathrm{char}(K) = 3$
24	$j(E) = 0, 1728$	$\mathrm{char}(K) = 2$

2.2 Shor's algorithm for discrete logarithm problem

Shor's algorithm for DLP uses the fact that the problem can be translated to the problem of finding period of a function. Particularly, let G be a group and $g \in G$. Given $h \in \langle g \rangle$, we would like to find the smallest integer a such that $g^a = h$. Hence, we have an equivalent problem as follows. Let $N = \mathrm{ord}(x)$. We define the function $f(x, y) = g^x h^y$ on $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Note that $f(x, y) = f(x', y')$ if and only if $(x - x', y - y') \in \langle (a, -1) \rangle$. Thus, finding the period of f on the group $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ solves the corresponding DLP.

The latter problem is also called the hidden subgroup problem on $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. The key tool of the quantum algorithm is *Fourier sampling method.* The details of the quantum algorithm is out of scope of this work, we refer the readers to [DW19] for example. Proos and Zalka [PZ03] present a specific case of Shor's algorithm for elliptic curve discrete logarithm problem.

3 A quantum algorithm for SPDLP on elliptic curves

We consider the semidirect key-exchange using supersingular elliptic curves and its endomorphism rings. Namely, given a supersingular elliptic curve E, we have semigroup $G = E \rtimes \mathrm{End}(E)$ where the multiplication is defined by $(P, \varphi)(Q, \psi) = (P + \varphi(Q), \varphi\psi)$. Therefore, we have the formula for

$$(P, \varphi)^n = \left(\sum_{i=0}^{n-1} \varphi^{n-i-1}(P), \varphi^n \right).$$

We consider the discrete logarithm problem in this group which is defined as follows.

Problem 2. *Given a supersingular elliptic curve E, $P \in E$, $\varphi \in \mathrm{End}(E)$, and an element of the form $A = \sum_{i=0}^{n-1} \varphi^{n-i-1}(P)$ for some integer n. The task is to find n.*

3.1 Easiest instances

First we observe the easiest instances of problem 2. If φ is the identity endomorphism, then problem 2 is the standard elliptic curve discrete logarithm problem (ECDLP). Moreover, if φ is an endomorphism given by a scalar multiplication $[m]$, then

$$A = \sum_{i=0}^{n-1} \left[m^{n-(i+1)}\right] P = \left[\frac{m^n - 1}{m-1}\right] P.$$

Hence, knowing P and m will reveal n by Shor's algorithm. Specifically, we can use the standard Shor's algorithm to $[m-1]A + P = [m^n]\,P$ to get m^n. Thus, another application of Shor's algorithm on m^n with the knowledge of m will reveal n.

Another straight forward applications of Shor's algorithm can be done when φ is an automorphism of E. Recall that given an elliptic curve over a finite field, the endomorphism ring $\mathrm{End}(E)$ has order at most 24. Let φ be an automorphism of order $m \leq 24$ and let $Q = \sum_{i=0}^{m-1} \varphi^i(P)$. Then $A = \sum_{i=0}^{n-1} \varphi^{n-i-1}(P)$ is one of $kQ, kQ + P, kQ + P + \varphi(P), \ldots, kQ + \sum_{i=0}^{m-2} \varphi^i(P)$ where $k = \lfloor n/m \rfloor$. Hence, one can reveal n by at most m applications of Shor's algorithm.

3.2 General endomorphisms

Recall that any endomorphism $\varphi \in \mathrm{End}(E)$ satisfies $\varphi^2 = \mathrm{tr}(\varphi)\varphi - \deg \varphi$. Hence, we have the recursive formula $\varphi^n = \mathrm{tr}(\varphi)\varphi^{n-1} - \deg(\varphi)\varphi^{n-2}$ and the summation $A = \sum_{i=0}^{n-1} \varphi^{n-i-1}(P)$ can be simplified as a linear combination of P and $\varphi(P)$, i.e.,

$$A = a_n(t,d)P + b_n(t,d)\varphi(P),$$

where a_n and b_n are polynomial in $t = \mathrm{tr}(\varphi)$ and $d = \deg(\varphi)$. If we can explicitly write down the formula for a_n and b_n, then we can solve the problem 2 using the generalization of Shor's algorithm for the abelian hidden subgroup problem on the subgroup $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ where $m = \mathrm{lcm}\left(\mathrm{ord}(P), \mathrm{ord}(\varphi(P)\right)$ using the following hiding function

$$F(x,y) = a_x(t,d)P + b_x(t,d)\varphi(P) + yA,$$

where the hidden subgroup is $\langle (n, -1) \rangle$.

If we expand the recursive function $\varphi^n = \mathrm{tr}(\varphi)\varphi^{n-1} - \deg(\varphi)\varphi^{n-2}$ to get a linear function of φ, we know that the coefficient of φ in the expansion satisfies the recursive function $f(n) = \mathrm{tr}(\varphi)f(n-1) - \deg(\varphi)f(n-2)$ where $f(1) = 1$ and $f(2) = \mathrm{tr}(\varphi)$. Hence, we can write it in the matrix form as $F_n = M \cdot F_{n-1}$ where

$$F_n = \begin{pmatrix} f(n) \\ f(n-1) \end{pmatrix}, \text{ and } M = \begin{pmatrix} \mathrm{tr}(\varphi) & -\deg(\varphi) \\ 1 & 0 \end{pmatrix}.$$

Therefore, we have $F_n = M^n \cdot F_1$, where $F_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

By the above discussion, Calculating M^n will give the explicit formula for the coefficient of φ in the expansion of φ^n. This can be done using eigenvalue decomposition of M. Let V be the matrix of eigenvectors of M and D be the diagonal matrix of eigenvalues of M. Then $M = V \cdot D \cdot V^{-1}$ and thus $M^n = V \cdot D^n \cdot V^{-1}$. Therefore, by summing up all the explicit formula for φ^i for $0 \leq i \leq n-1$, we have the explicit formula for $b_n(t,d)$.

Similar computations using the recursive function $f(n) = \mathrm{tr}(\varphi)f(n-1) - \deg(\varphi)f(n-2)$ where $f(1) = 0$ and $f(2) = -\deg(\varphi)$, will give $F_n = M^n \cdot F_2$ where $F_2 = \begin{pmatrix} -d \\ 0 \end{pmatrix}$, the explicit formula for the scalar in the expansion of φ^n. Hence, we can also obtain the explicit formula for $a_n(t,d)$ in the similar way as $b_n(t,d)$.

Finally, the task left to be done is the problem of computing $\mathrm{tr}(\varphi)$, given an endomorphism φ of E. Kohel shows in theorem 81 of [Koh96] that there exists a polynomial time algorithm that can compute the trace of a given endomorphism using a modified Schoof's algorithm. Furthermore, Wills [Wil21] presents an explicit algorithm built upon Kohel's result.

4 Conclusion

The semidirect product discrete logarithm problem on elliptic curves can be seen as a natural generalization of the standard elliptic curve discrete logarithm problem. However, prior to this work, elliptic curves have never been considered as a platform for the semidirect product key exchange which was introduced in [HKKS13]. One of the reasons might be that this requires an efficient way to generate and evaluate an endomorphism of a given elliptic curve E on arbitrary point of E. As shown by Wesolowski [Wes22], generating a random endomorphism is as hard as computing the full endomorphism ring which is a central problem in isogeny-based cryptography. Moreover, given an endomorphism of E, it is not clear how to efficiently evaluate the endomorphism on arbitrary points of E. This depends on how the endomorphism is represented.

The two obstacles can be fixed by using some efficient tools developed in isogeny-based cryptography. Particularly, Petit and Lauter in [PL17] present an algorithm that given a prime $p > 2$ computes a supersingular elliptic curve E such that $\mathrm{End}(E)$ is isomorphic to a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ as classified by Pizer [Piz80]. This way, we can efficiently generate and evaluate a random endomorphism of E which is represented as an element of the quaternion algebra.

Unfortunately, as we analyzed the complexity of the semidirect product discrete logarithm problem in $E \rtimes \mathrm{End}(E)$ for arbitrary elliptic curves E, we show that the structure of endomorphisms of elliptic curves allows us to efficiently solve the SPDLP on $E \rtimes \mathrm{End}(E)$ using an adaptation of Shor's algorithm. Therefore, one should not use elliptic curves for semidirect product key exchange for post-quantum cryptography.

References

[BKPS22] Christopher Battarbee, Delaram Kahrobaei, Ludovic Perret, and Siamak F Shahandashti. A subexponential quantum algorithm for the semidirect discrete logarithm problem. In *NIST Fourth PQC Standardization Conference*, 2022.

[BKS22] Christopher Battarbee, Delaram Kahrobaei, and Siamak F Shahandashti. Semidirect product key exchange: the state of play. *arXiv preprint arXiv:2202.05178*, 2022.

[CLM$^+$18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: an efficient post-quantum commutative group action. In *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24*, pages 395–427. Springer, 2018.

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. *Cryptology ePrint Archive*, 2006.

[DW19] Ronald De Wolf. Quantum computing: Lecture notes. *arXiv preprint arXiv:1907.09415*, 2019.

[GS14] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography. *Communications in Algebra*, 42(6):2624–2632, 2014.

[GS19] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography ii: extensions by homomorphisms. *Communications in Algebra*, 47(10):4224–4229, 2019.

[HKKS13] Maggie Habeeb, Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain. Public key exchange using semidirect product of (semi) groups. In *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11*, pages 475–486. Springer, 2013.

[Koh96] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields.* University of California, Berkeley, 1996.

[KS16] Delaram Kahrobaei and Vladimir Shpilrain. Using semidirect product of (semi) groups in public key cryptography. In *Pursuit of the Universal: 12th Conference on Computability in Europe, CiE 2016, Paris, France, June 27-July 1, 2016, Proceedings*, pages 132–141. Springer, 2016.

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

[Piz80] Arnold Pizer. An algorithm for computing modular forms on $\gamma 0$ (n). *Journal of algebra*, 64(2):340–390, 1980.

[PL17] Christophe Petit and Kristin Lauter. Hard and easy problems for supersingular isogeny graphs. *Cryptology ePrint Archive*, 2017.

[PZ03] J Proos and Ch Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Information and Computation*, 3(4):317–344, 2003.

[RS21] Nael Rahman and Vladimir Shpilrain. Mobs (matrices over bit strings) public key exchange. *arXiv preprint arXiv:2106.01116*, 2021.

[RS22] Nael Rahman and Vladimir Shpilrain. Make: A matrix action key exchange. *Journal of Mathematical Cryptology*, 16(1):64–72, 2022.

[Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Wes22] Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. In *Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part III*, pages 345–371. Springer, 2022.

[Wil21] Michael Thomas Wills. *Computing the trace of an endomorphism of a supersingular elliptic curve.* PhD thesis, Virginia Tech, 2021.