

On the Design and Optimization of a Quantum Polynomial-Time Attack on Elliptic Curve Cryptography

Donny Cheung¹, Dmitri Maslov¹, Jimson Mathew², and Dhiraj K. Pradhan²

¹ Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada

² Department of Computer Science, University of Bristol, Bristol, BS8 1UB, UK

Abstract. We consider a quantum polynomial-time algorithm which solves the discrete logarithm problem for points on elliptic curves over $GF(2^m)$. We improve over earlier algorithms by constructing an efficient circuit for multiplying elements of binary finite fields and by representing elliptic curve points using a technique based on projective coordinates. The depth of our proposed implementation is $O(m^2)$, which is an improvement over the previous bound of $O(m^3)$.

1 Introduction

Quantum computing [1] has the ability to solve problems whose best classical solutions are considered inefficient. Perhaps the best-known example is Shor's polynomial-time integer factorization algorithm [2], where the best known classical technique, the General Number Field Sieve, has superpolynomial complexity $\exp O(\sqrt[3]{n \log^2 n})$ in the number of bits n [3]. Since a hardware implementation of this algorithm on a suitable quantum mechanical system could be used to crack the RSA cryptosystem [3], these results force researchers to rethink the assumptions of classical cryptography and to consider optimized circuits for the two main parts of Shor's factorization algorithm: the quantum Fourier transform [1, 4] and modular exponentiation [5]. Quantum noise and issues of scalability in quantum information processing proposals require circuit designers to consider optimization carefully.

Since the complexity of breaking RSA is subexponential, cryptosystems such as Elliptic Curve Cryptography (ECC) have become increasingly popular. The best known classical attack on ECC requires an exponential search with complexity $O(2^{n/2})$. The difference is substantial: a 256-bit ECC key requires the same effort to break as a 3072-bit RSA

key. The largest publicly broken ECC system has a key length of 109 bits [6], while the key lengths of 1024 bits and higher are strongly recommended for RSA. ECC has been recently acknowledged by National Security Agency as a secure protocol and included in their Suite B [7]. Most ECC implementations are built over $GF(2^m)$. Software implementations, such as ECC over $GF(2^{155})$, are also publicly available [8].

However, there does exist a quantum polynomial-time algorithm that cracks elliptic curve cryptography [9]. As with Shor's factorization algorithm, this algorithm should be studied in detail by anyone interested in studying the threat posed by quantum computing to ECC. The quantum algorithm for solving discrete logarithm problems in cyclic groups such as the one used in ECC requires computing sums and products of finite field elements, such as $GF(2^m)$ [10]. Addition in $GF(2^m)$ requires only a depth-1 circuit consisting of parallel CNOT gates [11]. We present a depth $O(m)$ multiplication circuit for $GF(2^m)$ based on the construction by Mastrovito [12]. Previously, a depth $O(m^2)$ circuit was given in [11].

In Section 2 we give an overview of quantum computation, $GF(2^m)$ field arithmetic, and elliptic curve arithmetic. Section 3 outlines the quantum algorithm, and presents our improvements: the $GF(2^m)$ multiplication circuit, and projective coordinate representation. The paper concludes with some observations and suggestions for further research.

2 Preliminaries

We will be working in the quantum circuit model, where data is stored in qubits and unitary operations are applied to various qubits at discrete time steps as quantum gates. We assume that any set of non-intersecting gates may be applied within one time step. The total number of time steps required to execute an algorithm as a circuit is the *depth*. Further details on quantum computation in the circuit model can be found in [1].

We will make use of the CNOT and Toffoli gates. The CNOT gate is defined as the unitary operator which performs the transformation $|a\rangle|b\rangle \mapsto |a\rangle|a \oplus b\rangle$. The Toffoli gate [13] can be described as a controlled CNOT gate, and performs the transformation over the computational basis given by the formula $|a\rangle|b\rangle|c\rangle \mapsto |a\rangle|b\rangle|c \oplus ab\rangle$.

2.1 Binary Field Arithmetic

The finite field $GF(2^m)$ consists of a set of 2^m elements, with an addition and multiplication operation, and additive and multiplicative identities

0 and 1, respectively. $GF(2^m)$ forms a commutative ring over these two operations where each non-zero element has a multiplicative inverse. The finite field $GF(2^m)$ is unique up to isomorphism.

We can represent the elements of $GF(2^m)$ where $m \geq 2$ with the help of an irreducible *primitive polynomial* of the form $P(x) = \sum_{i=0}^{m-1} c_i x^i + x^m$, where $c_i \in GF(2)$ [14]. The finite field $GF(2^m)$ is isomorphic to the set of polynomials over $GF(2)$ modulo $P(x)$. In other words, elements of $GF(2^m)$ can be represented as polynomials over $GF(2)$ of degree at most $m - 1$, where the product of two elements is the product of their polynomial representations, reduced modulo $P(x)$ [14, 15]. As the sum of two polynomials is simply the bitwise XOR of the coefficients, it is convenient to express these polynomials as bit vectors of length m . Additional properties of finite fields can be found in [14].

Mastrovito has proposed an algorithm along with a classical circuit implementation for polynomial basis (PB) multiplication [12, 16], popularly known as the Mastrovito multiplier. Based on Mastrovito algorithm, [15] presents a formulation of PB multiplication and a generalized parallel-bit hardware architecture for special types of primitive polynomials, namely trinomials, equally spaced polynomials (ESPs), and two classes of pentanomials.

Consider the inputs \mathbf{a} and \mathbf{b} , with $\mathbf{a} = [a_0, a_1, a_2, \dots, a_{m-1}]^T$ and $\mathbf{b} = [b_0, b_1, b_2, \dots, b_{m-1}]^T$, where the coordinates a_i and b_i , $0 \leq i < m$, are the coefficients of two polynomials $A(x)$ and $B(x)$ representing representing two elements of $GF(2^m)$ with respect to a primitive polynomial $P(x)$. We use three matrices in this construction:

1. an $m \times (m - 1)$ reduction matrix Q ,
2. an $m \times m$ lower triangular matrix L , and
3. an $(m - 1) \times m$ upper triangular matrix U .

We define vectors \mathbf{d} and \mathbf{e} as:

$$\mathbf{d} = L\mathbf{b} \tag{1}$$

$$\mathbf{e} = U\mathbf{b}, \tag{2}$$

where L and U are defined as

$$L = \begin{bmatrix} a_0 & 0 & \dots & 0 & 0 \\ a_1 & a_0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m-2} & a_{m-3} & \dots & a_0 & 0 \\ a_{m-1} & a_{m-2} & \dots & a_1 & a_0 \end{bmatrix}, \quad U = \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \dots & 0 & a_1 \\ 0 & 0 & a_{m-1} & \dots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{m-1} & a_{m-2} \\ 0 & 0 & 0 & \dots & 0 & a_{m-1} \end{bmatrix}.$$

Note that \mathbf{d} and \mathbf{e} correspond to polynomials $D(x)$ and $E(x)$ such that $A(x)B(x) = D(x) + x^m E(x)$. Using $P(x)$, we may construct a matrix Q which converts the coefficients of any polynomial $x^m E(x)$ to the coefficients of an equivalent polynomial modulo $P(x)$ with degree less than m . Thus, the vector

$$\mathbf{c} = \mathbf{d} + Q\mathbf{e} \tag{3}$$

gives the coefficients of the polynomial representing the product of \mathbf{a} and \mathbf{b} . The construction of the matrix Q , which is dependent on the primitive polynomial $P(x)$, is given in [15].

2.2 Elliptic Curve Groups

In the most general case, we define an *elliptic curve* over a field F as the set of points $(x, y) \in F \times F$ which satisfy the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5.$$

By extending this curve to the projective plane, we may include the point at infinity \mathcal{O} as an additional solution. By defining a suitable addition operation, we may interpret the points of an elliptic curve as an Abelian group, with \mathcal{O} as the identity element.

In the specific case of the finite field $GF(2^m)$, it is possible to reduce the degrees of freedom in the coefficients defining the elliptic curve by the use of linear transformations on the variables x and y . In addition, it was shown in [17] that for a class of elliptic curves called *supersingular* curves, it is possible to reduce the discrete logarithm problem for the elliptic curve group to a discrete logarithm problem over a finite field in such a way that makes such curves unsuitable for cryptography. For $GF(2^m)$, these correspond to elliptic curves with parameter $a_1 = 0$. We will restrict our attention to non-supersingular curves over $GF(2^m)$, which are of the form $y^2 + xy = x^3 + ax^2 + b$, where $b \neq 0$.

The set of points over an elliptic curve also forms an Abelian group with \mathcal{O} as the identity element. For a non-supersingular curve over $GF(2^m)$, the group operation is defined in the following manner. Given a point $P = (x_1, y_1)$ on the curve, we define $(-P)$ as $(x_1, x_1 + y_1)$. Given a second point $Q = (x_2, y_2)$, where $P \neq \pm Q$, we define the sum $P + Q$ as the point (x_3, y_3) where $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$ and $y_3 = (x_1 + x_3)\lambda + x_3 + y_1$, with $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$. When $P = Q$, we define $2P$ as the point (x_3, y_3) where $x_3 = \lambda^2 + \lambda + a$ and $y_3 = x_1^2 + \lambda x_3 + x_3$, with $\lambda = x_1 + \frac{y_1}{x_1}$. Also, any group operation involving \mathcal{O} simply conforms to the properties of a group

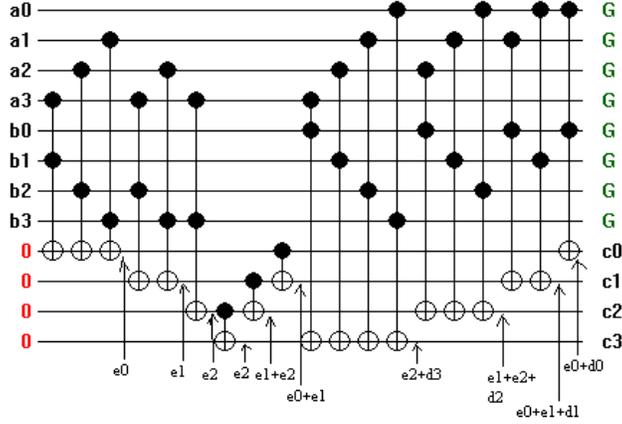


Fig. 1. Circuit for $GF(2^4)$ multiplier with $P(x) = x^4 + x + 1$

identity element. Finally, scalar multiplication by an integer can be easily defined in terms of repeated addition or subtraction.

The elliptic curve discrete logarithm problem (ECDLP) is defined as the problem of retrieving a constant scalar d given that $Q = dP$ for known points P and Q . With this definition, we may define cryptographic protocols using the ECDLP by modifying analogous protocols using the discrete logarithm problem over finite fields.

3 Quantum Polynomial-Time Attack

With a reversible implementation for the basic elliptic curve group operations, it is possible to solve the ECDLP with a polynomial-depth quantum circuit. Given a base point P and some scalar multiple $Q = dP$ on an elliptic curve over $GF(2^m)$, Shor's algorithm for discrete logarithms [2] constructs the state

$$\frac{1}{2^m} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^m-1} |x\rangle |y\rangle |xP + yQ\rangle,$$

then performs a two-dimensional quantum Fourier transform over the first two registers. It was shown in [9] that this task can be reduced to adding a classically known point to a superposition of points.

3.1 Linear-Depth Circuit for $GF(2^m)$ Multiplication

We now discuss how to implement multiplication over $GF(2^m)$ as a quantum circuit. We perform the following steps:

1. Using equations (1-3), derive expressions for \mathbf{d} , \mathbf{e} and \mathbf{c} .
2. Compute \mathbf{e} in an ancillary register of m qubits.
3. Transform \mathbf{e} into $Q\mathbf{e}$, using a linear reversible implementation.
4. Compute and add \mathbf{d} to the register occupied by $Q\mathbf{e}$.

We illustrate the above steps with an example using $P(x) = x^4 + x + 1$.

1. Expressions for \mathbf{d} and \mathbf{e} derived from equations (1-2) are shown below.

$$\mathbf{d} = \begin{bmatrix} a_0b_0 \\ a_1b_0 + a_0b_1 \\ a_2b_0 + a_1b_1 + a_0b_2 \\ a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \end{bmatrix}, \quad \mathbf{e} = \begin{bmatrix} a_3b_1 + a_2b_2 + a_1b_3 \\ a_3b_2 + a_2b_3 \\ a_3b_3 \end{bmatrix}.$$

We also construct the matrix $Q = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

From (3), we compute the multiplier output

$$\mathbf{c} = \mathbf{d} + Q\mathbf{e} = \begin{bmatrix} d_0 + e_0 \\ d_1 + e_1 + e_0 \\ d_2 + e_1 + e_2 \\ d_3 + e_2 \end{bmatrix}.$$

2. We first compute e_0 , e_1 , and e_2 in the ancilla, as shown in Figure 1 (gates 1-6).
3. We next implement the matrix transformation $Q\mathbf{e}$ (gates 7-9).
4. Finally, we compute the coefficients d_i , $0 \leq i < m$, and add them to the ancilla to compute \mathbf{c} (gates 10-19).

At this point, we have a classical reversible circuit which implements the transformation $|a\rangle |b\rangle |0\rangle \mapsto |a\rangle |b\rangle |a \cdot b\rangle$. However, if we input a superposition of field elements, then the output register will be entangled with the input. If one of the inputs, such as $|b\rangle$ is classically known, then we may also obtain $|b^{-1}\rangle$ classically. Since we may construct a circuit which maps $|a \cdot b\rangle |b^{-1}\rangle |0\rangle \mapsto |a \cdot b\rangle |b^{-1}\rangle |a\rangle$, we may apply the inverse of this circuit to the output of the first circuit to obtain $|a\rangle |b\rangle |a \cdot b\rangle \mapsto |0\rangle |b\rangle |a \cdot b\rangle$ using an ancilla set to $|b^{-1}\rangle$. This gives us a quantum circuit which takes

a quantum input $|a\rangle$ and classical input $|b\rangle$, and outputs $|a \cdot b\rangle |b\rangle$. When $|b\rangle$ is not a classical input, the output of the circuit may remain entangled with the input, and other techniques may be required to remove this entanglement. However, we emphasize that this is not required for a polynomial-time quantum algorithm for the ECDLP [9].

This technique can be applied for any primitive polynomial $P(x)$. In some circumstances, we may derive exact expressions for the number of gates required.

Lemma 1. *A binary field multiplier for primitive polynomial $P(x)$ can be designed using at most $2m^2 - 1$ gates. If $P(x)$ is a trinomial or an all-one polynomial, where each coefficient is 1, we require only $m^2 + m - 1$ gates.*

Proof. There are three phases to the computation: computing \mathbf{e} , computing $Q\mathbf{e}$, and adding \mathbf{d} to the result. For \mathbf{e} and \mathbf{d} , each pair of coefficients which are multiplied and then added to another qubit requires one Toffoli gate. This requires

$$\sum_{i=0}^{m-1} i = \frac{m(m-1)}{2}, \text{ and } \sum_{i=0}^m i = \frac{m(m+1)}{2}$$

gates respectively, for a total of m^2 gates. Now, we consider the implementation of the transformation Q .

In general, $m^2 - 1$ CNOT gates suffice for any linear reversible computation defined by the matrix Q in equation (3) [18]. This gives a general upper bound of $2m^2 - 1$ gates. In the specific case of the All-One-Polynomial, the operation Q consists of adding e_1 to each of the other qubits, requiring $m - 1$ CNOT operations. This gives a total of $m^2 + m - 1$ operations.

For a trinomial, we have a primitive polynomial $P(x) = x^m + x^k + 1$ for some constant k such that $1 \leq k < m$. To upper bound the number of gates required to implement Q , we may consider the inverse operation, in which we begin with a polynomial of degree at most $m - 1$, and we wish to find an equivalent polynomial where each term has degree between $m - 1$ and $2m - 2$. Increasing the minimum degree of a polynomial requires one CNOT operation, and this must be done $m - 1$ times. Again, this gives a total of $m^2 + m - 1$ operations.

3.2 Parallelization

We construct a parallelized version of this network by considering the three parts of the computation: \mathbf{e} , $Q\mathbf{e}$ and adding \mathbf{d} . For \mathbf{e} and \mathbf{d} , note

that given coefficients a_i and b_j where the value of $i - j$ is fixed, the target qubit of each separate term $a_i b_j$ is different. This means that they may be performed in parallel. In the case of \mathbf{e} , we evaluate $a_i b_j$ whenever $i + j \geq m$. This means that the values of $i - j$ may range from $-(m - 2)$ to $m - 2$, giving a depth $2m - 3$ circuit for finding e . Similarly, for \mathbf{d} , we evaluate $a_i b_j$ whenever $i + j < m$. The values of $i - j$ range from $-(m - 1)$ to $m - 1$, giving a depth $2m - 1$ circuit.

To compute $Q\mathbf{e}$, at most $m^2 - 1$ CNOT gates are used. In [18], it is shown that such a computation can be done in a linear number of stages, with a depth of $6m + O(1)$. This gives us a total depth of $10m + O(1)$ for the multiplication circuit. An implementation which replaces the Toffoli gate with 1- and 2-qubit gates requires a circuit depth of $26m + O(1)$.

3.3 Projective Representation

When points on an elliptic curve are represented as *affine coordinates* (x, y) , performing group operations on such points requires finding the multiplicative inverse of elements of $GF(2^m)$. This operation takes much longer to perform than the other field operations required, and it is desirable to minimize the number of division operations. For example, [19] gives a quantum circuit of depth $O(m^2)$ which uses the extended Euclidean algorithm.

By using *projective* coordinate representation, we can perform group operations without division. Instead of using two elements of $GF(2^m)$ to represent a point, we use three elements, (X, Y, Z) to represent the point $(\frac{X}{Z}, \frac{Y}{Z})$ in affine coordinates. Dividing X and Y by a certain quantity is now equivalent to multiplying the third coordinate (Z) by this quantity. Extensions to this concept have also been explored, where different information about an elliptic curve point is stored in several coordinates. Another advantage to projective coordinates is that the point at infinity \mathcal{O} can simply be represented by setting Z to zero. Unfortunately, one issue with projective coordinates for reversible computing is that there are more than one representation for any particular point.

To represent the point (x, y) , we use the equal superposition of all of these representations

$$|P(x, y)\rangle = \frac{1}{\sqrt{2^m}} \sum_{z \in GF(2^m)} |xz\rangle |yz\rangle |z\rangle.$$

We construct this state by starting with the state $1/\sqrt{2^m} \sum_z |z\rangle |z\rangle |z\rangle$, and multiplying the first and second registers by x and y , respectively.

Exact formulas for point addition in projective coordinates can be easily derived by taking the formulas for the affine coordinates under a common denominator and multiplying the Z coordinate by this denominator. These are detailed in [20]. Since the ECDLP can be solved by implementing elliptic curve point addition where one point is “classically known” [9], we may implement these formulas using the multiplication algorithm presented in Section 3.1 and by being careful to uncompute any temporary registers used. Since the number of multiplication operations used in these formulas is fixed, we may implement elliptic curve point addition with a known classical point with a linear depth circuit. This represents an improvement on the algorithm of [19], which makes use of an $O(m^2)$ -depth circuit for inversion of $GF(2^m)$ field elements.

Finally, to construct the state required for solving the ECDLP, we use the standard “double and add” technique, which requires implementing the point addition circuit for each value $2^i P$ and $2^i Q$, where $0 \leq i < m$. Performing $2m$ instances of a linear depth circuit, followed by a quantum Fourier transform gives a final depth complexity of $O(m^2)$ for the circuit which solves the ECDLP over $GF(2^m)$. This improves the previously known upper bound of $O(m^3)$ [9].

4 Conclusion

We considered the optimization of the quantum attack on the elliptic curve discrete logarithm problem, on which elliptic curve cryptography is based. Our constructions include a linear depth circuit for binary field multiplication and efficient data representation using projective coordinates. Our main result is the depth $O(m^2)$ circuit for computing the discrete logarithm over elliptic curves over $GF(2^m)$. Further research may be devoted toward a better optimization, study of architectural implications, and the fault tolerance issues.

References

1. M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
2. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing*, 26:1484–1509, 1997.
3. J. Von Zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.
4. R. Cleve and J. Watrous. Fast parallel circuits for the quantum Fourier transform. *IEEE Symposium on Foundations of Computer Science*, 41:526–536, 2000.

5. R. V. Meter and K. M. Itoh. Fast quantum modular exponentiation. *Physical Review A*, 71:052320, 2005.
6. Certicom. Certicom announces elliptic curve cryptography challenge winner. Certicom press release, 2004.
7. NSA Suite B Factsheet. http://www.nsa.gov/ia/industry/crypto_suite_b.cfm.
8. G. B. Agnew, R. C. Mullin, and S. A. Vanstone. An implementation of elliptic curve cryptosystems over $GF(2^{155})$. *IEEE Journal on Selected Areas in Communications*, 11(5):804–813, 1993.
9. J. Proos and C. Zalka. Shor’s discrete logarithm quantum algorithm for elliptic curves. *Quantum Information and Computation*, 3:317–344, 2003.
10. R. Jozsa. Quantum algorithms and the Fourier transform. *Proc. R. Soc. Lond. A*, 454:323–337, 1998.
11. S. Beauregard, G. Brassard, and J. M. Fernandez. Quantum arithmetic on Galois fields. [arXiv:quant-ph/0301163](https://arxiv.org/abs/quant-ph/0301163), 2003.
12. E. D. Mastrovito. VLSI designs for multiplication over finite fields $GF(2^m)$. *Proceedings of the Sixth Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes*, 6:297–309, 1988.
13. T. Toffoli. Reversible computing. Tech memo MIT/LCS/TM-151, MIT Lab for Computer Science, 1980.
14. D. K. Pradhan. A theory of Galois switching functions. *IEEE Transactions on Computers*, 27:239–248, 1978.
15. A. Reyhani-Masoleh and M. A. Hasan. Low complexity bit parallel architectures for polynomial basis multiplication over $GF(2^m)$. *IEEE Transactions on Computers*, 53:945–959, 2004.
16. E. D. Mastrovito. *VLSI Architectures for Computation in Galois Fields*. PhD Thesis, Linköping University, Linköping, Sweden, 1991.
17. A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.
18. D. Maslov. Linear depth stabilizer and quantum Fourier transformation circuits with no auxiliary qubits in finite neighbor quantum architectures. To appear in *Physical Review A*, [arXiv:quant-ph/0703211](https://arxiv.org/abs/quant-ph/0703211), 2007.
19. P. Kaye and C. Zalka. Optimized quantum implementation of elliptic curve arithmetic over binary fields. [arXiv:quant-ph/0407095](https://arxiv.org/abs/quant-ph/0407095), 2004.
20. D. Hankerson, J. López Hernandez, and A. Menezes. Software implementation of elliptic curve cryptography over binary fields. *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*, 2:1–24, 2000.