# Optimized Implementation of Quantum Binary Field Multiplication with Toffoli Depth One

**Kyungbae Jang**, Wonwoong Kim, Sejin Lim, Yeajun Kang,
Yu-Jin Yang, and **Hwajeong Seo**

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

# Contents

# Our Contribution

- **Quantum binary field multiplication using the Karatsuba algorithm**
  - **Karatsuba algorithm is one of the best choices for quantum implementations**
- **Efficient quantum circuit implementation techniques**
  - **76% performance improvement (TD × M) *TD: Toffoli depth, M: qubit count**

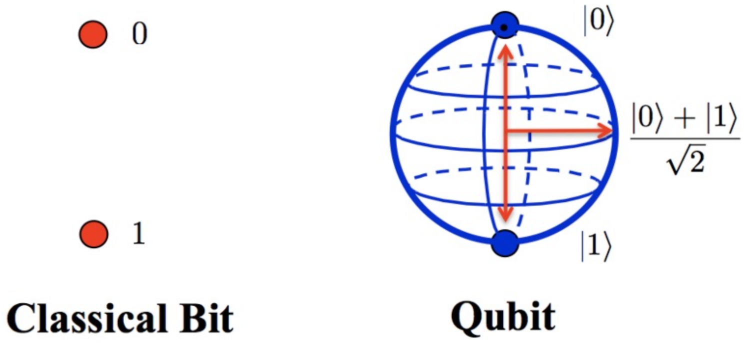
| Field size $2^n$ | Source | #CNOT | #1qCliff | $\#T$ | Toffoli depth | #Qubits | Full depth | $TD \cdot M$ |
|---|---|---|---|---|---|---|---|---|
| $n = 8$ | This work (Sec. 3.5) | 323 | 54 | 189 | 1 | 81 | 32 | 81 |
| | [7] | 405 | 30 | 448 | 28 | 24 | 216 | 672 |
| | [8] | 270 | 54 | 189 | 8 | 43 | 88 | 344 |
| | [6] | 382 | 54 | 189 | N/A | 24 | N/A | N/A |

$TD$ = Toffoli depth, $M$ = number of qubits.

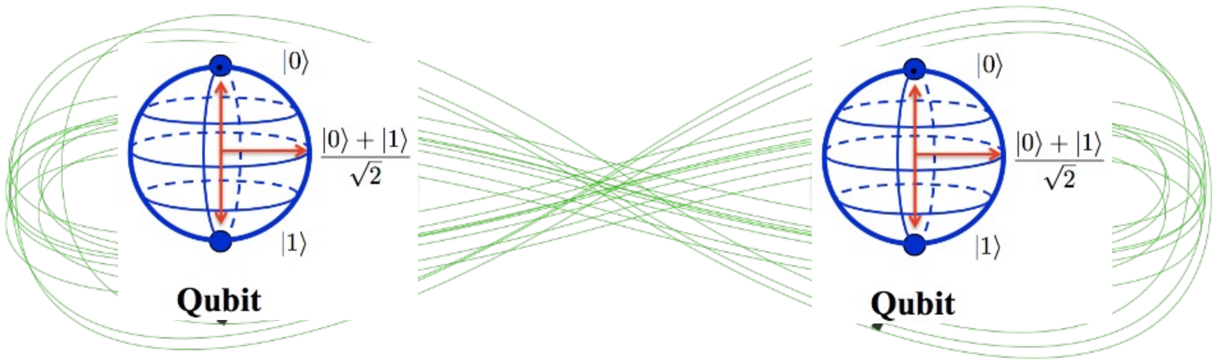
- **Optimized primitive for quantum cryptanalysis of ECC**

# Quantum Computing

- **Qubit (Quantum bit)**
  - **Superposition**

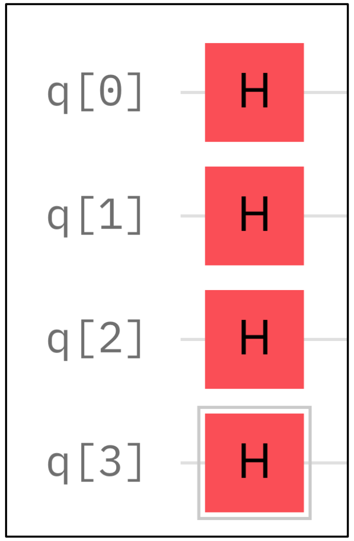


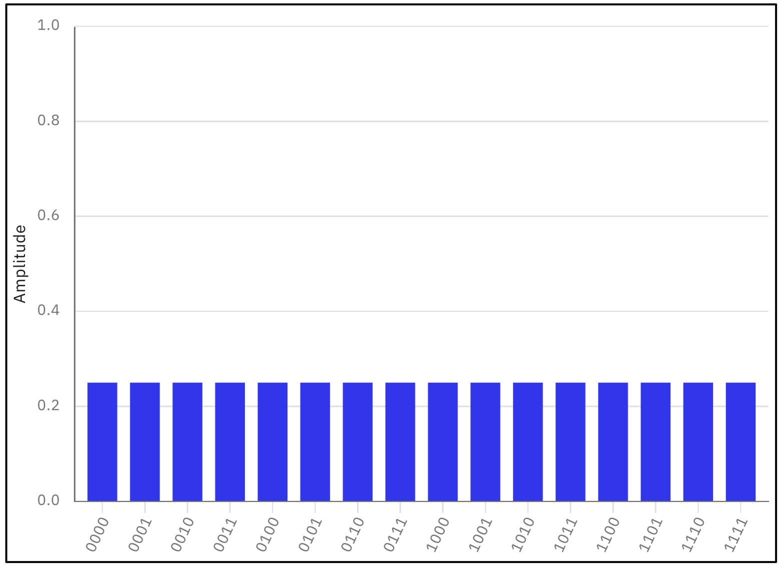

  - **Entanglement**



# Quantum Computer

- **$n$-qubit with superposition state?**



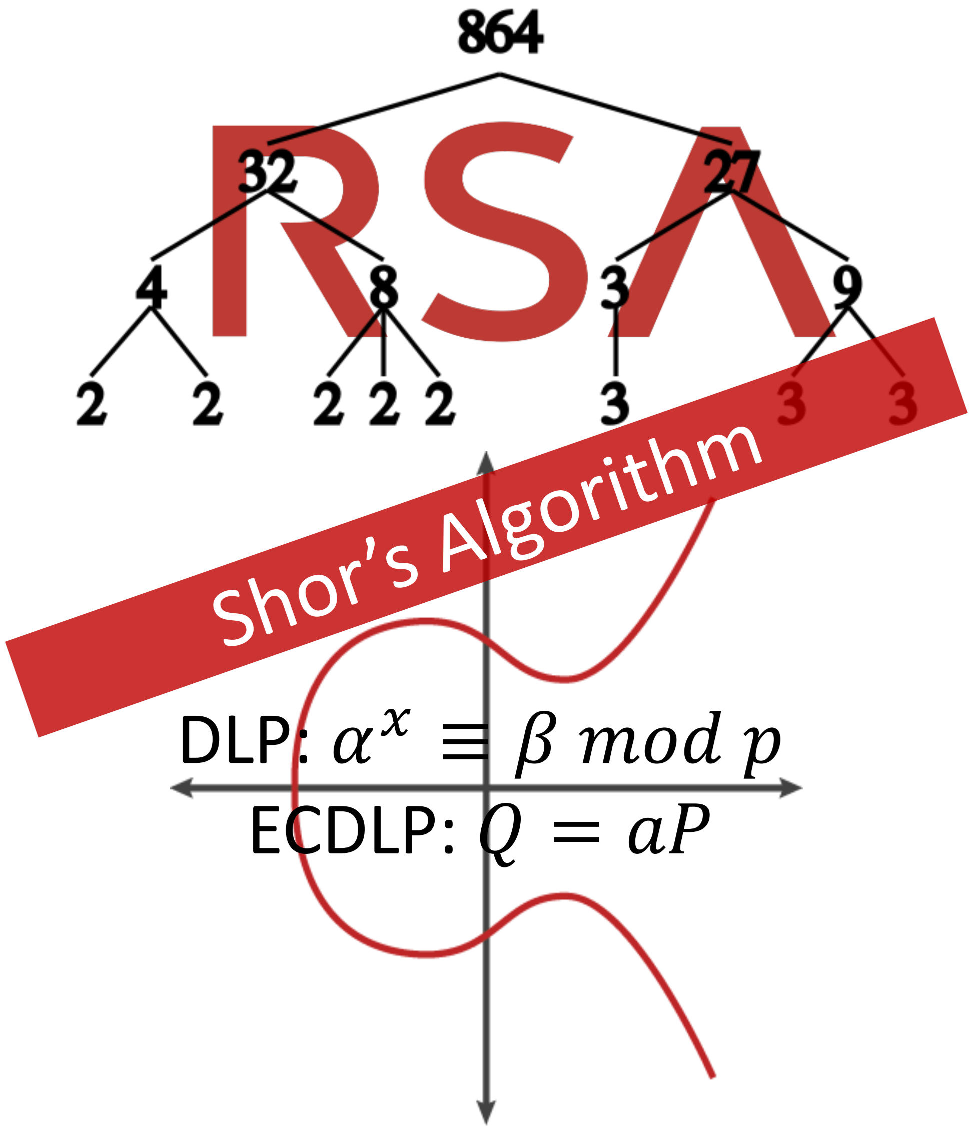




**We can prepare $2^n$ states (as probability) at once!**

**With proper quantum algorithm? (Shor, Grover, Simon etc…)**

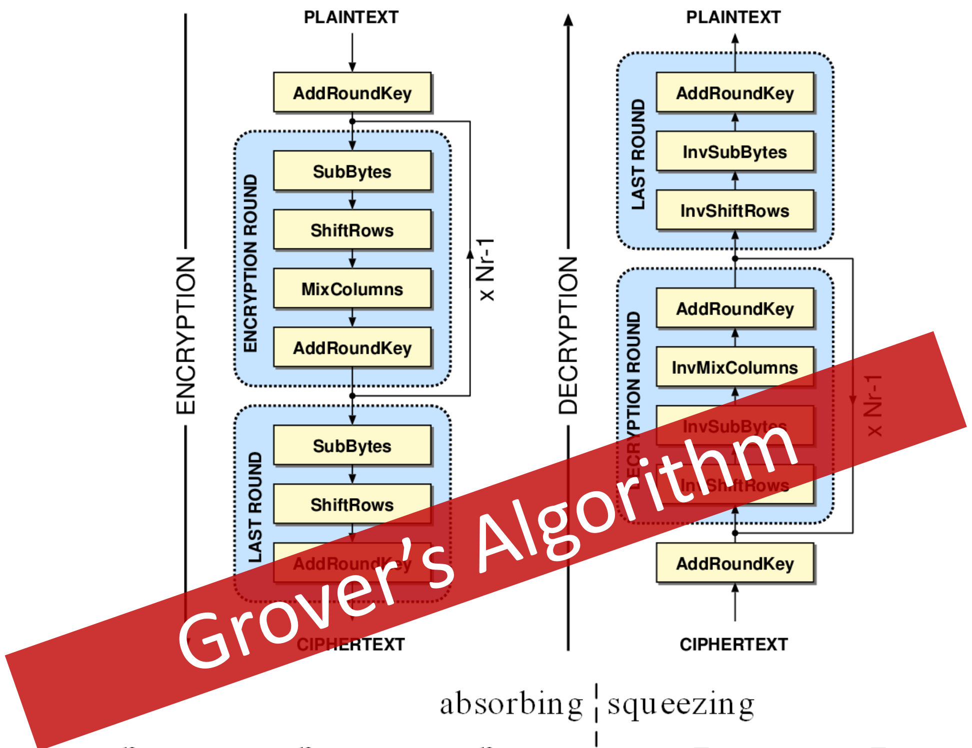
**→ Meaningful result can be achieved**

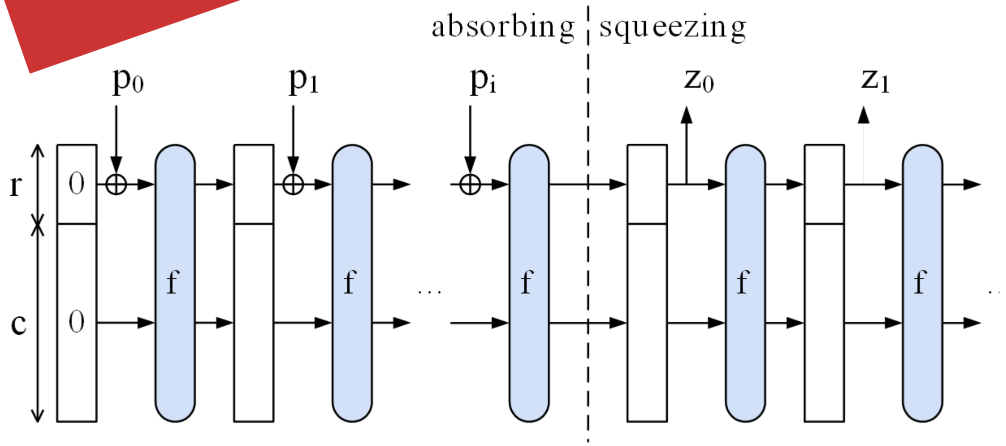
# Cryptosystems in Quantum World




DLP: $\alpha^x \equiv \beta \bmod p$

ECDLP: $Q = aP$



# Shor on RSA

- **Häner(2016): To apply Shor algorithm to RSA using $n$-bit key, $2n + 2$ qubits are required**
- **Gidney(2018): To apply Shor algorithm to RSA using $n$-bit key, $2n + 1$ qubits are required**

| | | Häner (2016) | Gideny (2018) |
|---|---|---|---|
| Qubits | RSA-3072 | 6,146 | 6,145 |
| | RSA-7680 | 15,362 | 15,361 |
| | RSA-15630 | 30,722 | 30,271 |

**< Comparison of resources (Shor on RSA factorization problem)>**


Thomas Häner, M. Rötteler, K. Svore", Factoring using 2n+2 qubits with Toffoli based modular multiplication, 2016

Craig Gidney, "Factoring with n + 2 clean qubits and n − 1 dirty qubits", 2018

# Shor on ECDLP (Elliptic Curve Discrete Logarithmic Problems)

- **Shor algorithm on ECDLP**
  - **NIST curves target**
  - **ASIACRYPT(2017)** : "Quantum resource estimates for computing elliptic curve discrete logarithms"
    - Estimate the quantum resources required to solve the DLP in the elliptic curve
      - **RSA is more vulnerable to quantum attacks than ECC**
  - **PQCrypto(2020)** : "Improved quantum circuits for elliptic curve discrete logarithms"
    - **They further reduced quantum resources** (qubits, depth) **than results of ASIACRYPT.**
  - **CHES (2020)** : "Concrete quantum cryptanalysis of binary elliptic curves"
    - **Shows that the Shor algorithm for binary ECC can be attacked with fewer resources.**

# Shor on ECDLP (Elliptic Curve Discrete Logarithmic Problems)

- **CHES 2020 paper results show the least resource-consuming quantum attack**
  - **They targeted Binary curves, Not Prime curves(ASIACRYPT, PQCrypto)**
  - **Since Binary arithmetic (Hardware-friendly ) is used, it is also optimized on quantum computers**
    - **Binary addition → XOR operation, Binary multiplication → AND operation, no carry**

| | Curve (Prime) | Asiacrypt | PQCrypto |
|---|---|---|---|
| Qubits | P256 | **2,338** | **2,124** |
| | P384 | **3,492** | **3,151** |
| | P521 | **4,727** | **4,258** |
| Depth | P256 | - | $1.38 \cdot 2^{32}$ |
| | P384 | - | $1.77 \cdot 2^{34}$ |
| | P521 | - | $1.09 \cdot 2^{36}$ |

| | Curve (Binary) | CHES (2020) |
|---|---|---|
| Qubits | B233 | **1,647** |
| | B283 | **1,998** |
| | B571 | **4,015** |
| Depth | B233 | $1.14 \cdot 2^{21}$ |
| | B283 | $1.67 \cdot 2^{21}$ |
| | B571 | $1.57 \cdot 2^{23}$ |

**<Quantum resources for applying Shor algorithm to ECDLP>**

# Shor on ECDLP (Elliptic Curve Discrete Logarithmic Problems)

- **What is the most important thig to present an optimized quantum attack?**
  - **Quantum Fourier Transformation (QFT)?, Quantum Phase Estimation (QFT)?**
    - **Essential, but default**

- **In our understanding,**
  - **Scalar multiplication…**

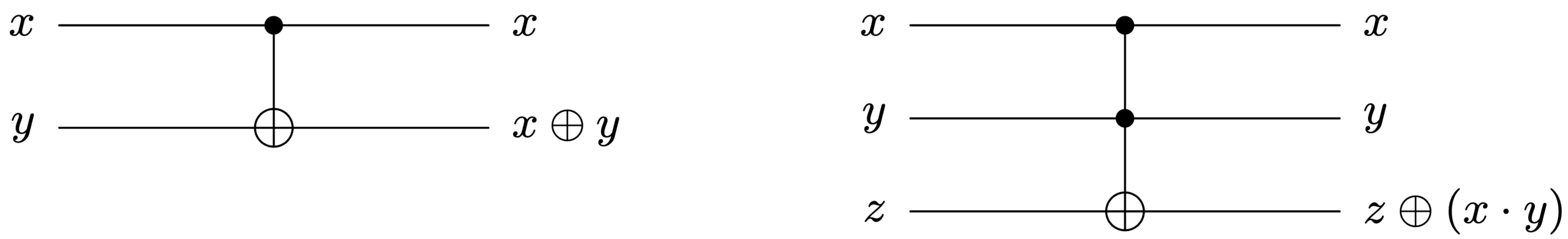
    → **Point addition…**

    → **Field arithmetic…**

$\mathbb{F}_p$, $\mathbb{F}_{2^n}$ **in Quantum!**

# Quantum Gates

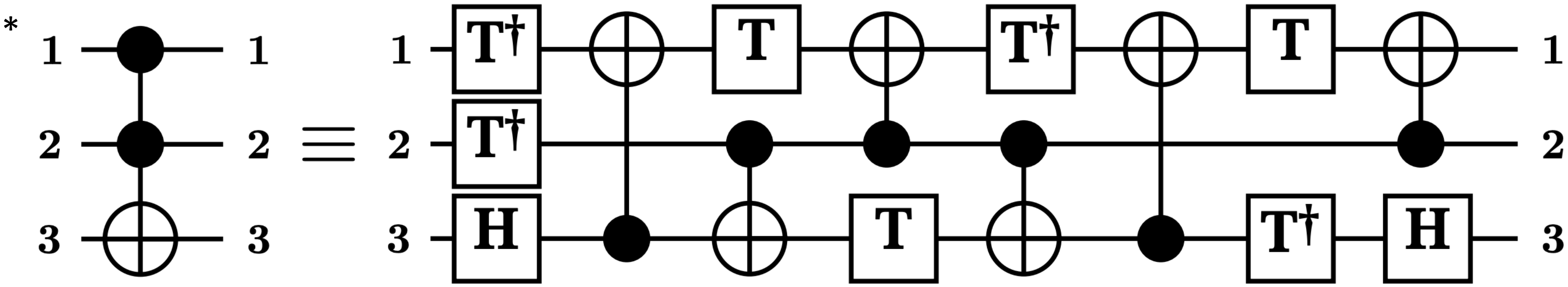
- **The CNOT gate** replaces **classical XOR operation**
- **The Toffoli gate** replaces **classical AND operation**




(a) CNOT gate (b) Toffoli gate

# Quantum Gates

- **Actually, the Toffoli gates are more complex than other quantum gates**




(a) Toffoli gate ($T$-depth 4, total depth 8).

- **This is why we should reduce the use of Toffoli gates (depth) !!**

* M. Amy, D. Maslov, M. Mosca, M. Roetteler, and M. Roetteler, "A meet- in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits,"

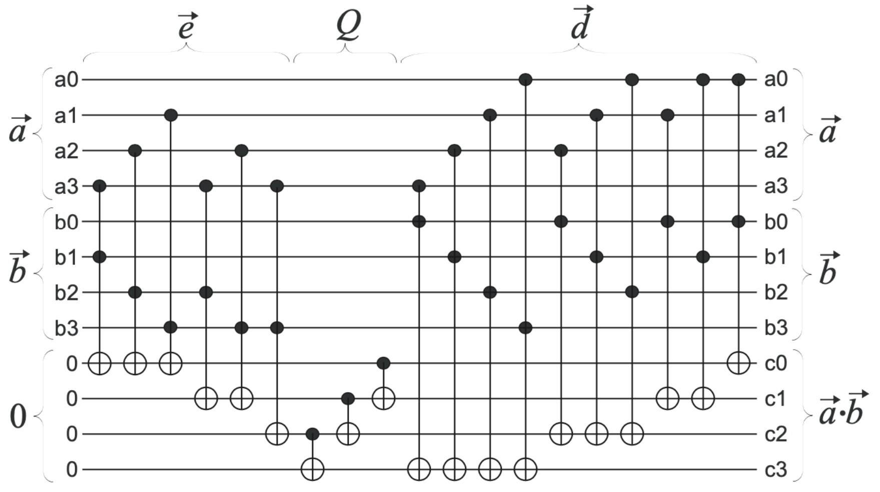
# Related Work: D. Maslov et al.

- **Generic Schoolbook Multiplication**
  - For $h = f \cdot g\ (size = n)$, **$3n$ qubits are required** → **Probably, this the minimum qubits**

- **They consider modular reduction in advance**
  - **Upper part multiplication operations are performed earlier**

- **$n^2$ Toffoli gates are used → Not optimized with Toffoli gate count → Maximum number**

*



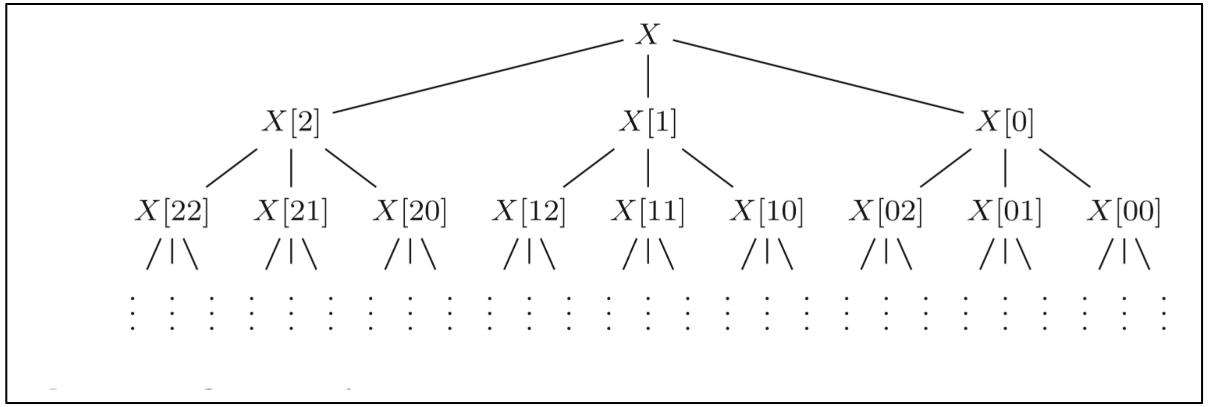

**< Quantum multiplication circuit>**

* D. Maslov et al. "On the design and optimization of a quantum polynomial time attack on elliptic curve cryptography"

# Related Work: S. Kepley et al.

- **They applied Karatsuba algorithm to quantum binary field multiplication**
- **For $h = f \cdot g\ (size = n)$, Karatsuba applied recursively**
- **Additional CNOT gates are required, but Toffoli gates can be reduced**
  - $n^2 \cdot \frac{3^{\log_2 n}}{4}$ **Toffoli gates are required**
- **More qubits are required : $2n$ + Number of Toffoli gates**

*




**< Recursive division in Karatsuba >**

* S. Kepley et al, "Quantum circuits for F2*n* -multiplication with subquadratic gate count"

# Related Work: I. van Hoof

- **They apply Karatsuba recursively → Toffoli gates are reduced**
  - **Same approach** with S. Kepley et al.'s work

- **Different is qubit count**
  - **By utilizing LUP decomposition**, only **$3n$ qubits are required**
  - They use more CNOT gates → However, **this is not a loss** **(reducing qubit is more important!)**

- In CHES 2020 paper (Shor on binary ECC), They adopted this quantum multiplication

- **But we should note this!**
  - **Reducing qubits → Circuit Space is reduced**
  - **Quantum gate operations in limited space causes high circuit depth**
    - Toffoli Depth and Full depth are higher than S. Kepley's quantum multiplication

**We should consider carefully the tradeoff between depth and qubit count.**

# Proposed Quantum Binary Multiplication

- **Previous works do not consider circuit depth**
- **Our quantum multiplication optimizes the Toffoli depth (i.e., one)**
  - **Full depth is also reduced (Full depth depends on Toffoli depth)**
- **We also apply Karatsuba recursively**
  - **Multiplication is divided → This alone is also effective**
  - **However, we remove the dependencies in the divided multiplications**
- **We provide rooms for removing dependencies.**
  - **When there is a dependency when dividing by Karatsuba?**
    - **We provide a room (ancilla qubits)**

**For any Field size $2^n$, we can implement quantum multiplication with Toffoli depth one**

# Proposed Quantum Binary Multiplication

- **Karatsuba algorithm**
  - **One of the efficient algorithms for multiplication**
  - **For multiplication** $h = f \cdot g \bmod N$
  - Split polynomials $f$ and $g$ into the size of $s = n/2$

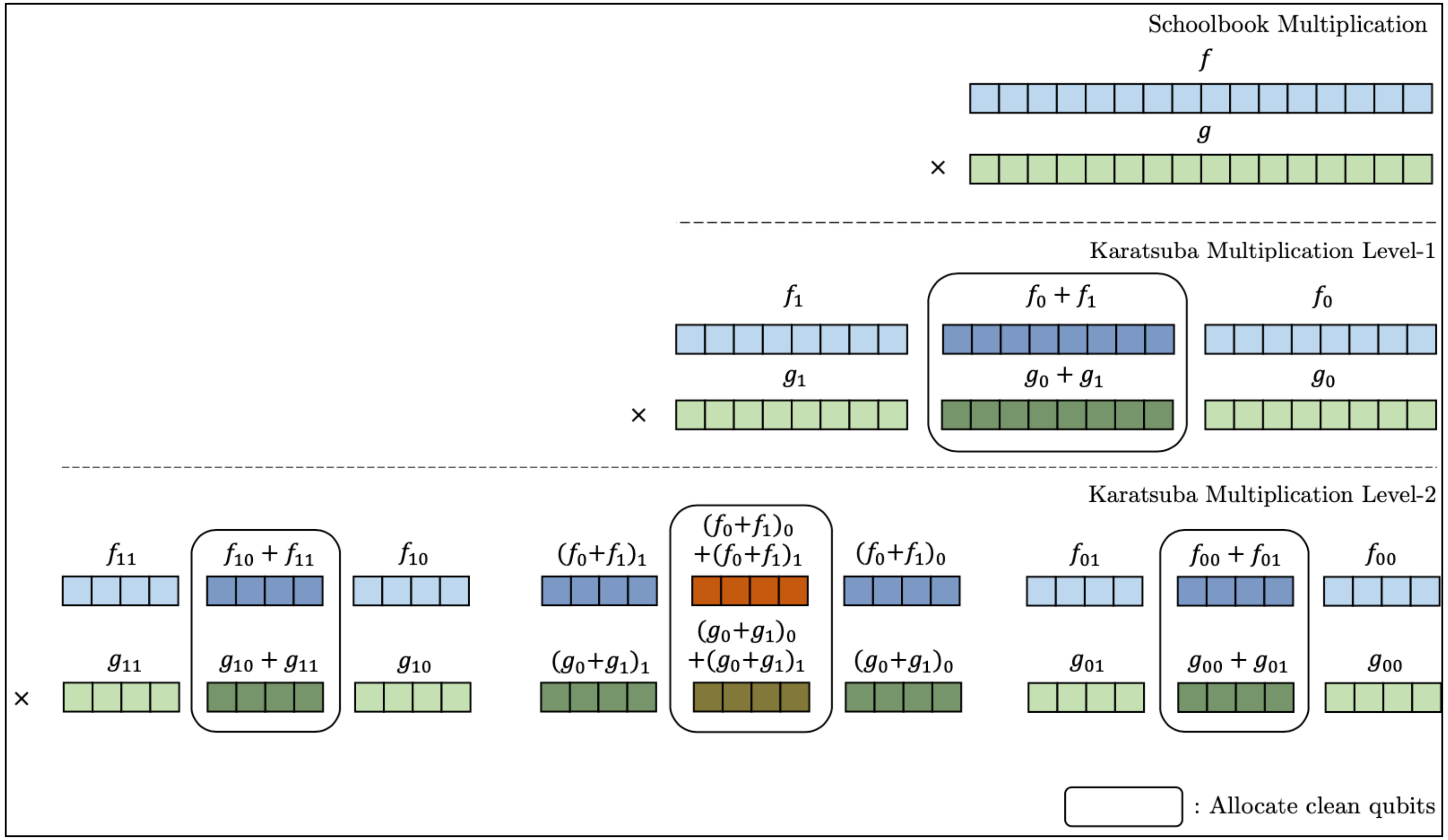
$$f = f_1 x^s + f_0$$
$$g = g_1 x^s + g_0$$

  - Then, Karatsuba multiplication is done,
    - Additions are required, but multiplication **complexity $O(n^2)$ is reduced to $O(n^{log_2 3})$**

$$f_0 \cdot g_0 + \{(f_0 + f_1) \cdot (g_0 + g_1) + f_0 \cdot g_0 + f_1 \cdot g_1\} x^s + f_1 \cdot g_1 x^{2s}$$

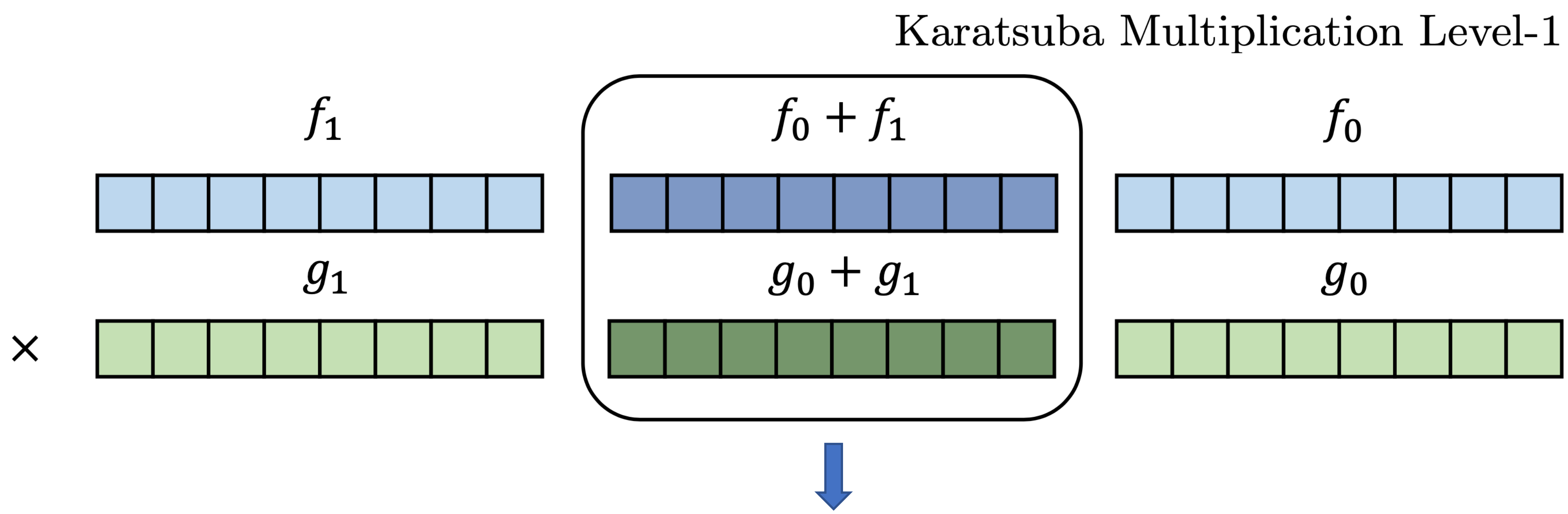
# Proposed Quantum Binary Multiplication

- **We apply Karatsuba recursively (in quantum), Level-1, Level-2, Level-3 …**
- **We provide rooms to remove dependencies between split multiplications (Rectangles)**



# Proposed Quantum Binary Multiplication

- In the room (ancilla qubits), we prepare $(f_0+f_1)$ and $(g_0+g_1)$
  - We copy $(f_0+f_1)$ and $(g_0+g_1)$ to ancilla qubits (clean state )with CNOT gates
  - Then, three multiplications become independent
    - Three multiplications can be preformed at once!

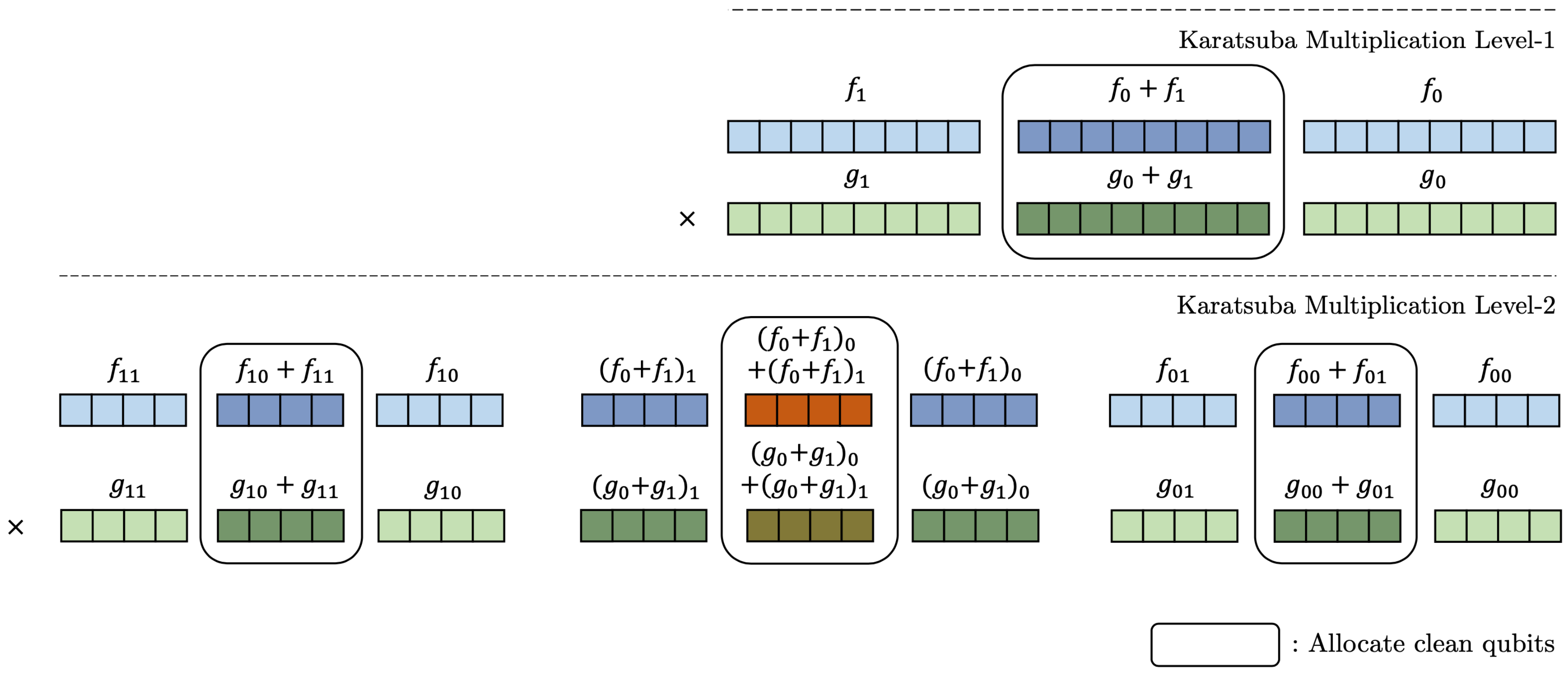



**Ancilla qubits and CNOT gates are required**

# Proposed Quantum Binary Multiplication

- **If we apply Karatsuba recursively and provide rooms for removing dependencies**
  - **Finally, at last Karatsuba level, all products $(1 \times 1)$ are generated at once!**

    **→ Toffoli depth is one, and full depth is also reduced**



# Proposed Quantum Binary Multiplication

- **Quantum resources are reduced according to the Karatsuba level (in our work)**
  - **Toffoli gates (depth) and Full depth are reduced**
  - **The number of qubits increases (because of rooms → ancilla qubits)**

Table 1: Quantum resources required for each Karatsuba level of multiplication.

| Field size $2^n$ | #CNOT | #Toffoli | Toffoli depth | #Qubits | Full depth |
|---|---|---|---|---|---|
| Schoolbook | $\cdot$ | $n^2$ | $3n-2$ | $4n-1$ | $8\cdot(3n-2)$ |
| Karatsuba Level-1 | $5n-4$ | $3\cdot(n/2)^2$ | $3n/2-2$ | $3\cdot(2n-1)$ | $8\cdot(3n/2-2)+5$ |
| Karatsuba Level-2 | $(5n-4)+$ $3\cdot(5n/2-4)$ | $3^2\cdot(n/2^2)^2$ | $3n/2^2-2$ | $3^2\cdot(n-1)$ | $8\cdot(3n/2^2-2)+10$ |
| Karatsuba Level-3 | $(5n-4)+3\cdot(5n/2-4)$ $+9\cdot(5n/4-4)$ | $3^3\cdot(n/2^3)^2$ | $3n/2^3.-2$ | $3^3\cdot(n/2-1)$ | $8\cdot(3n/2^3-2)+15$ |

# Proposed Quantum Binary Multiplication

- **High qubit count..**
  - **However, we overcome! (Let's talk about later)**
- **Optimized with Toffoli depth one, minimum Toffoli gates**
- **Low full depth**

Table 2: Quantum resources required for multiplication of Toffoli depth one.

| Field size $2^n$ | Karatsuba Level | #CNOT | #1qCliff | $\#T$ | $T$-depth※ | #Qubits | Full depth |
|---|---|---|---|---|---|---|---|
| $n = 4$ | 2 | 88 | 18 | 63 | 4 | 27 | 17 |
| $n = 8$ | 3 | 300 | 54 | 189 | 4 | 81 | 23 |
| $n = 16$ | 4 | 976 | 162 | 567 | 4 | 243 | 28 |

※: Toffoli depth one has a $T$-depth of four.

# Proposed Quantum Binary Multiplication

- **In our method, ancilla qubits that allocated each time the Karatsuba algorithm is applied, which is obviously an overhead.**

- **Recycling rooms (ancilla qubits)**
  - **After all products are generated at once in the last Karatsuba level, we initialize (cleaning) the rooms**
  - **Operations performed on rooms are reversed**
    - **From the lower layer to the upper layer**

**As a result, the ancilla qubits allocated for the rooms are initialized to zero!**

# Proposed Quantum Binary Multiplication

- **The cleaned ancilla qubits can be reused in the next operation**

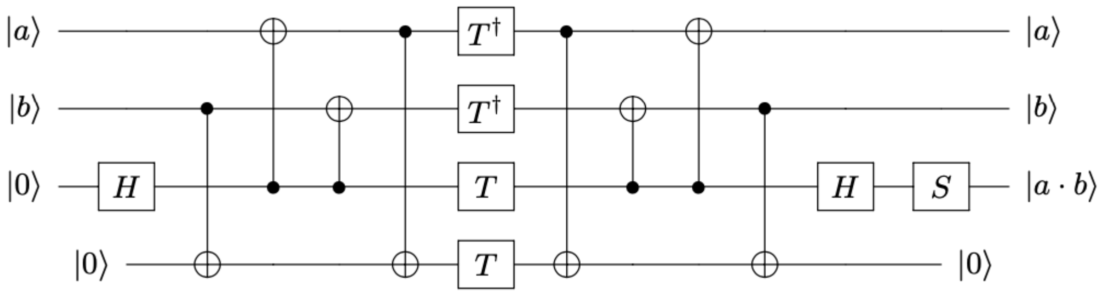
  **→ Strong advantage**
  - **i.e., not stand-alone multiplication**
  - **e.g., Itoh-Tsujii based inversion, scalar multiplication, point addition on ECC…**

| Field size $2^n$ | Karatsuba Level | #CNOT | #1qCliff | $\#T$ | $T$-depth※ | #Qubits | Full depth |
|---|---|---|---|---|---|---|---|
| $n = 4$ | 2 | 88 | 18 | 63 | 4 | 27 | 17 |
| $n = 8$ | 3 | 300 | 54 | 189 | 4 | 81 | 23 |
| $n = 16$ | 4 | 976 | 162 | 567 | 4 | 243 | 28 |

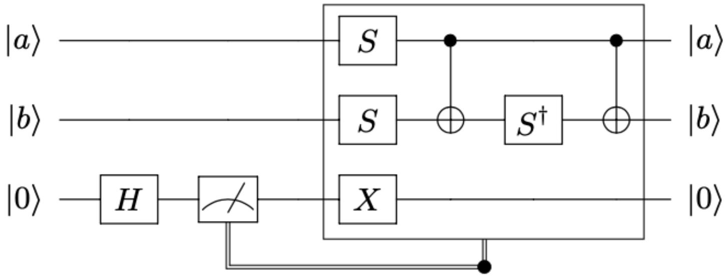
Can be reduced

17
43
113

# Proposed Quantum Binary Multiplication




(a) Quantum AND gate.




(b) Quantum AND$^\dagger$ gate.

Fig. 3: Quantum AND gate of $T$-depth one.

Table 4: Coefficients after performing modular reduction of $\mathbb{F}_{2^8}/(x^8 + x^4 + x^3 + x + 1)$.

| $x^n$ | Coefficient |
|---|---|
| $n = 0$ | $c_0 + c_8 + c_{12} + c_{13}$ |
| $n = 1$ | $c_1 + c_8 + c_9 + c_{12} + c_{14}$ |
| $n = 2$ | $c_2 + c_9 + c_{10} + c_{13}$ |
| $n = 3$ | $c_3 + c_8 + c_{10} + c_{11} + c_{12} + c_{12} + c_{13} + c_{14}$ |
| $n = 4$ | $c_4 + c_8 + c_9 + c_{11} + c_{14}$ |
| $n = 5$ | $c_5 + c_9 + c_{10} + c_{12}$ |
| $n = 6$ | $c_6 + c_{10} + c_{11} + c_{13}$ |
| $n = 7$ | $c_7 + c_{11} + c_{12} + c_{14}$ |

Table 3: Quantum resources required for multiplication of $T$-depth one using AND gate.

| Field size $2^n$ | Karatsuba Level | #CNOT | #1qCliff | $\#T$ | $T$-depth | #Qubits | Full depth |
|---|---|---|---|---|---|---|---|
| $n = 4$ | 2 | 106 | 27 | 36 | 1 | 36 | 16 |
| $n = 8$ | 3 | 354 | 81 | 108 | 1 | 108 | 22 |
| $n = 16$ | 4 | 1138 | 243 | 324 | 1 | 324 | 27 |

**Omitted from this presentation!**
**(detailed in the paper)**

# Performance

- **Our quantum multiplication is optimized with Toffoli depth one (depth is also low)**
  - **Our work achieves the best trade-off of $TD \cdot M$**
    - **TD is Toffoli depth, M is the number of qubits.**
    - **This metric represents the quantum circuit performance and is adopted in [1]**

Table 6: Comparison of quantum resources required for multiplication of $\mathbb{F}_{2^8}/(x^8+x^4+x^3+x+1)$.

| Field size $2^n$ | Source | #CNOT | #1qCliff | $\#T$ | Toffoli depth | #Qubits | Full depth | $TD \cdot M$ |
|---|---|---|---|---|---|---|---|---|
| $n=8$ | This work (Sec. 3.5) | 323 | 54 | 189 | 1 | 81 | 32 | 81 |
| | Schoolbook [7] | 405 | 30 | 448 | 28 | 24 | 216 | 672 |
| | Karatsuba1 [8] | 270 | 54 | 189 | 8 | 43 | 88 | 344 |
| | Karatusba2 [6] | 382 | 54 | 189 | N/A | 24 | N/A | N/A |

$TD$ = Toffoli depth, $M$ = number of qubits.

[1] J. Zou, Z. Wei, S. Sun, X. Liu, and W. Wu, "Quantum circuit implementations of AES with fewer qubits," in International Conference on the Theory and Application of Cryptology and Information Security,

# Conclusion & Future work

- **In this paper, we present an optimized quantum binary field multiplication**

- **Main contribution is optimized with Toffoli depth one for any field size.**
  - **Further…**
    - **Recycling technique that offsets the overhead of qubits**
    - **Optimization with T-depth one**
    - **Efficient implementation of modular reduction.**

- **Future work**
  - **Efficient quantum cryptanalysis (i.e., Shor) for ECC (binary)**
  - **In our understanding, quantum binary multiplication is paramount here**
    - **In CHES 2020 paper, Van hoof's work was used**

# Thank you!