Quantum binary quadratic form reduction

A $O(n \log n)$ depth circuit and application to lattice reduction

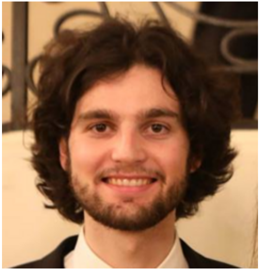
Nicolas David Thomas Espitau Akinori Hosoyamada

Inria, NTT

September 20, 2022

Human Context

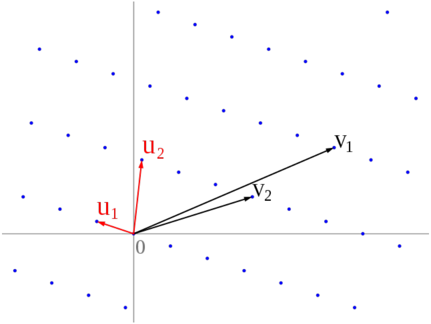
Nicolas David
PHD student at Inria Paris
Symmetric Cryptography and
Quantum Cryptanalysis



Thomas Espitau
Postdoc at NTT in Tokyo
Lattice Based Crytpography

Akinori Hosoyamada
Researcher at NTT in Tokyo
Symmetric Cryptography and
Quantum Cryptography

Lattice



- A lattice is a discrete subgroup of $\mathbf{R}^n$
- u_1, u_2 is a reduced basis

Scientific Context

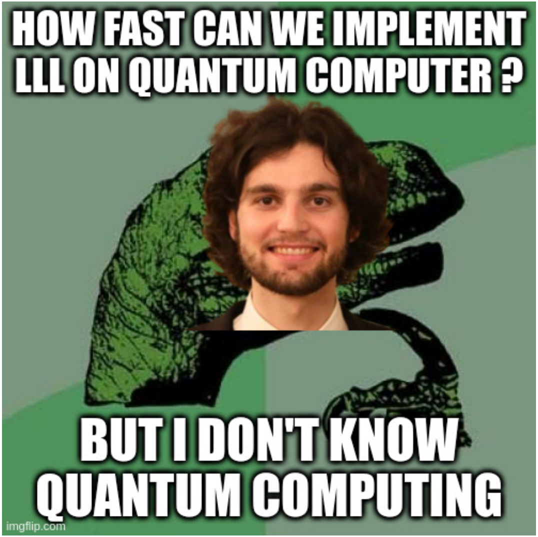
Lattice

- Lattice based cryptography is based on the difficulty of finding a reduced basis
- LLL is an algorithm that computes a reduced basis

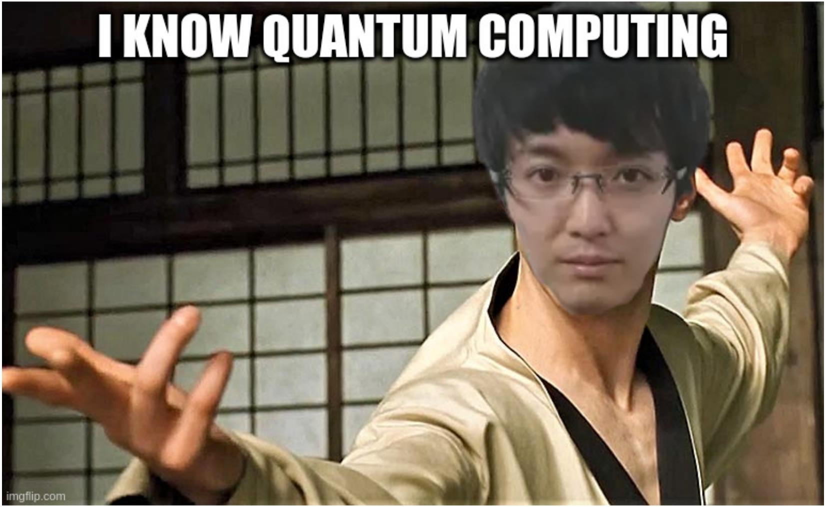
Quantum Cryptanalysis

- With the help of quantum computer it is possible to break some cryptographic primitives

How it all started



How it all started



Efficient reversible shallow circuits

Designing efficient shallow circuits is a new domain of research. It mainly consists in

- Designing efficient circuit for basic operations
- Give its precise complexity allowing to derive precise costs in applications

State of the art

Some previous work

- Addition
- Multiplication
- GCD

Today we will look into Binary quadratic form reduction

- first circuit designed for quadratic form reduction
- Application to LLL

[0]Yasuhiro Takahashi and Noboru Kunihiro. "A fast quantum circuit for addition with few qubits. Quantum Information Computation"
Srijit Dutta, Debjyoti Bhattacharjee, and Anupam Chattopadhyay. "Quantum circuits for toom-cook multiplication." Mehdi Saeedi and Igor L Markov. "Quantum Circuits for GCD Computation with O(nlogn) Depth and O(n) Ancillae."

Outline

1. **Preliminaries**
   - Quantum Circuits
   - Binary quadratic form
2. **Quantum Quadratic form reduction**
3. **Quantum multiplication by 2^x**

Outline

1. **Preliminaries**
   - Quantum Circuits
   - Binary quadratic form
2. **Quantum Quadratic form reduction**
3. **Quantum multiplication by 2^x**

Quantum circuit

Qubit

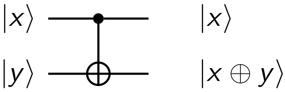
A qubit is the basic unit of quantum information

- pure states : $|0\rangle, |1\rangle$ (extended to $|00\rangle, |01\rangle, |11\rangle$ etc.)
- superposition : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbf{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

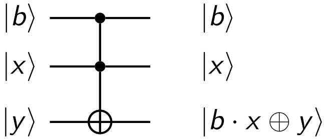
Some Quantum Gates

- NOT.

- Bitwise addition (CNOT).

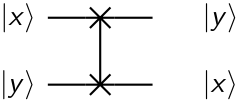


- Toffoli (CCNOT).

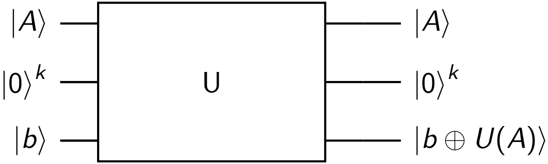


Some Quantum Gates

- Swap.

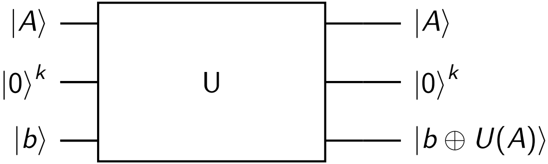


Quantum circuit and complexity measures



$|0\rangle^k$ are called Ancilae qubits

Quantum circuit and complexity measures



$|0\rangle^k$ are called Ancilae qubits

- Depth : Related to the speed of the execution.
- Width : Related to the memory ($\sharp$ Ancilae).
- Volume: Total number of operations.

Outline

1. **Preliminaries**
   - Quantum Circuits
   - Binary quadratic form
2. **Quantum Quadratic form reduction**
3. **Quantum multiplication by 2^x**

Binary quadratic form : Definition

Definition

An (integral) Binary quadratic form $\mathcal{Q} = [A, B, C]$ is a polynomial $(A\,X^2 + B\,XY + C\,Y^2) \in [X, Y]$. The integer $\Delta = B^2 - 4AC$ is called the *discriminant* of $\mathcal{Q}$. The form is said to be:

- **Degenerate** when $\Delta = 0$
- **Positive (resp. Negative) Definite** when $\Delta < 0$ and $\mathcal{Q}(x, y) \geq 0$ (resp. $\mathcal{Q}(x, y) \leq 0$) for any $(x, y) \in \mathbf{R}^2$.

Associated matrix : $Q = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$

Binary quadratic form : Class

Definition (Class)

Let $\mathcal{Q}$ be a Binary quadratic form, the following set define the class of $\mathcal{Q}$

$$< \mathcal{Q} >= \{S^T QS : S \in \mathrm{Sl}(2, \mathbf{Z})\}$$

Some notes:

- The determinant is invariant
- Every class contains a **reduced** binary quadratic form

Reduced Binary quadratic form

Definition (Reduced form)

A binary quadratic form $[A, B, C]$ is reduced if

$$\begin{Bmatrix} |B| \leq A \leq C \\ B \geq 0 \text{ if } |B| = A \text{ or } C \end{Bmatrix} \quad \text{when } [A, B, C] \text{ is positive definite}$$

Quadratic form: Link with lattices

	Lattice formalism	Quadratic form formalism
Object	Basis $M = (u, v)$	Gram matrix $G = M^t M$
Step operation	$M \leftarrow MS_\lambda$	$G \leftarrow S_\lambda^t G S_\lambda$
Reduceness condition	$\|\|v\|\|^2 \geq \|\|u\|\|^2 \geq 2\|\langle u, v\rangle\|$	$C \geq A \geq \|B\|$

Outline

1. Preliminaries
   - Quantum Circuits
   - Binary quadratic form
2. **Quantum Quadratic form reduction**
3. Quantum multiplication by 2^x

Gauss Reduction

Algorithm 1 Gauss reduction

Compute Δ
while Q is not reduced **do**
  if $|C| \leq \sqrt{|\Delta|}$ **then**
    $t \leftarrow -sgn(C) \cdot \left\lfloor \frac{B}{2|C|} \right\rceil$
  else
    $t \leftarrow -sgn(C) \cdot \left\lfloor \frac{\sqrt{|\Delta|}+B}{2|C|} \right\rceil$
  end if
  $S \leftarrow \begin{pmatrix} 0 & 1 \\ 1 & t \end{pmatrix}$
  $Q \leftarrow S^T\, Q\, S$
end while
return Q

From Multiplication to 2^x operations

Algorithm 2 Positive Definite Reduction

$m \leftarrow 0$,$\epsilon \leftarrow \mathrm{sgn}(B)$
if $C < A$ **then**
    $(C, A) \leftarrow (A, C)$
end if
if $\neg(|B| \leq 2A)$ **then**
    $m \leftarrow 2^{\lfloor \log_2 |B| \rfloor - \lfloor \log_2 A \rfloor - 1}$
else
    $m \leftarrow \left\lfloor \frac{|B|}{2A} \right\rceil$
end if
if $m = 0$ **then**
    return $[A, (-1)^{\delta(A=-B)} B, C]$
else
    Reduce$(C - \epsilon m B + m^2 A, B - \epsilon 2mA, A)$
end if

More global optimisations

Some more optimisations can be done:

- Iterative version : independance from the input
- Fewer conditions branches : reduce the quantum cost

We now focus on implementing the following subroutines:

- 2^x multiplication
- (Integer logarithm)

Outline

Aimed Circuit

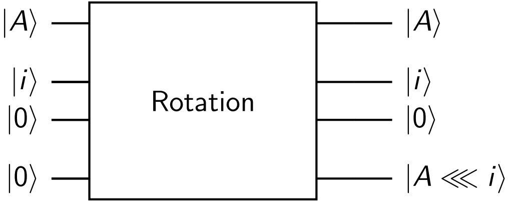


Figure: The quantum circuit for bit rotation.

Simplified circuit

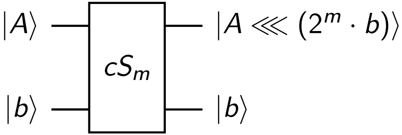


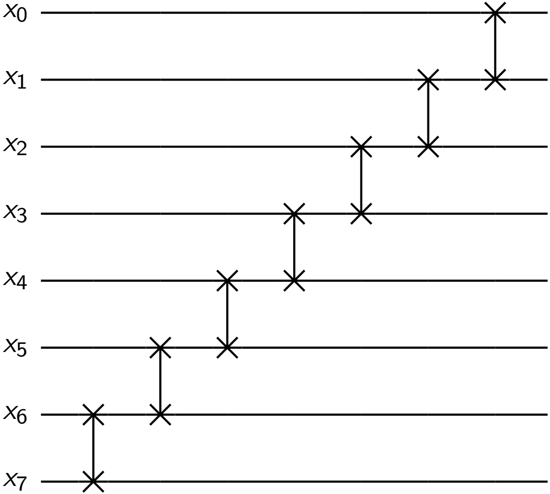
Figure: The quantum circuit cS_m ($A \in \{0,1\}^n$ and $b \in \{0,1\}$).

Even more simplified circuit

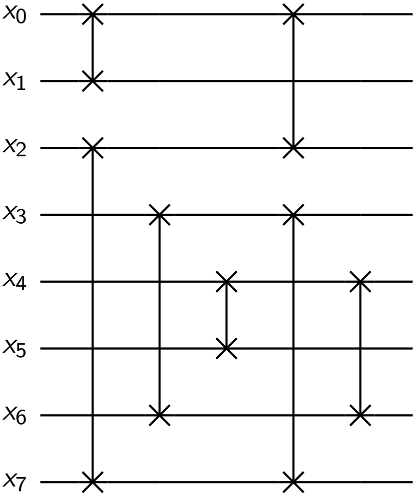
$$|A\rangle \; — \boxed{S_m} — \; |A \lll 2^m\rangle$$

Figure: The quantum circuit S_m ($A \in \{0,1\}^n$).

Example of 1-bit rotation



Example of Constant time 1-(qu)bit rotation



Constant time i-(qu)bit rotation

efficient i-(qu)bit rotation

The cyclic permutation on n qubits of parameter 2^i can be implemented :

- Depth : $\mathrm{O}(1)$
- Ancilae: none
- Volume : $\mathrm{O}(n)$

$$\sigma_0 = \left((1,0)\prod_{i=1}^{n/2-1}(i+1, n-i)\right)\cdot\left(\prod_{i=0}^{n/2-2}(i+1, n-i-1)\right)$$

From circuit to controlled circuit

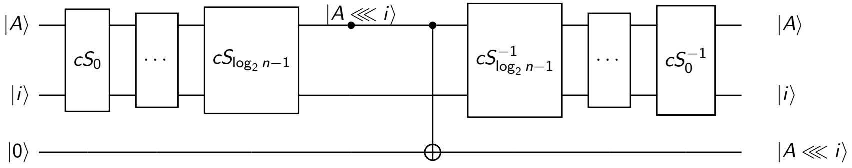
Controlled Version

Building a controlled version of S_j : cS_j can be done in with

- Depth : $\mathrm{O}(\log n)$
- Ancilae : $\mathrm{O}(n)$
- Volume : $\mathrm{O}(n)$

[0]Cristopher Moore and Martin Nilsson "Parallel quantum computation and quantum codes"

Overall circuit for multiplication by 2^x



- $i = \sum_i i_j 2^j$
- $A \lll i = A \lll i_0 2^0 \lll i_1 2^1 \lll \cdots \lll i_{\log_2(n-1)} 2^{log_2(n-1)}$
- The j-th bit of the decomposition of i in base 2 : i_j acts as the control bit of the circuit cS_j.

Complexity

Fine grain complexity analysis

The multiplication by a power of 2 can be inplemented on a circuit with:

- Depth : $12\lceil \log n \rceil$
- Ancilae: $n\lceil \log n \rceil$
- Volume : $12n\lceil \log n \rceil$

Results

Algorithm	Toffoli depth	♯ Ancilae	♯ Toffoli gates
Modular Addition	$O(\log n)$	$O\left(\frac{n}{\log n}\right)$	$O(n)$
Multiplication	$O\left(n^{1.143}\right)$	$O\left(n^{1.404}\right)$	$O\left(n^{1.55}\right)$
GCD	$O(n \log n)$	$O(n)$	$O\left(n^2\right)$
Bit rotation	$12 \log n$	$n \log n$	$12n \log n$
Logarithm	$4 \log n$	$4n$	$4n$
Binary quadratic form Reduction	$568n \log n + 896n$	$7n^2 + 26n$	$144n^2 \log n + 2834n^2$

Conclusion

We designed the first quantum circuit that

- generalizes GCD and is very important for number theory
- performs the core step of LLL Algorithm

We also derived a fine grain complexity analysis allowing a fine estimation for applications.
Article on eprint : https://eprint.iacr.org/2022/466.pdf

Conclusion

Thank you for your attention