量子計算機の到来を正しく恐れたい

國廣　昇
（東京大学）

NICT サイバーセキュリティシンポジウム2019
2019年2月7日

自己紹介

國廣昇（くにひろ　のぼる）

所属：東京大学大学院
　　情報理工学系研究科コンピュータ科学専攻

主な研究テーマ：

公開鍵暗号の安全性評価

- 楕円曲線暗号の安全性評価
- 量子計算機を用いた公開鍵暗号の安全性評価
- 秘密鍵が小さいRSA暗号の安全性評価（格子理論）
- RSA暗号の秘密鍵が確率的に漏洩した時の安全性評価

暗号技術はセキュリティの基盤

安全・安心な情報社会実現のためには，
暗号技術の安全性評価は必須

暗号の安全性は，いくつかの方法により確認される

- 安全性の根拠となる仮定が本当に正しいか？
- 仮定の下で安全性が適切に証明されているか？
- 適切に実装されているか？
- サイドチャネル攻撃に対する耐性はあるか？

現在利用されている暗号方式の多くは，

- 素因数分解
- 楕円離散対数問題

が困難であるという仮定の下で安全性が確認されている．

素因数分解はそもそも難しいのか？

現状把握

(1) 理論的に知られていること

- 多項式時間アルゴリズムは知られていない
- 知られている最善のアルゴリズムは，準指数関数時間

$$\exp\left(\left(\sqrt[3]{64/9}+o(1)\right)(\ln n)^{1/3}(\ln\ln n)^{2/3}\right)$$

(2) 実験で確認されていること

- 2009年12月 : 768ビット (232桁)の素因数分解
- 数体ふるい法を使用
- ふるいフェーズ : 1500年 AMD Opteron processor (2.2 GHz with 2 GB RAM)

未来を予測

(3) 計算機能力の向上

- ムーアの法則:
  集積回路上のトランジスタ数は「18か月ごとに2倍になる」
- スーパーコンピュータの性能向上

暗号の将来の脆弱性をできるだけ正確に予測するには. . .
(1) 理論的にどこまでわかっているか？
(2) 現在の技術で, 実際にどこまで破られるか？
(3) 計算機能力向上の将来動向
を調査することにより行う.

CRYPTREC暗号技術評価委員会では，

1. 理論的な最新成果をもとに，
2. 現在の立ち位置を把握し，
3. 将来の計算能力を推定する，

ことにより，1024, 2048ビットの素因数分解の困難性を評価

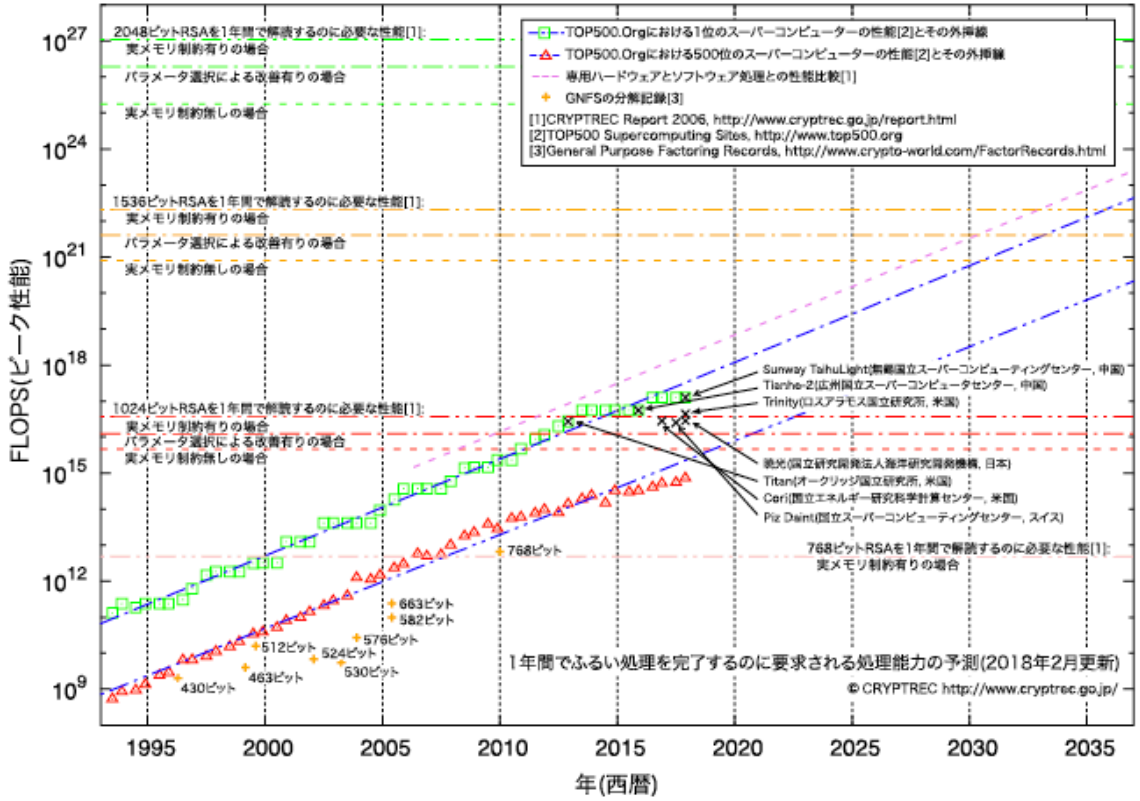


図 3-2: 素因数分解の困難性に関する計算量評価

(1 年間でふるい処理を完了するのに要求される処理能力の予測、2018 年 2 月更新)

CRYPTREC Report2017
https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2017.pdf
34ページより

この講演で話したいこと

量子計算機を用いた場合は？
（古典計算機では，根拠を積み重ねて評価している）

「安全」，「危険」の極論ではなく，
- できるだけ正確に危険性を理解したい．
- もしくは，理解に向けて少しでも前進したい．

量子計算機の場合でも．．．
(1) 理論的にどこまでわかっているか？
(2) 現在の技術で，実際にどこまで破られるか？
(3) 計算機能力向上の将来動向
を知りたい．

量子アルゴリズム

1985年: Deutschが，量子Turing Machineを提案
1994年: Simonのアルゴリズム（周期関数の位数発見）
1994年: Shorの素因数分解アルゴリズム，
　　離散対数問題の解法アルゴリズムの提案
　　（可換隠れ部分群問題への拡張）
1996年： Groverのアルゴリズム（探索問題）

参考：これ以外のアルゴリズム
Quantum Algorithm Zoo
https://math.nist.gov/quantum/zoo/

量子計算機と暗号を取り巻く環境の変化

1.ポスト量子暗号の募集

2015年8月：NSAが，ポスト量子暗号への移行を表明
2016年2月：NISTが，ポスト量子暗号の標準化計画を公表
量子計算機の実現に備えて，素因数分解，離散対数問題の困難さに依存しない暗号の募集

69件が応募
~~2019年1月10日に，Round 2 algorithmsを公表予定（ただし，1月28日現在で公表されていない）~~
2019年1月30日，Round 2 algorithmsを公表
2022～2024年までに標準化

2. Noisy Intermediate-scale Quantum (NISQ)の開発

小さいながらも，実際の量子計算機が出来てきた

Noisy Intermediate-scale Quantum (NISQ) system

- Google 72量子ビット
- IBM 50量子ビット
- Intel 49量子ビット

ただし，ノイズは大きい

このまま，大規模化が進むのか？

(3) 将来の量子計算機の動向を予測する

Quantum Computing: Progress and Prospects (2018)*

- 大規模でノイズの小さい（誤り訂正機能付き）量子計算機がいつ出来るかの予測をするには早すぎる
  (it is still too early to be able to predict the time horizon for a scalable quantum computer.)
- NISQの開発を当分を目指す．まずは，できるものを作る．
- 商業的に成功すれば，もっと大きい物を目指す

*National Academies of Sciences, Engineering, and Medicine発行

(1) 量子計算機による素因数分解に関する事実

1. 素因数分解，離散対数問題を多項式時間で解くことができる
2. 実際の回路構成や精密なリソース（量子ビット数，ゲートの個数）はよく理解されている．
   - 素因数分解 (K05, TK08, HRS16)
   - 楕円離散対数問題 (RNSL17)

nビットの素因数分解を行うのに．．．

- 標準的な回路構成では，
  $3n+2$ 量子ビット，$O(n^3)$個の基本ゲート
- 量子ビットを削減した回路では，
  $2n+2$量子ビット，$O(n^4)$個の基本ゲート

（理想的な環境下：誤りは全く無い，各量子ビットは完全結合）

Shorの素因数分解アルゴリズムの概略

戦略: 合成数N, 自然数aに対して, $a^r = 1 (\mathrm{mod}\ N)$
となる最小の自然数 r (位数)を求める,

Step1: 初期状態 |0＞|1＞を構成

Step2: Hadamard変換を適用

$$\rightarrow \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle |1\rangle$$

Step3: べき乗剰余演算を適用

$$\rightarrow \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle |a^j \bmod N\rangle$$

Step:4 逆QFTを適用

$$\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\frac{\tilde{s}}{r}\right\rangle |u_s\rangle$$

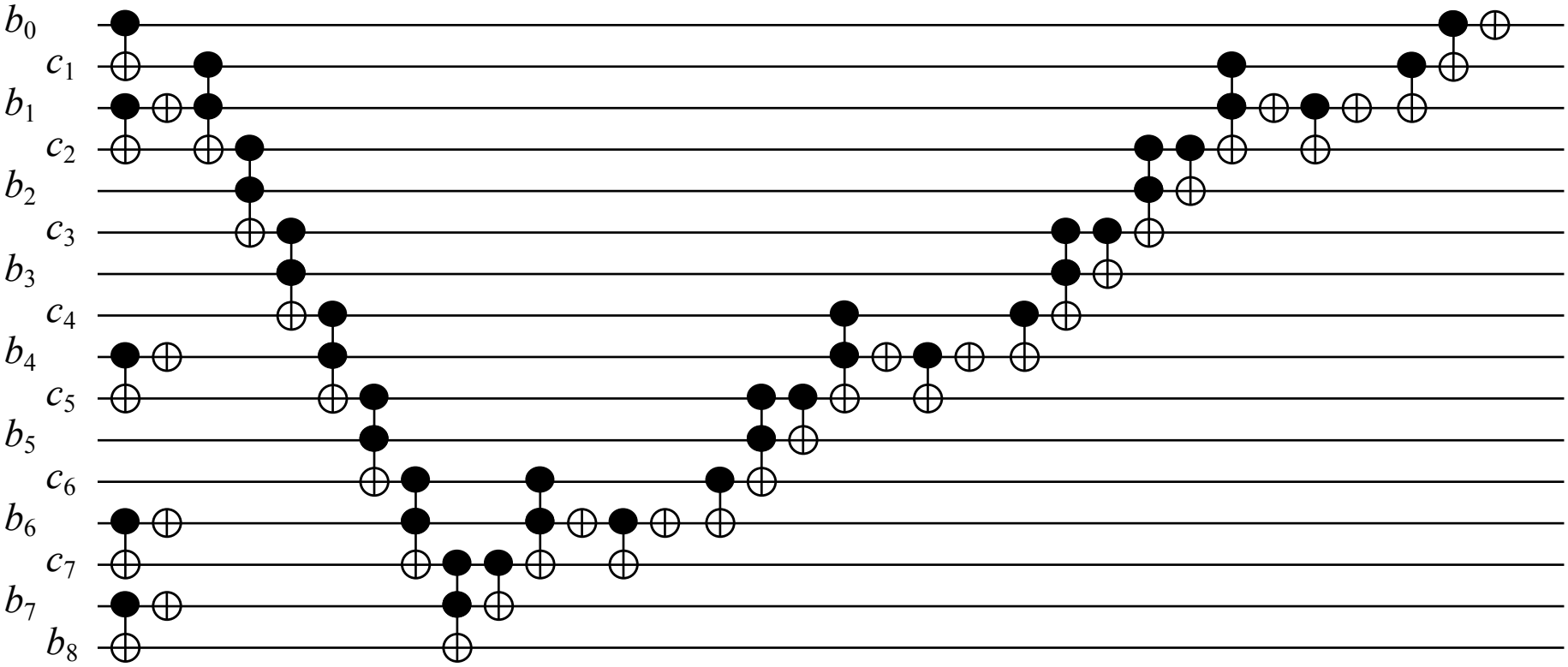
Step5: 第1レジスタを観測:

$$\rightarrow \frac{\tilde{s}}{r}$$

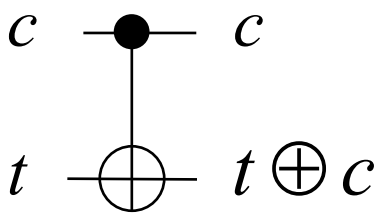
Step6: 連分数展開を行い r を求める.

回路の(一部分の)例:

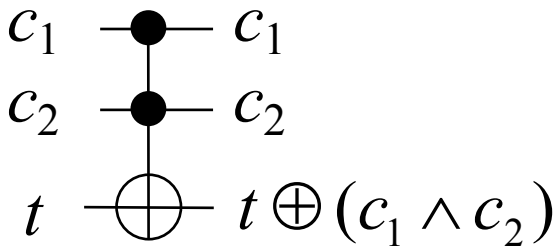
$(11010011)_2$=211の加算



C-NOT gate



Toffoli gate



素因数分解をするのに必要な量子ビット数，ゲート数*

	768ビット合成数		2048ビット合成数	
	# of qubits	# of gates	# of qubits	# of gates
標準的な構成	2306	1.22×10^{11}	6146	3.04×10^{12}
量子ビット削減回路	1539	--	4099	1.35×10^{15}
上記の近似版	1539	8.68×10^{11}	4099	1.22×10^{13}

* N. Kunihiro, “Exact Analysis of Computational Time for Factoring in Quantum Computers,” IEICE Trans. Vol. 88-A, No.1 2005.

(2) Shorのアルゴリズムに基づく素因数分解実験

[1] Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, 2001.

[2] Shor's Quantum Factoring Algorithm on a Photonic Chip, Science, 2009.

[3] Computing prime factors with a Josephson phase qubit quantum processor, Nature Physics, 2012.

[4] Realization of a scalable Shor algorithm, Science, 2016.

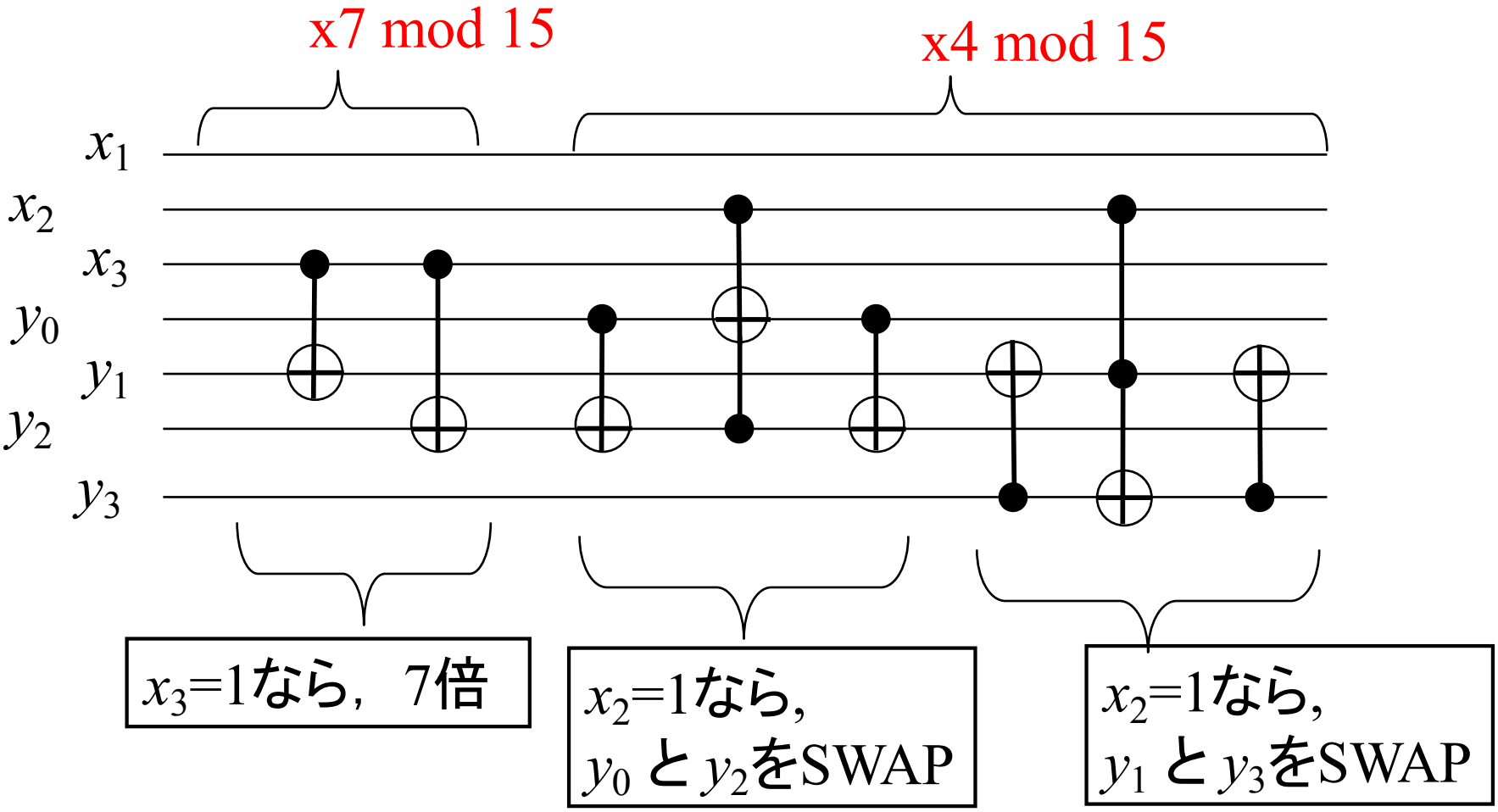
[5] Experimental realisation of Shor's quantum factoring algorithm using qubit recycling, Nature Photonics, 2012.

Device	研究機関	Year	合成数	Journal
NMR	IBM	2001	15	Nature
Photonic chip	U. of Bristol	2009	15	Science
Superconductivity	UCSB	2012	15	Nature Physics
Ion Trap	U. Innsbruck	2016	15	Science
Photon	U. of Bristol	2012	21	Nature Photonics

- 標準的な回路構成では，10〜14 qubit必要.
- いずれも，かなり少ないqubit数で実験を行っている.
- 汎用的ではない回路構成になっている.

[1]で用いられた回路（IBM, NMR）

$$\frac{1}{\sqrt{2^3}}\sum_{x=0}^{7}|x\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2^3}}\sum_{x=0}^{7}|x\rangle|7^x \bmod 15\rangle$$



この回路は，N=15 であることを利用

1 → x_3==1のとき，1に6を足す
→ x_2==1のとき，$4y$ mod 15を実行

$y=(y_3 y_2 y_1 y_0)_2$とすると，

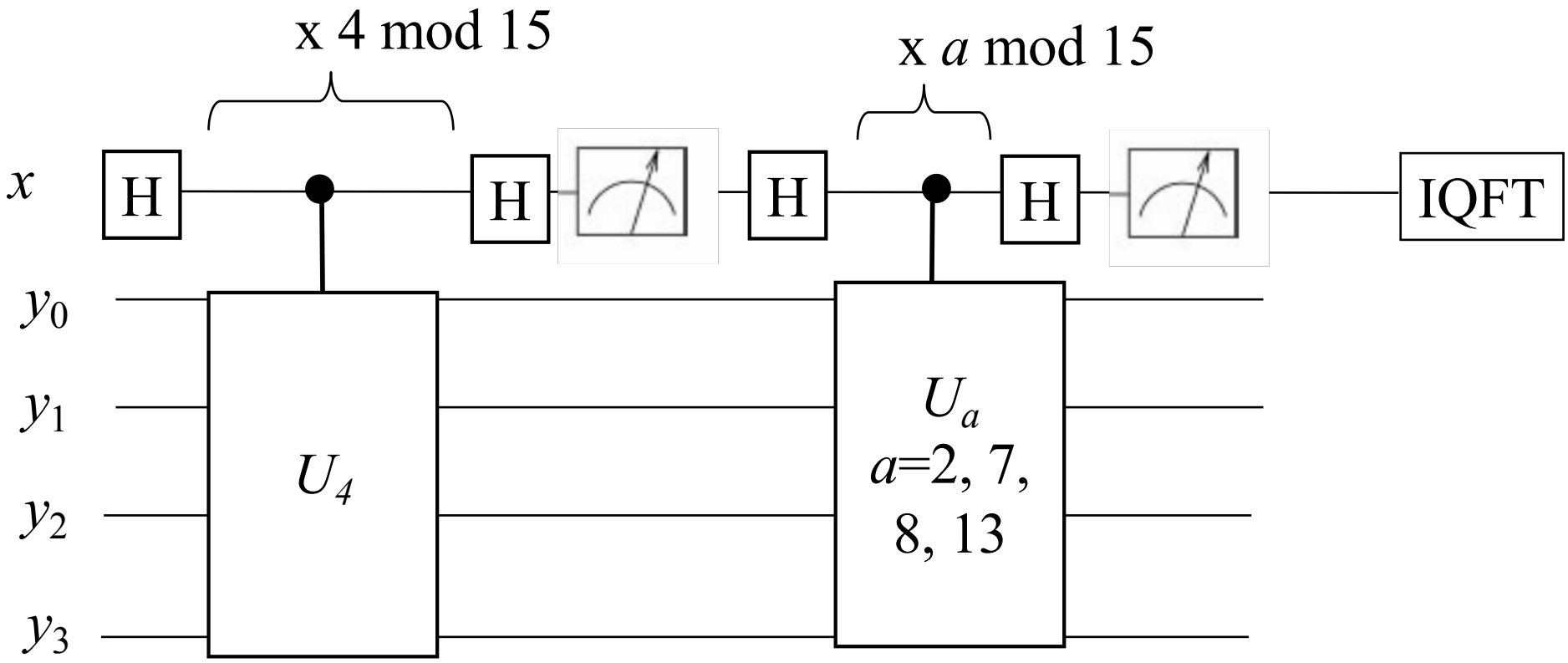
$4y=(y_3 y_2 y_1 y_0 00)_2=16\times(y_3 y_2)_2+(y_1 y_0 00)_2$

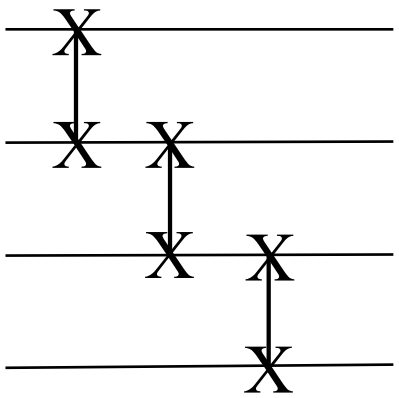
$4y \bmod 15=(y_3 y_2)_2+(y_1 y_0 00)_2=(y_1 y_0 y_3 y_2)_2$

2個のSWAPで実行可能

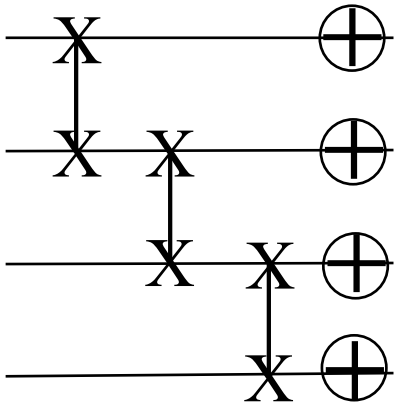
[4]で用いられた回路 (Innsbruck, Ion Trap)

a=2, 7, 8, 13を使用

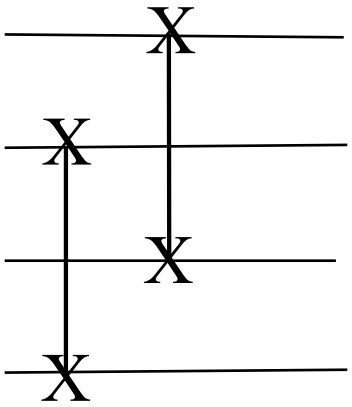




U_2

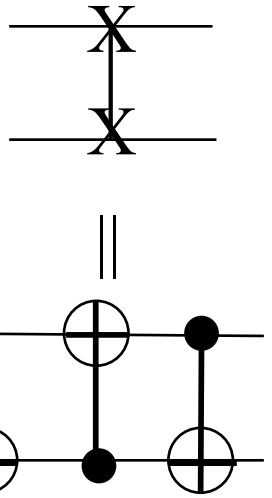


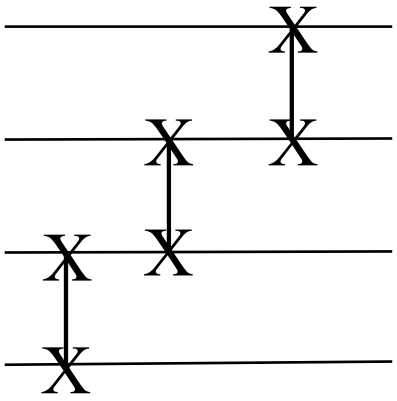
U_{13}



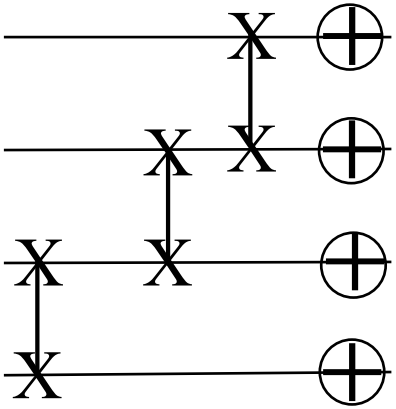
U_4

SWAP

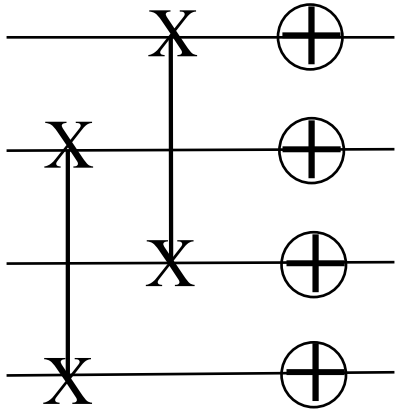




U_8

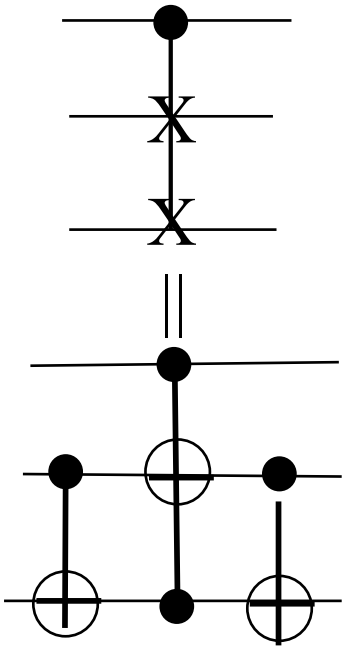


U_7

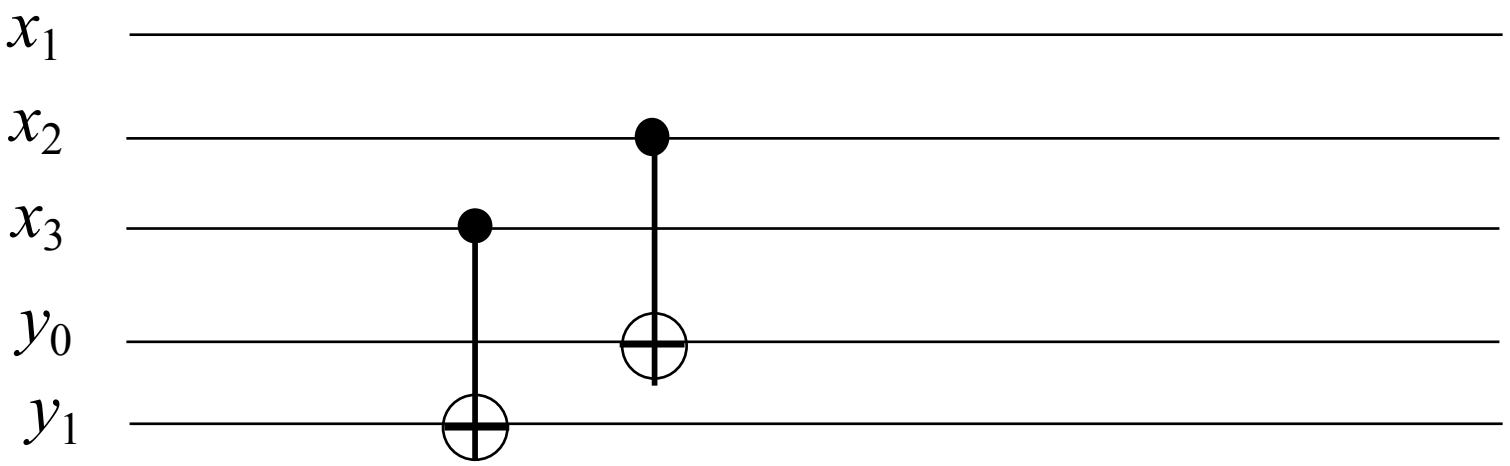


U_{11}

C-SWAP



[2]で用いられた回路 (U. of Bristol, Photonic chip)



a=7を使用

$7^0=1$, $7^1=7$, $7^2=4$, $7^3=13$, $7^4=1$であることを使用

Trick: 以下のencodeを使用

$1\rightarrow (00)_2$, $7\rightarrow (01)_2$, $4\rightarrow (10)_2$, $13\rightarrow (11)_2$.

U_7: $(00)_2\rightarrow (01)_2$, U_4: $(0x)_2\rightarrow (1x)_2$

この回路は，位数が4であるという事実を使いすぎている.
Shorのアルゴリズムの目的は位数を求めること.

[2][5]の回路の一般化

Shorのアルゴリズムのもともとの形

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|a^x \bmod N\rangle$$

“simplified” or “compiled”版のShorのアルゴリズム

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|x \bmod r\rangle$$

*r*は，そもそも計算したかったもの．
Shorのアルゴリズム（の簡略版）としては不適当
[5]では，21の素因数分解を行っているが，不適当．

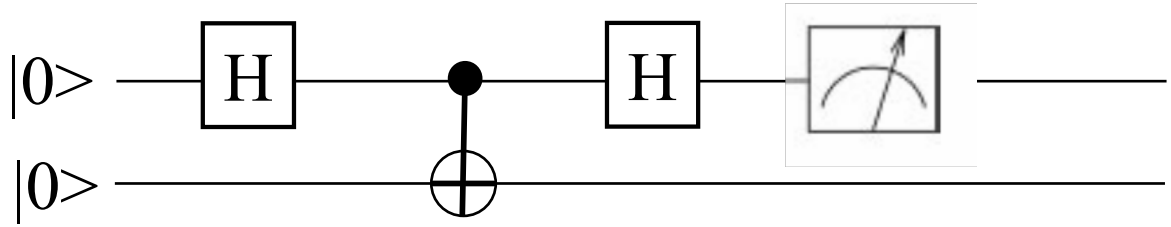
Oversimplifying Quantum Factoring*

aを位数2の元とする $(a^2 \bmod N = 1)$

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|a^x \bmod N\rangle$$

“oversimplified”版Shorのアルゴリズム

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|x \bmod 2\rangle$$



- 論文中では，20,000-bit！の素因数分解を示している
- ビットサイズだけを追求しても意味はないことを主張

* A Smolin, John & Smith, Graeme & Vargo, Alexander. (2013). Oversimplifying quantum factoring. Nature. 499. 163-165.

*N, a*の具体的な計算法

SageMathによる実装

```
k=4096
p=random_prime(2^k-1, false, 2^(k-1))
q=random_prime(2^k-1, false, 2^(k-1))
N=p*q
a= crt(1, -1, p, q)
```

計算時間:
2048-bit RSAの場合:一瞬
4096-bit RSAの場合:1秒程度
8192-bit RSAの場合:10秒程度

量子計算機を用いた素因数分解実験の現状把握

- 素因数分解された合成数で最大のものは15
- ただし，「15」であることを利用している．

我々が貢献できそうなこと

- できるだけ合成数の特徴を用いない回路構成を行い，
- 実際の量子計算機（NISQなど）で実験をしてみる
  - 理想的な環境ではないので，様々な最適化が必要
  - 何を指針に回路を構成するのかも検討が必要

Quantum Computing: Progress and Prospectsの主張の抜粋（関連部分のみ）

Key Finding 1:
Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm based public key cryptosystems will be built within the next decade.

Key Finding 10:
Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough - and the time frame for transitioning to a new security protocol is sufficiently long and uncertain - that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster.

Key Finding 3:
Research and development into practical commercial applications of noisy intermediate scale quantum (NISQ) computers is an issue of immediate urgency for the field. The results of this work will have a profound impact on the rate of development of large-scale quantum computers and on the size and robustness of a commercial market for quantum computers.

Key Finding 4:
Given the information available to the committee, it is still too early to be able to predict the time horizon for a scalable quantum computer. Instead, progress can be tracked in the near term by monitoring the scaling rate of physical qubits at constant average gate error rate, as evaluated using randomized benchmarking, and in the long term by monitoring the effective number of logical (error corrected) qubits that a system represents.

今回お話出来なかったこと

量子計算機による共通鍵暗号の安全性評価

- Groverのアルゴリズムを用いた評価
  - 汎用的な鍵探索 ($2^{n/2}$)
  - ハッシュ関数の衝突探索 ($2^{n/3}$)
- Simonのアルゴリズムを用いた評価 (2010-)
  - Even-Mansour構成，3-round Feistel schemeに対する攻撃（多項式時間）(Kuwakado-Morii, ISIT2010)
  - LWR構成，多くの暗号利用モードに対する攻撃（多項式時間）(CRYPTO2016)

現在，活発に研究が行われている

まとめ

量子計算機と暗号技術の関係について整理

(1) 理論的には，多項式時間で解読可能
- 回路構成，必要なリソースもよく知られている

(2) 実際の素因数分解実験を紹介
- いくつかの物は，素因数分解実験としては不適当
- いくつかの物は，ターゲットとする合成数に強く依存
- 汎用的な回路による実験が望ましい

(3) 量子計算機の将来の動向を調査
- 将来を予測することは難しい

- 量子計算機の到来を適切に恐れることができるのは，まだまだ当分先の話.
- 色々な方面から研究を進める必要がある.