計算量的安全な量子暗号の最近の進展

耐量子計算機暗号と量子情報の数理（2022.8.3）

NTT社会情報研究所

山川高志

量子暗号

- 初期の「量子暗号」は主に情報理論的安全なものを扱っていた
  - 量子マネー[Wiesner70]、量子鍵配送[BB84]
- 2000年頃から計算量的安全な「量子暗号」の研究が少しずつ始まる
  - 量子コミットメント[DMS00]、量子公開鍵暗号[OUT00,KKNY05]、量子準同型暗号[BJ15] etc.
- 2017-18にMahadevらによるブレークスルー
- 以降研究が非常に活発化している
- 本講演ではそれらのうち特に自分の研究を中心に紹介する

Mahadevらによるブレークスルー

格子問題（LWE問題）が量子多項式時間で解けないという仮定の下で以下を実現

- 量子性の古典検証
- 乱数性の検証

[Brakerski-Christiano-Mahadev-Vazirani-Vidick18]

- 量子完全準同型暗号

→ブラインド量子計算

[Mahadev18a]

- 量子計算の検証

[Mahadev18b]
（FOCS18ベストペーパー）

[Brakerski-Christiano-Mahadev-Vazirani-Vidick18]:
A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device, FOCS ‘18
[Mahadev18a]: Classical Homomorphic Encryption for Quantum Circuits, FOCS ‘18
[Mahadev18b]: Classical Verification of Quantum Computations FOCS ‘18

本講演の内容

1．Mahadevの量子計算の古典検証の改良
2．Mahadevの技法の別の応用
3．格子問題以外からの構成に向けて

本講演の内容

1．Mahadevの量子計算の古典検証の改良

2．Mahadevの技法の別の応用

3．格子問題以外からの構成に向けて

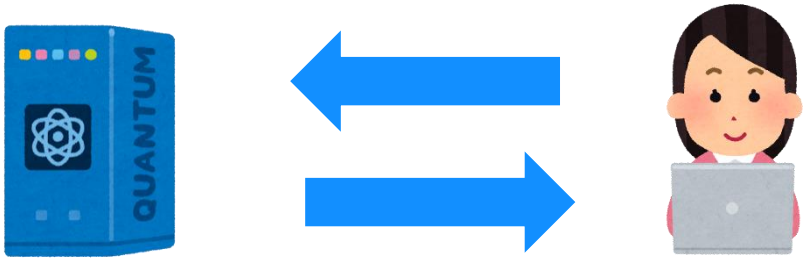
量子計算の古典検証

- 量子計算の正しさを古典で検証

- [Mahadev18b]：4ラウンドのプロトコルを構成
  - 完全性：証明者が正しく実行した時受理確率≈ 1
  - 健全性：間違った計算結果を受理する確率≤ $\frac{3}{4} + negl$
- 自然な問題：
  - 健全性エラーをneglに出来ないか？
  - 4ラウンドより減らせないか？

並列繰り返し＋ラウンド数削減[CCY20,ACGH20]

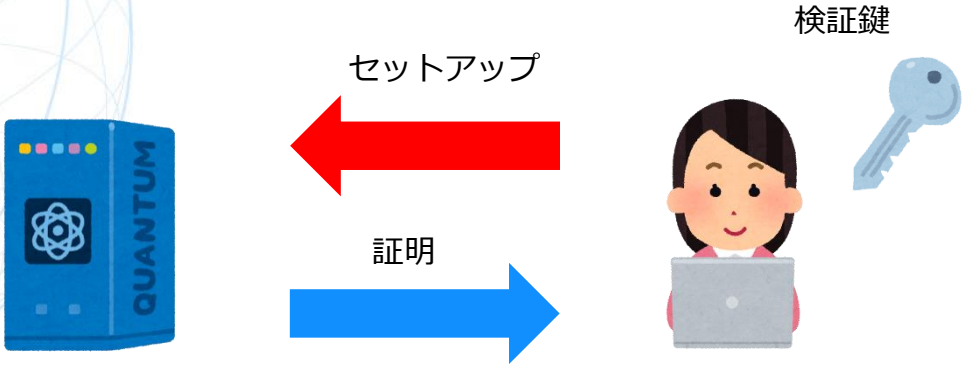
- **健全性エラーnegl**
  - Mahadevのプロトコルを並列に繰り返し実行
  - 並列繰り返しによる健全性低減は一般には成り立たない
    → Mahadevのプロトコルの具体的な性質を用いる
- 量子ランダムオラクルモデルで4ラウンド→**2ラウンド**
  - 検証者のメッセージをハッシュ関数の出力で置き換える（Fiat-Shamir変換）
  - 1ラウンド目はinstance非依存に出来るので事実上**非対話**[ACGH20] (次頁)



[CCY20]: Classical Verification of Quantum Computations with Efficient Verifier, TCC'20
[ACGH20]: Non-interactive Classical Verification of Quantum Computation, TCC'20

非対話？

[ACGH20]



- 検証鍵を持ってる人しか検証できない！(designated verifier model)
- **公開検証**可能な非対話な量子計算の古典検証プロトコルは？
  - [BM22]:理想的難読化に基づくヒューリスティック
  - 妥当な仮定に基づく構成は非常に重要なopen problem

[BM22]: Indistinguishability Obfuscation of Null Quantum Circuits and Applications, ITCS'22

検証の効率化[CCY20,BKLMMVVY22]

NTT

- Mahadev（およびその2ラウンド版）は時間Tの量子計算を検証するのに時間**poly(T)**の古典計算が必要
- **古典**の世界では、時間Tの古典計算を時間**polylog(T)**で検証できる(delegation protocol)[Kilian92,Micali00]
- 時間Tの**量子**計算も時間**polylog(T)**の古典計算で検証出来るか？
- 出来た（ただし追加でiO＝indistinguishability obfuscationを仮定）
  - アイディア：Mahadevのプロトコルの検証アルゴリズムも古典delegation protocolを使って証明者に行わせる
- Open problem: LWEのみからpolylog(T)検証出来るか？

[BKLMMVVY22]: Succinct Classical Verification of Quantum Computation, CRYPTO'22

さらなる改良

- ゼロ知識[ACGH20]
  - 検証者は計算の正しさ以上の「知識」を得ない
- 量子知識の証明[VZ21]
  - 証拠量子状態を「知っている」ことを証明
- 証明者の効率化[Zhang22]
  - 時間Tの量子計算を時間$O(T)$で証明（Mahadevは$O(T^3)$）

[VZ21]:Classical Proofs of Quantum Knowledge, Eurocrypt ‘21
[Zhang22]: Classical Verification of Quantum Computations in Linear Time, FOCS’22

本講演の内容

1．Mahadevの量子計算の古典検証の改良

2．Mahadevの技法の別の応用

3．格子問題以外の仮定に基づくアプローチ

Mahadevのアイディア

- $f: X \to Y$を2対1のトラップドア衝突困難関数とする
  - $f(x) = f(x')$なる$x \neq x'$が見つけられない
  - トラップドアを使うとyから$f(x) = f(x') = y$なる$x \neq x'$を見つけられる
- 以下の操作を考える：

第2レジスターを測定

$$\frac{1}{\sqrt{|X|}}\sum_{x\in X}|x\rangle \to \frac{1}{\sqrt{|X|}}\sum_{x\in X}|x\rangle|f(x)\rangle \to \frac{1}{\sqrt{2}}(|x\rangle + |x'\rangle)|y\rangle$$

ここで、$f(x) = f(x') = y$

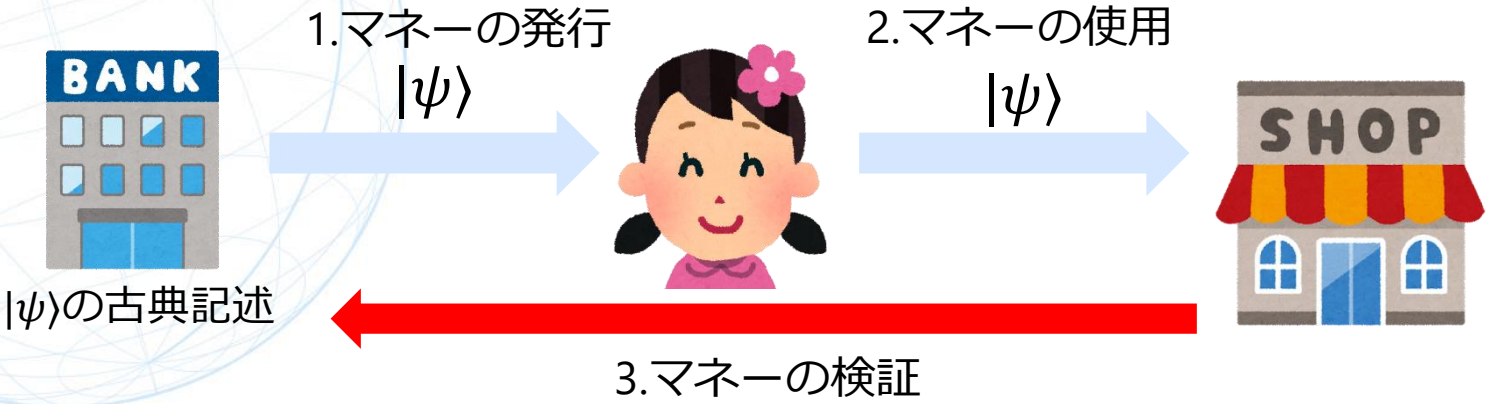
- **xとx'を知らずに$\frac{1}{\sqrt{2}}(|x\rangle + |x'\rangle)$が生成できる！**
- 自分で作った量子状態なのに、その古典記述を知らないのでコピー出来ない

→外部から量子状態が送られてきた状況を「擬似的に実現」できる

→量子通信を古典通信に置き換える応用多数（ある意味Mahadevもその例）

注：このアイディア自体は必ずしもMahadevらが最初とは言えない。
(先行研究の例:[Lutomirski-Aaronson-Farhi-Gosset-Kelner-Hassidim-Shor ICS10]: Breaking and making quantum money: Toward a new quantum cryptographic protocol)
これをLWEと結び付けて重要な応用を示したのが貢献

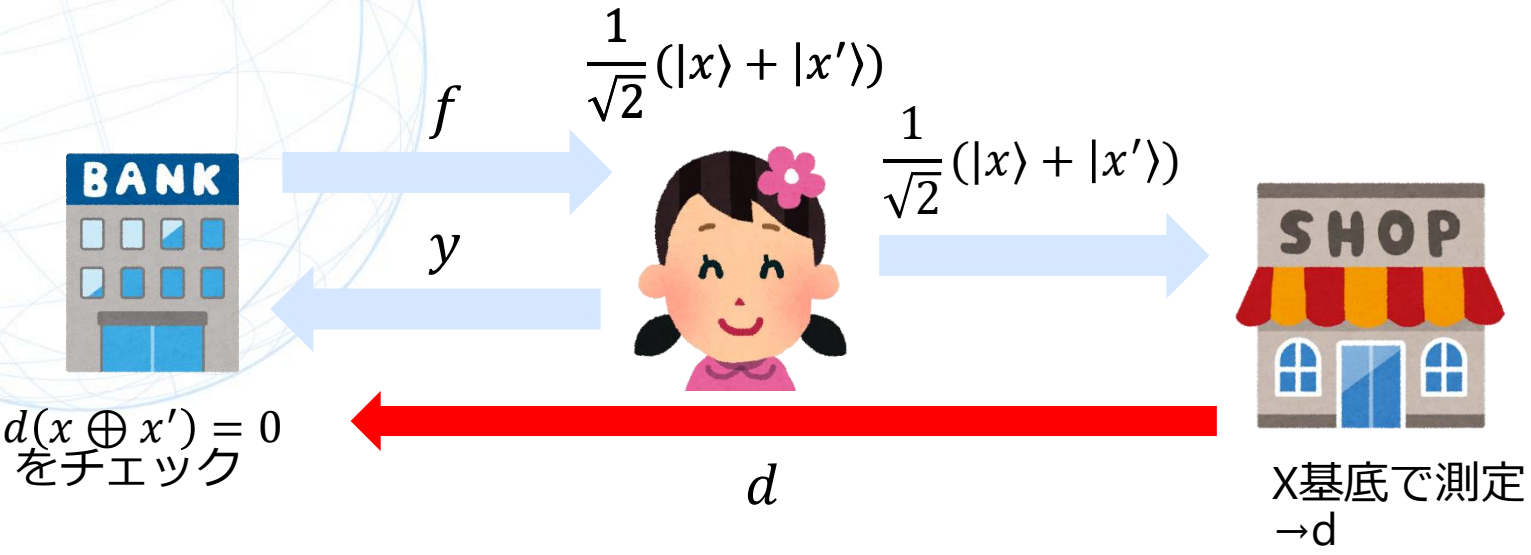
量子マネー



- 1と3が古典 (semi-quantum money) [RS19]
  - LWEに基づく
- 1が古典、3が不要(public-key semi-quantum money) [Zhandry19,Shmueli22]
  - 識別不可性難読化（iO）に基づく
- 1,2が古典、3が不要 [AGKZ20]
  - 理想的な難読化ヒューリスティックに基づく
  - 具体的仮定からの構成はopen

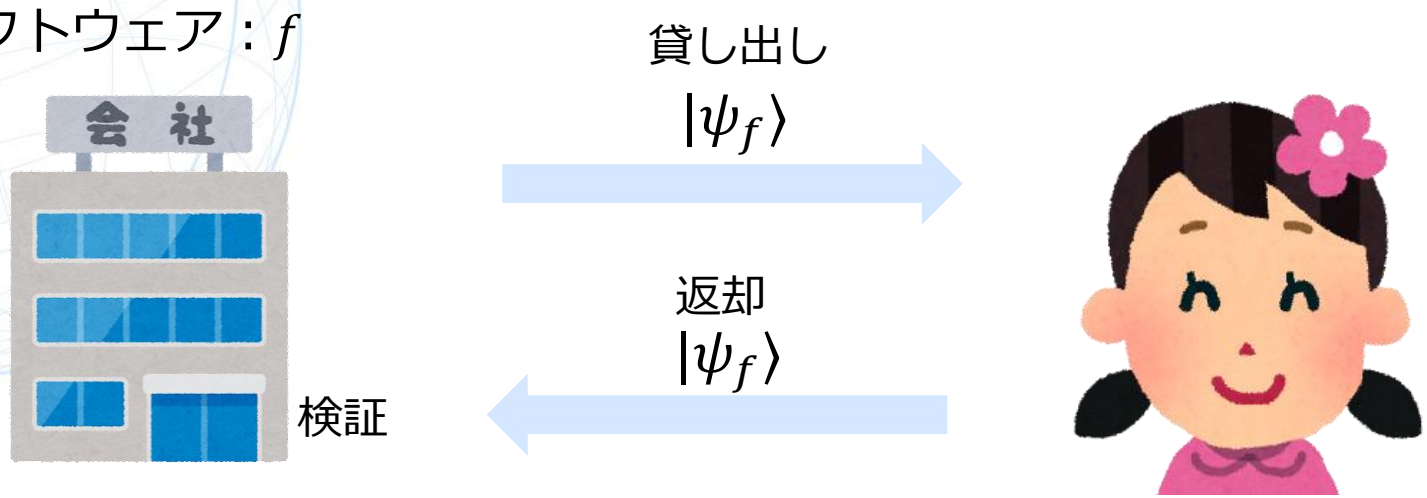
[RS19]: Semi-Quantum Money
[Zhandry19]: Quantum Lightning Never Strikes the Same State Twice, Eurocrypt '19
[Shmueli22]: Public-key Quantum money with a classical bank STOC'22
[AGKZ20]: One-shot Signatures and Applications to Hybrid Quantum/Classical Authentication, STOC'20

Semi-Quantum Money from LWE [RS19]



（上記だけだとでたらめにdを送っても受理確率1/2なので、
並列繰り返しでこの確率をneglに低減する）

ソフトウェア貸し出し[Ananth-La Placa 21]



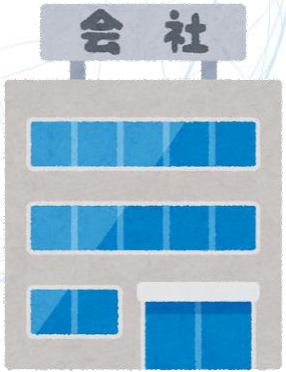
- 返却後の検証にパスしたら、もはやユーザーはfを計算出来ない
  - 😢任意のfに対しては不可能 [ALP20]
  - 😄特別なfについては構成可能
    - Compute-and-compare関数：$f_{g,y}(x) = 1 \Leftrightarrow g(x) = y$

[Ananth-La Placa 21]: Secure Software Leasing, Eurocrypt'21

ソフトウェア貸し出し with 古典通信[KNY21]

古典通信！

ソフトウェア：f



検証

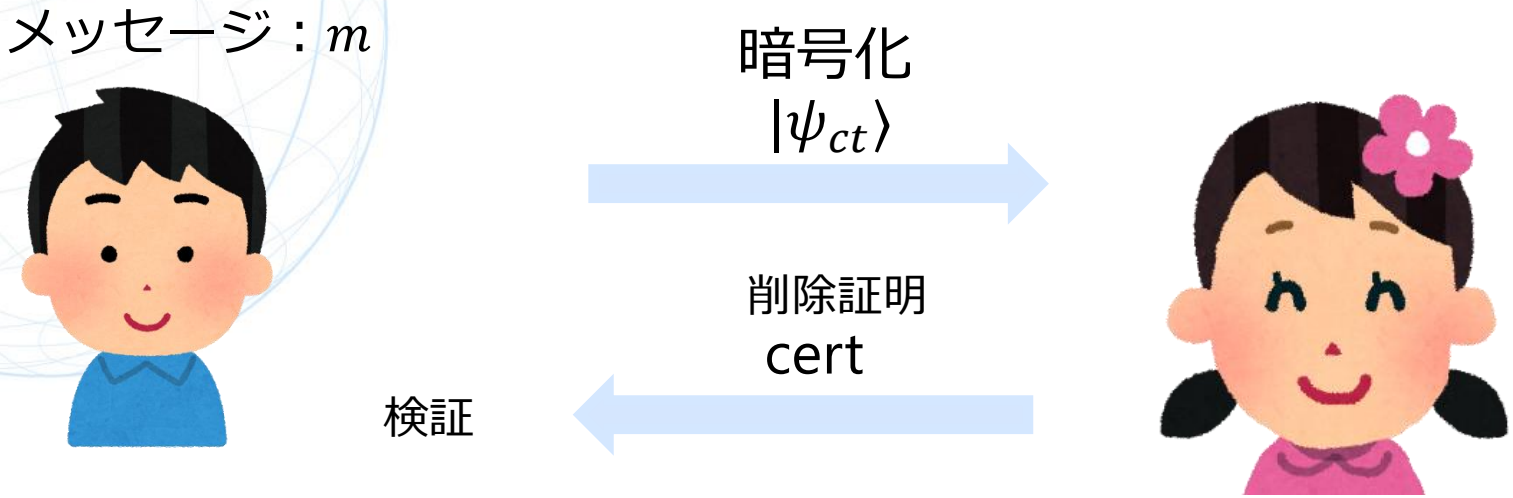
貸し出し

返却
cert

$|\psi_f\rangle$

[KNY21]: Secure Software Leasing from Standard Assumptions, TCC'21

削除証明可能暗号[Broadbent-Islam 20]



- 削除証明の検証にパスしたら、もはや復号鍵を得てもmを計算出来ない
  - 情報理論的安全
  - ワンタイム共通鍵暗号
    - 事前に鍵の共有が必要、かつ一度しか使えない

[BI20]: Quantum encryption with certified deletion, TCC'20

削除証明可能暗号 with 古典通信[HMNY 21]

メッセージ：m

古典通信！

暗号化

$|\psi_{ct}\rangle$

削除証明

cert

検証

- 事前の鍵共有不要（公開鍵）
- 計算量的安全性

[HMNY21]: Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication, Asiacrypt'21

量子通信を古典通信に一般に置き換えられるか？

- 量子通信がランダムBB84状態の送信の場合（ある意味）出来る [Gheorghiu-Metger-Poremba 22]
- 彼らの結果：**Remote State Preparation** for BB84状態を LWEから構成
  - 古典の検証者が指定した基底のBB84状態を量子の証明者がローカルに生成するが、証明者は自分の作った状態が何かわからない
- 多くの暗号プロトコルの量子通信を統一的方法により古典通信に置き換え可
- ただし、1/polyセキュリティロスかつ、polyラウンド
  - 個別の方法ならば多くの場合neglセキュリティロス、constantラウンド
- 個別の方法と同等の性能を持った一般的手法はopen

[Gheorghiu-Metger-Poremba 22]: Quantum cryptography with classical communication: Parallel remote state preparation for copy-protection, verification, and more

本講演の内容

1．Mahadevの量子計算の古典検証の改良

2．Mahadevの技法の別の応用

3．格子問題以外からの構成に向けて

LWE以外の仮定

- Mahadevの結果＆その応用は全てLWEに基づく
- 他の仮定から出来ないか？

NIST耐量子暗号標準化で用いられた主な仮定の候補：

- 格子（含LWE）
- 符号
- 同種写像
- 多変数多項式
- ハッシュ関数

「構造」を持った数学的仮定
公開鍵暗号＆電子署名

特定の数学的「構造」を持たない
電子署名のみ
公開鍵暗号は（ブラックボックスには）不可能
[Impagliazzo-Rudich89]

- ハッシュ関数のみでどこまで行けるか？

我々の結果[YZ22]

- 量子性の古典検証
- 乱数性の検証
- 量子完全準同型暗号
  →ブラインド量子計算
- 量子計算の検証

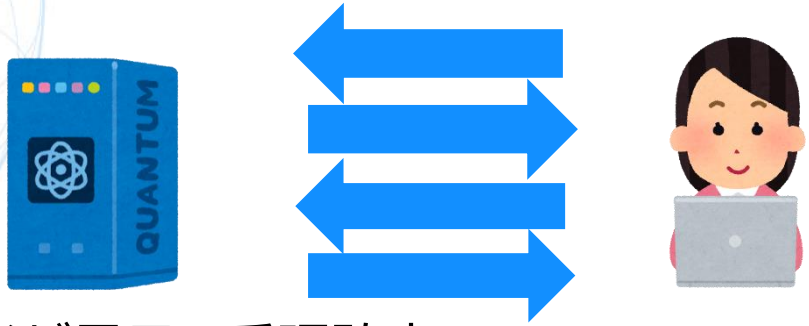
ここまでハッシュ関数で出来た！

ここはOpen

[YZ22]:Verifiable Quantum Advantage without Structure, FOCS'22

量子性の古典検証

- 量子コンピュータを持ってる事を古典で検証



- 完全性：証明者が量子→受理確率≈ 1
- 健全性：証明者が古典→受理確率≪ 1
- Mahadev: LWEに基づいて構成
- Shor: 素因数分解または離散対数問題に基づいて（暗黙に）構成
- 他にも検証可能かつ指数的量子加速のある任意の問題で出来る
  - ペル方程式[Halgren02], 行列群メンバーシップ[BBS09]

→**検証可能な指数的量子加速はハッシュ関数のみで実現出来るか？**

Observation and Our Result

- 既存の検証可能指数的量子加速を与える問題は全て
  1．**公開鍵暗号**の構成に使える
  2．量子加速は本質的に**周期発見**アルゴリズムに基づく

→これらはある種の「構造」を持った問題

- 「構造」のない問題で検証可能指数的量子加速はあるか？
- “The Need for Structure in Quantum Speedups” [AA14]
  - 「構造」を持たない「判定」問題は指数的量子加速を持たないだろう（Aaronson-Ambainis Conjecture）
- 我々の結果：「構造」を持たない検証可能**「探索」**問題に対して指数的量子加速が存在
  - ランダムオラクルに相対化して、あるNP探索問題が存在して、量子多項式時間で解けるが古典確率的多項式時間で解けない

我々の探索問題

- $C \subseteq \mathbb{F}_q^n$: 線形符号（線形部分空間）
- $H_i: \mathbb{F}_q \to \{0,1\}$ $(i = 1, \ldots, n)$ ハッシュ関数（ランダムオラクルとしてモデル化）

問題：符号語$x = (x_1, \ldots, x_n) \in C$であって、
$$H_i(x_i) = 1 \text{ for } i = 1, \ldots, n$$
を満たすものを求めよ

- 古典困難性の直観：
  - でたらめに符号語を取ると、条件を満たす確率$= 2^{-n}$
  - 各iについて$H_i(x_i) = 1$なるx_iをでたらめに取ると$(x_1, \ldots, x_n) \in C$ となる確率は指数的に低い（Cはsparseになるようにパラメータ設定するため）

古典困難性

- 攻撃者によるH_iへのクエリの集合： $S_i \subseteq \mathbb{F}_q$ $(|S_i| = poly(n))$
- もし$\#\{(x_1, \dots, x_n) \in C : x_i \in S_i \text{ for } i = 1, \dots, n\} \gg 2^n$とすると・・・

→その中で$H_i(x_i) = 1$ for $i = 1, \dots, n$ なる答えが見つかる確率が高い

- これを防ぐため、Cが**list-recoverability**を仮定

$\exists 0 < \delta, \epsilon, \epsilon' < 1$ s.t. for any $S_i \subseteq F_q$ s.t. $|S_i| = 2^{n^\epsilon}$ for $i = 1, \dots, n$,

$\#\{(x_1, \dots, x_n) \in C : x_i \notin S_i$ なるiがδn個以下$\} \leq 2^{n^{\epsilon'}}$

古典困難性の証明：

- 攻撃者の最終出力$(x_1, \dots, x_n)$について、 すべてのiについてx_iはH_iにクエリされたとwlogで仮定
- 途中のどこかで、 x_iがH_iにクエリされて**いない**iの個数はちょうどδn個となったはず
- その状態から、 $(x_1, \dots, x_n)$が答えになるためには、まだクエリしていないiについてたまたま$H_i(x_i) = 1$にならないといけないので、その確率は$2^{-\delta n}$
- List-recoverabilityから、そのような$(x_1, \dots, x_n)$の候補は高々$2^{n^{\epsilon'}}$個
- Union boundにより、攻撃者の成功確率$\leq 2^{n^{\epsilon'}} \cdot 2^{-\delta n} = 2^{-\Omega(n)}$

量子容易性(1/2)

- $V\colon \mathbb{F}_q^n \to \mathbb{C},\ W\colon \mathbb{F}_q^n \to \mathbb{C}$

(QFT: 量子フーリエ変換)

$$\sum_{x\in\mathbb{F}_q^n} (V\cdot W)(x)|x\rangle \underset{\mathrm{QFT}^{-1}}{\overset{\mathrm{QFT}}{\rightleftarrows}} \propto \sum_{x\in\mathbb{F}_q^n} \left(\hat{V} * \hat{W}\right)(x)|x\rangle$$

$$= \sum_{y,z\in\mathbb{F}_q^n} \hat{V}(y)\,\hat{W}(z)|y+z\rangle$$

- $V(x) = \begin{cases} 1\ (x \in C) \\ 0\ (\text{otherwise}) \end{cases}, W(x) = \begin{cases} 1\ (H_i(x_i) = 1 \text{ for } i = 1, \dots, n) \\ 0\ (\text{otherwise}) \end{cases}$
- $\sum_{x\in\mathbb{F}_q^n}(V\cdot W)(x)|x\rangle$が得られれば単に測定すれば問題が解ける

→ $\sum_{x\in\mathbb{F}_q^n}\left(\hat{V} * \hat{W}\right)(x)|x\rangle$を作れれば良い

量子容易性(2/2)

- $\sum_x (\hat{V} * \hat{W})(x)|x\rangle = \sum_{y,z} \hat{V}(y)\,\hat{W}(z)|y+z\rangle$を作りたい

$$\sum_y V(y)\,|y\rangle \otimes \sum_z W(z)\,|z\rangle$$

↓ QFT

$$\sum_y \hat{V}(y)\,|y\rangle \otimes \sum_z \hat{W}(z)\,|z\rangle$$

↓ 重ね合わせで足しこむ

$$\sum_{y,z} \hat{V}(y)\,\hat{W}(z)|y\rangle|y+z\rangle$$

↓ uncompute

$$\sum_{y,z} \hat{V}(y)\,\hat{W}(z)|y+z\rangle$$

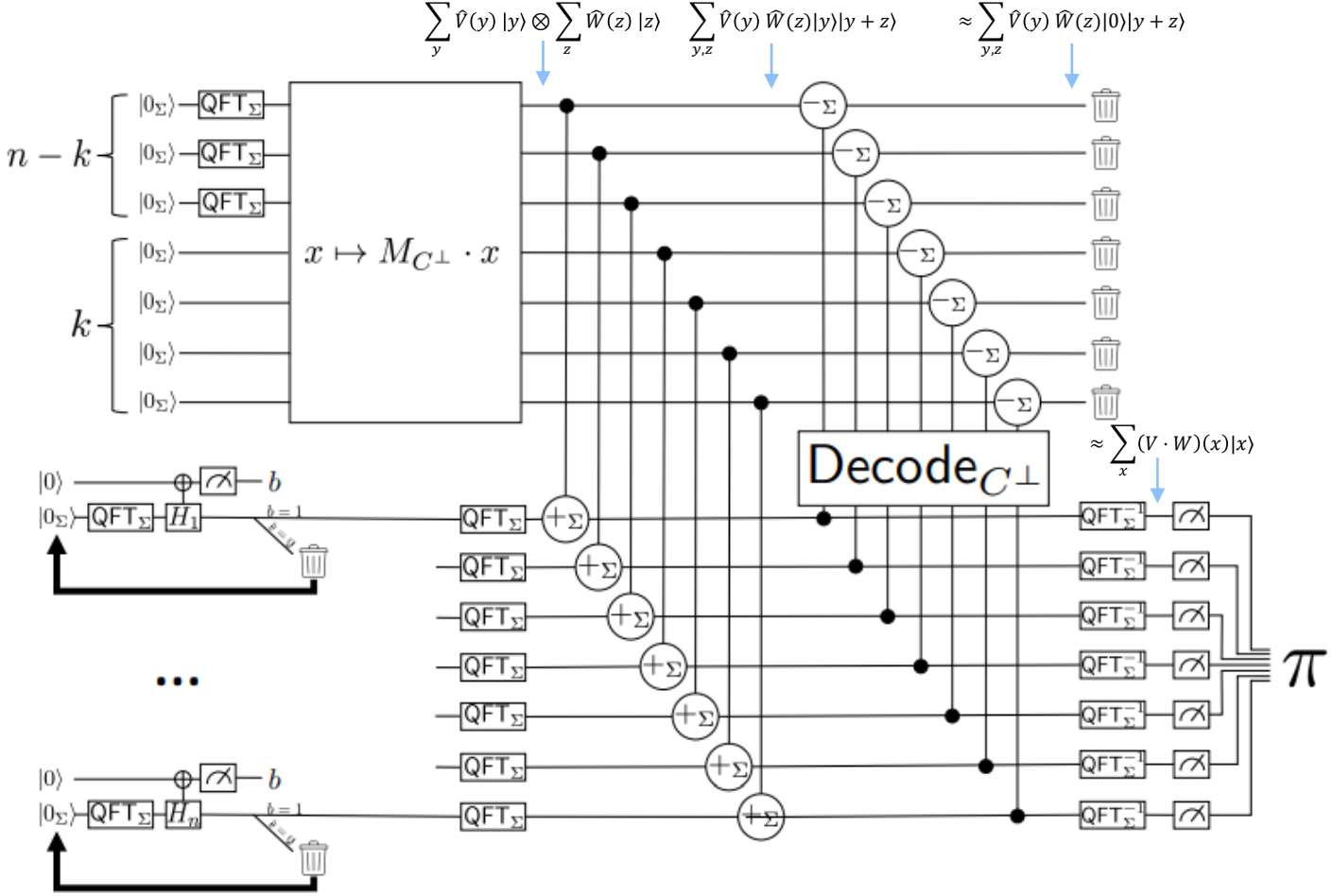
$$V(y) = \begin{cases} 1\ (y \in C) \\ 0\ (\text{otherwise}) \end{cases}$$

$$W(z) = \begin{cases} 1\ (H_i(z_i) = 1 \text{ for } i = 1, \dots, n) \\ 0\ (\text{otherwise}) \end{cases}$$

$$\hat{V}(y) = \begin{cases} 1\ (y \in C^{\perp}) \\ 0\ (\text{otherwise}) \end{cases}$$

$\hat{W}$はハミング重み小さいベクトルに集中している
（各iについて$H_i(x_i) = 1$なるx_iの割合≈1/2のため）
→ $C^{\perp}$が適切な効率的decodingアルゴリズムを持てば、
重ね合わせ実行でuncompute出来る！

量子回路


$\sum_y \hat{V}(y)\,|y\rangle \otimes \sum_z \hat{W}(z)\,|z\rangle$
$\sum_{y,z} \hat{V}(y)\,\hat{W}(z)|y\rangle|y+z\rangle$
$\approx \sum_{y,z} \hat{V}(y)\,\hat{W}(z)|0\rangle|y+z\rangle$
$n-k$
k
$|0_\Sigma\rangle$
QFT_Σ
$x \mapsto M_{C^\perp} \cdot x$
$\mathrm{Decode}_{C^\perp}$
$\approx \sum_x (V \cdot W)(x)|x\rangle$
$|0\rangle$
b
H_1
H_n
$b=1$
$a=y$
π

使用する符号

- 古典困難性のために、Cがlist-recoverable、
  量子容易性のために、 $C^{\perp}$ がefficiently decodable
  であることを仮定
- Folded Reed Solomon Code [Guruswami-Rudra ‘08]
  - Reed-Solomon Codeの複数シンボルを一塊でシンボルと見る
  - List-recoverable
  - Its dual is generalized Reed-Solomon code → efficiently decodable
  - （厳密に言うと線形符号でないが、線形符号の仕切りを変えただけなので、
    線形符号に対する手法がそのまま使える）

[Guruswami-Rudra ‘08]: Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy

RegevのSIS→LWE帰着との類似

SIS問題：$x = (x_1, \dots, x_n) \in C$であって、

$$|x_i| \leq \beta \text{ for } i = 1, \dots, n$$

を満たすものを求めよ

我々の問題：$x = (x_1, \dots, x_n) \in C$であって、

$$H_i(x_i) = 1 \text{ for } i = 1, \dots, n$$

を満たすものを求めよ

[Regev ‘05]: SISを解くためにはdual格子でLWEが解ければよい

我々：帰着は類似、ただし帰着先の”LWE”のようなものが
特殊な格子＋エラー分布のおかげで容易に解ける

乱数性の証明

- 私たちの量子アルゴリズム：
  $\sum_x (V \cdot W)(x)|x\rangle$を生成→測定
  →（ほぼ）一様ランダムな解を得る
- AA conjecture:「構造」を持たない「判定」問題は指数的量子加速を持たないだろう
- もし決定的に解ける量子アルゴリズムがあったとする

→出力の各ビットが0か1かの判定問題に帰着出来る

→AA conjectureのもとで指数的量子加速は起こらない

したがって、 AA conjectureのもと、我々の問題を解く量子アルゴリズムの出力は必ずランダムであることが示される

Open Problems

- ランダムオラクルの代わりにone-way functionやcollision-resistant hashではできないのか？
  - non-interactiveだとブラックボックスには不可能（folklore）
- 乱数性の証明をAA conjecture無しで出来るか？
- ランダムオラクルを使ってブラインド量子計算や量子計算の検証が出来るか？
- 我々の量子性の検証を現実世界で実装できるか？
- 我々の量子アルゴリズムの他の有用な応用はあるか？

今回（あまり）扱わなかった話題

- No-cloning定理の暗号理論的活用（必ずしも古典通信に限らない）
  - Quantum money [Aaronson09, AC12, RS19, Zhandry19,AGKZ20, Shmueli 21, Shmueli 22,KLS22], unclonable encryption[BL20,AK21,MST21,AKLLZ22], certified deletion [BI20,HMNY21,HMNY22b,BK22], revocable time-release encryption[Unruh14], copy-protection [Aaronson09,ALLZZ20,CMP20,CLLZ21], secure software leasing [ALP20,KNY20,BJLPS21]
- 量子コミットメント[DMS00,CLS01,KO09,KO11,YWLQ15,Yan20,FUYZ20,BB21,AQY22,MY22]
- 量子ゼロ知識証明[BJSW16,BG20,ACGH20,CVZ20,Shmueli21,MY21,BM21,CM21,BY22,HMNY22a]
- 量子秘密計算
  [CGS02,BCG+06,Unruh10,DNS12,KP17,DGJ+20,GLSV21,BCKM21a,BCKM21b,Bartusek21]
- 量子帰着の不可能性[CHS20,HY20,CX21,ACC+22]
- 量子情報的議論を用いた耐量子安全性の証明
  - 量子ランダムオラクルモデル[BDF+11,Zhandry12,TU16,Unruh15,Unruh17,SXY18,KLS18,JZC+18, KYY19,Zhandry19,LZ19,DFMS19,AHU19,BHH+19,CMS19,HXY19,CLQ19,KSS+20,DFM20,CGLQ20,GLLZ21,AGL22]
  - 量子攻撃者の巻き戻し技法
    [Watrous06,Unruh12,Unruh16a,Unruh16b,CCY20,Zhandry20,CMSZ21,KN22,CCLY22,BBK22,LMS22,LPY22]
  - 量子non-black-boxシミュレーション[BS20]

まとめ

1．Mahadevの量子計算の古典検証の改良

-大量の後続研究：健全性増幅、ラウンド数削減、ゼロ知識、効率的検証/証明、量子知識の証明、公開検証 etc.

2．Mahadevの技法の別の応用

-特に古典通信で量子暗号プロトコルを実現するのに有効

3．格子問題以外からの構成に向けて

- ハッシュ関数のみで量子性の検証