（耐量子）ゼロ知識証明入門

第三回量子情報ワークショップ（2020.7.3）

NTTセキュアプラットフォーム研究所
山川高志

目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

ゼロ知識証明とは？

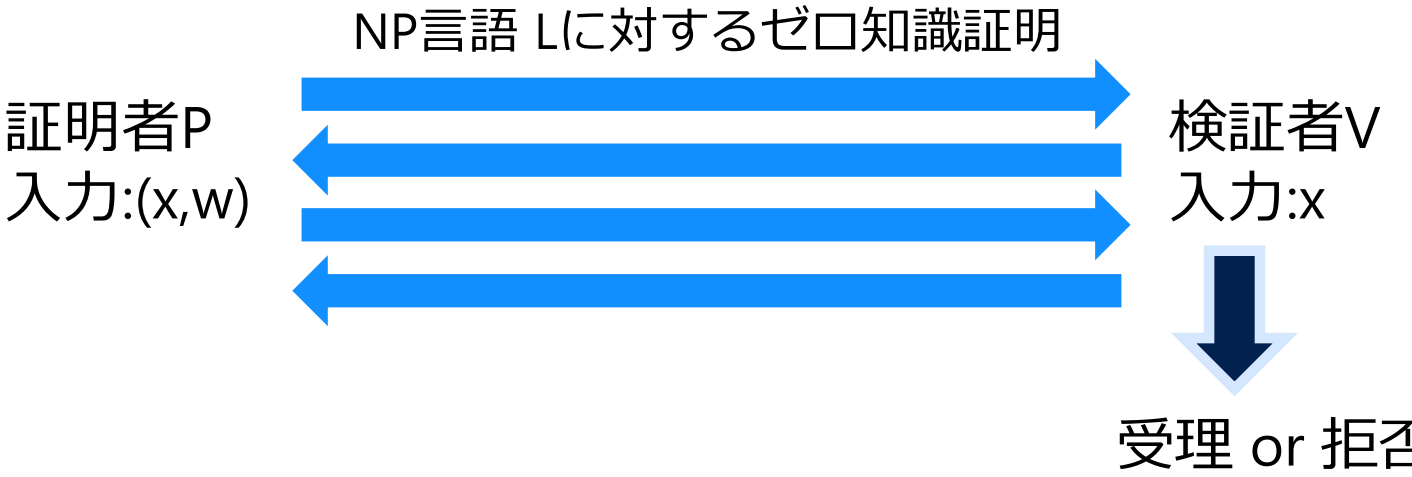
- 「暗号学において、**ゼロ知識証明**（ぜろちしきしょうめい、zero-knowledge proof）とは、ある人が他の人に、自分の持っている（通常、数学的な）命題が真であることを伝えるのに、真であること以外の何の知識も伝えることなく証明できるようなやりとりの手法である。」（Wikipediaより引用）
- 例：Aさんはパズルの難問をBさんに出題した
- あまりにも解けないのでBさんは答えが存在しないことを疑った
- Aさんは答えは確かに存在することを主張したい
- しかし、答え自体を送るともはやパズルとして意味をなさない
- 答えを送らずに答えが存在することを納得させたい

→**ゼロ知識証明！**[GMR89]

P言語とNP言語

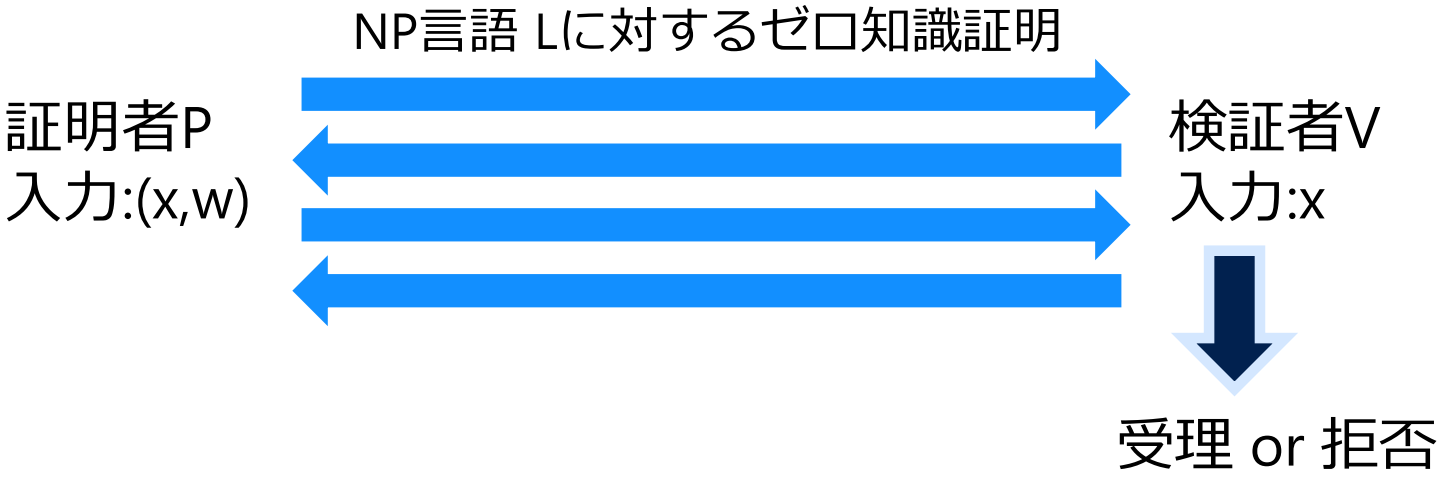
- P言語：多項式時間(Polynomial-Time)で解ける判定問題
  - ビット列の集合（言語）$L \subseteq \{0,1\}^*$ がP言語であるとは、
    ヨ古典多項式時間決定的チューリングマシン M s.t. $\forall x \in \{0,1\}^*$
    If $x \in L \Leftrightarrow M(x) = 1$
- NP言語：「答え」が正しいかを多項式時間で検証可能な判定問題
  - ビット列の集合（言語）$L \subseteq \{0,1\}^*$ がP言語であるとは、
    ヨ古典多項式時間決定的チューリングマシン M s.t. $\forall x \in \{0,1\}^*$
    If $x \in L \Leftrightarrow \exists w\, s.t.\, M(x,w) = 1$
- NP完全言語：任意のNP言語から帰着できるNP言語
  - 例：SAT, ハミルトン閉路、ナップサック、テトリス etc…
  - あるNP完全言語に対するゼロ知識証明→任意のNP言語に対するゼロ知識証明

NP言語に対するゼロ知識証明



完全性： $x \in L$ の時正しく実行すれば（無視可能な確率を除いて）受理
健全性： $x \notin L$の時Pがどんなずるをしても受理確率は無視可能
ゼロ知識性： $x \in L$ でPが正直に動くとき、Vはどんなずるをしても
「$x \in L$ である」という以上の"知識"を得られない

NP言語に対するゼロ知識証明

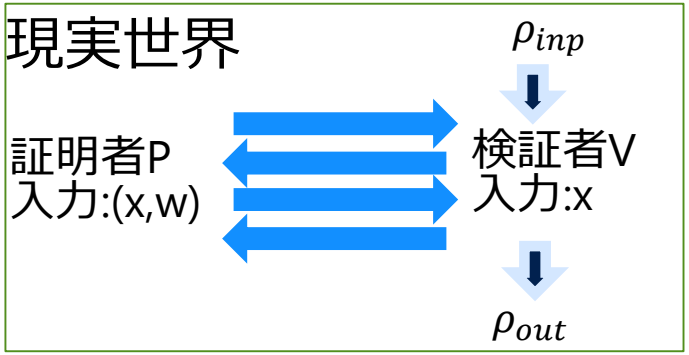


完全性： $x \in L$ の時正しく実行すれば（無視可能な確率を除いて）受理
健全性： $x \notin L$の時Pがどんなずるをしても受理確率は無視可能
ゼロ知識性： $x \in L$ でPが正直に動くとき、Vはどんなずるをしても
「$x \in L$ である」という以上の"知識"を得られない

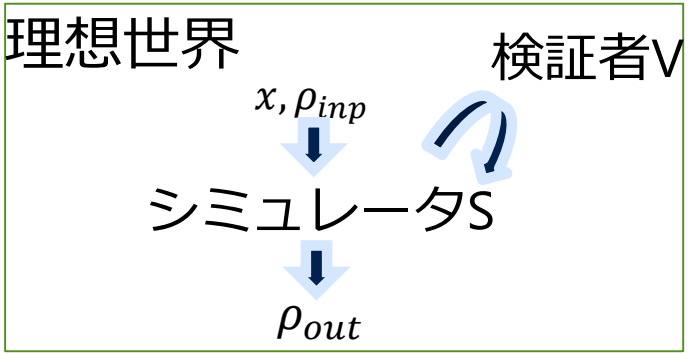
無視可能：セキュリティパラメータ（≒問題サイズ）に対して超多項式的に減衰すること

ゼロ知識性

証明プロトコルが（耐量子）ゼロ知識であるとは、
任意の多項式時間（量子）検証者Vに対して、あるシミュレーターSが存在して
以下の二つの世界での出力分布は（耐量子）計算量的識別不能



≈



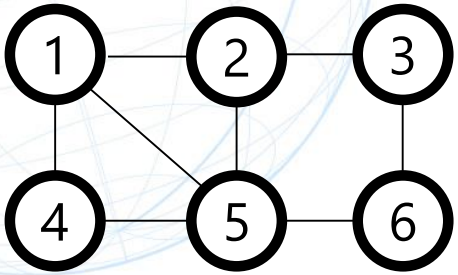
直感：Pとの対話後に出力できる分布はVの入力のみでシミュレート可能
→対話によって何も"知識"を得ていない

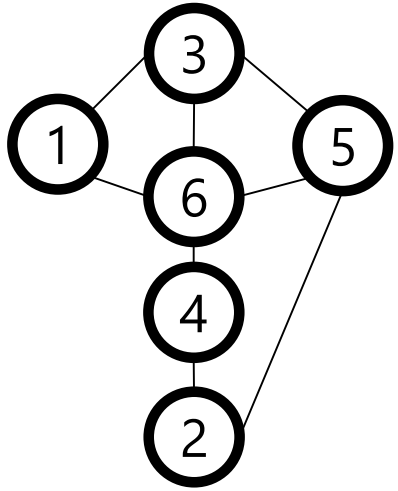
目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

グラフ同型問題

- 与えられた二つのグラフは同型か？





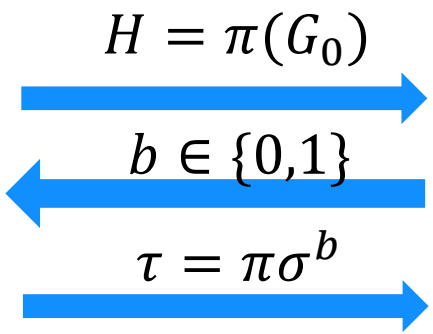
- 1↦3, 2↦5, 4↦1, 5↦6, 3↦2, 6↦4と割り当てれば同型であることが確かめられる
- NPだがPともBQPとも知られていない
  - NP完全ではないと考えられている
  - [Babai16]:古典quasi-polynomial time ($2^{(\log n)^{O(1)}}$時間)アルゴリズム？

グラフ同型問題に対するゼロ知識証明[GMW91]

証明者P
入力:

$$x = (G_0, G_1),$$
$$w = \sigma\ s.t.\ \sigma(G_1) = G_0$$

検証者V
入力: $x = (G_0, G_1)$



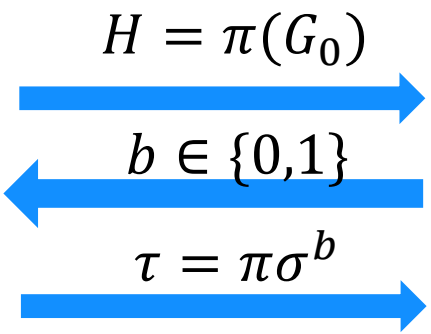
$\tau(G_b) = H$ ⇔受理

グラフ同型問題に対するゼロ知識証明[GMW91]

証明者P
入力:

$x = (G_0, G_1),$
$w = \sigma\ s.t.\ \sigma(G_1) = G_0$

検証者V
入力: $x = (G_0, G_1)$



$\tau(G_b) = H$ ⇔受理

完全性：

$b = 0$の時： $\tau = \pi \rightarrow \tau(G_0) = \pi(G_0) = H$→受理

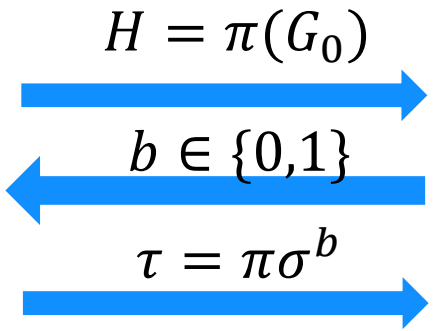
$b = 1$の時： $\tau = \pi\sigma \rightarrow \tau(G_1) = \pi\sigma(G_1) = \pi(G_0) = H$→受理

グラフ同型問題に対するゼロ知識証明[GMW91]

証明者P
入力:

$$x = (G_0, G_1),$$
$$w = \sigma\ s.t.\ \sigma(G_1) = G_0$$

検証者V
入力: $x = (G_0, G_1)$



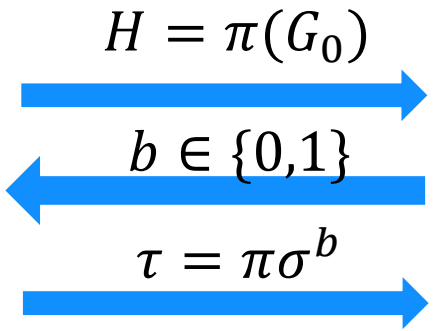
$\tau(G_b) = H$ ⇔受理

健全性:
G_0とG_1が同型でない時、HはG_0とG_1の高々一方としか同型になれない
→$b=0,1$の高々一方にしか正しく答えられない
→検証者の受理確率高々$1/2$
これを無視可能まで低減するために、上記プロトコルを多項式回直列に繰り返せばよい
（健全性低減のためだけなら並列でも良いが、並列繰り返しはゼロ知識性を保たない）

グラフ同型問題に対するゼロ知識証明[GMW91]

証明者P
入力:
$x = (G_0, G_1)$,
$w = \sigma\ s.t.\ \sigma(G_1) = G_0$

検証者V
入力: $x = (G_0, G_1)$



$\tau(G_b) = H$ ⇔受理

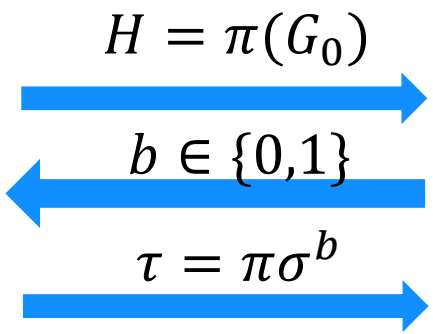
ゼロ知識性:
直感：$b = 0$でも$b = 1$でも検証者が見るのはG_bと同型なグラフHとその間の同型写像τのみ
→それなら自分で簡単に生成できる

グラフ同型問題に対するゼロ知識証明[GMW91]

証明者P
入力:

$$x = (G_0, G_1),$$
$$w = \sigma\ s.t.\ \sigma(G_1) = G_0$$

検証者V
入力: $x = (G_0, G_1)$



$\tau(G_b) = H$ ⇔受理

検証者が量子の場合、元に戻れる保証がない！

（古典）ゼロ知識性:
シミュレーター

1. $b' \in \{0,1\}$とτをランダムに取り、$H = \tau(G_b)$を検証者に送る
2. 検証者が$b \in \{0,1\}$を返す。**$b \neq b'$ならステップ1に戻る**。さもなくば次へ
3. τを検証者に送る
4. 検証者の出力を出力する

耐量子シミュレーションの難しさ

検証者V

シミュレータ

$|\psi_{inp}\rangle|0\rangle|0\rangle$

耐量子シミュレーションの難しさ

検証者V

シミュレータ

$|\psi_{inp}\rangle|0\rangle|0\rangle$

$b' \in \{0,1\}$と
τをランダムに選ぶ

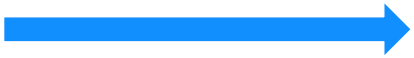
耐量子シミュレーションの難しさ

検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ

$H = \tau(G_{b'})$



$|\psi_{inp}\rangle|0\rangle|0\rangle$

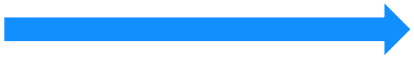
耐量子シミュレーションの難しさ

検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ

$H = \tau(G_{b'})$



$|\psi_{inp}\rangle|0\rangle|H\rangle$

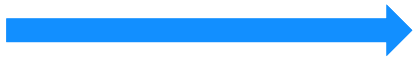
耐量子シミュレーションの難しさ

検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ

$H = \tau(G_{b'})$



$|\psi_{inp}\rangle|0\rangle|H\rangle$

U

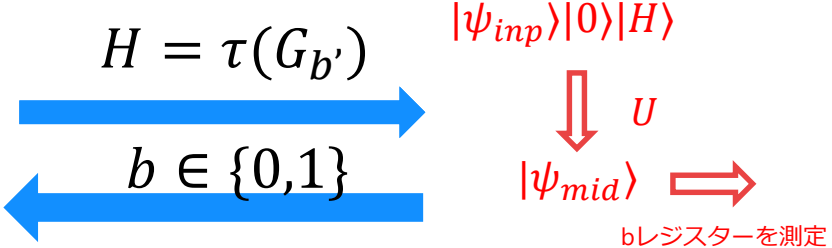
$|\psi_{mid}\rangle$

耐量子シミュレーションの難しさ

検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ



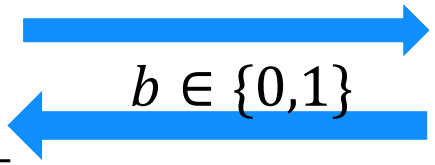
耐量子シミュレーションの難しさ

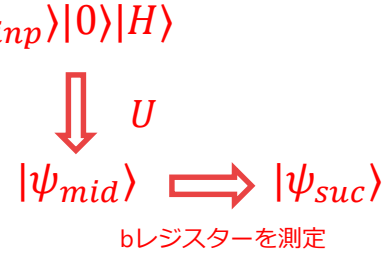
検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ

$b = b'$なら古典と同様に
シミュレーション続行可能





耐量子シミュレーションの難しさ

検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ

$H = \tau(G_{b'})$

$b \in \{0,1\}$

$|\psi_{inp}\rangle|0\rangle|H\rangle$

U

$|\psi_{mid}\rangle \Rightarrow |\psi_{fail}\rangle$

bレジスターを測定

$b = b'$なら古典と同様に
シミュレーション続行可能

$b \neq b'$の時、最初の状態
に巻き戻したい

耐量子シミュレーションの難しさ

検証者V

シミュレータ

$b' \in \{0,1\}$と
τをランダムに選ぶ

$H = \tau(G_{b'})$

$b \in \{0,1\}$

$|\psi_{inp}\rangle|0\rangle|H\rangle \neq |\psi'_{inp}\rangle$

U ⇓　　⇑ U^*

$|\psi_{mid}\rangle \Rightarrow |\psi_{fail}\rangle$

bレジスターを測定

$b = b'$なら古典と同様に
シミュレーション続行可能

$b \neq b'$の時、最初の状態
に巻き戻したい

元に戻らない！

Watrousのシミュレータ[Watrous09]

検証者V

シミュレータ

$b' \in \{0,1\}$とτを確率的に
ランダムに取る代わりに、
それらの均等量子重ね合わせで
実行

$|\psi_H\rangle = \Sigma_{\tau,b'}|\tau(G_{b'})\rangle|\tau\rangle|b'\rangle$

$b = b'$なら古典と同様に
シミュレーション続行可能

$b \neq b'$の時・・・
$|\psi_{fail}\rangle$を$|\psi_{suc}\rangle$に効率的に変換できる！

$|\psi_{inp}\rangle|0\rangle|0\rangle$

$\Downarrow T$

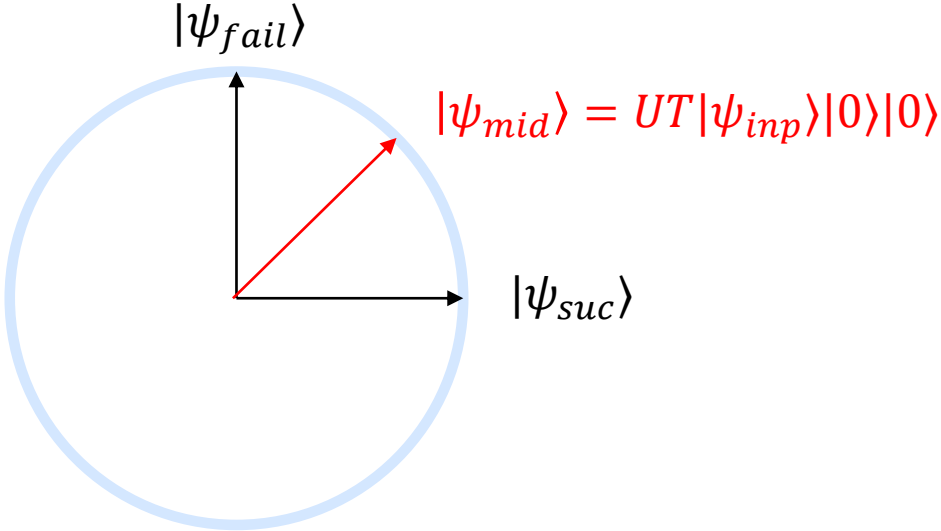
$|\psi_{inp}\rangle|0\rangle|\psi_H\rangle$

$\Downarrow U$

$|\psi_{mid}\rangle \Rightarrow |\psi_{fail}\rangle$

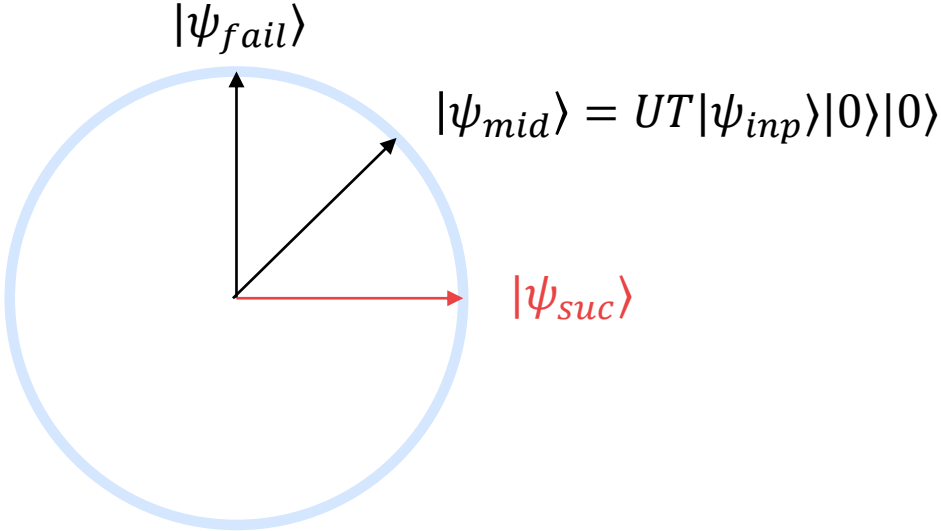
b=b'かを測定

Watrousのシミュレータ[Watrous09]



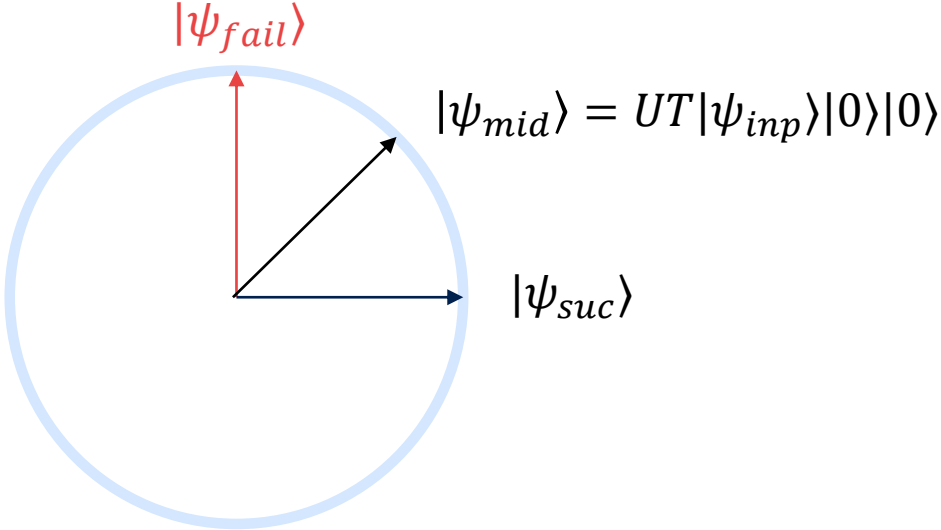
基底$\{|\psi_{suc}\rangle, |\psi_{fail}\rangle\}$で測定（＝(b=b′)かを測定）

Watrousのシミュレータ[Watrous09]



$b = b'$の場合
古典と同様にシミュレーション続行可能

Watrousのシミュレータ[Watrous09]

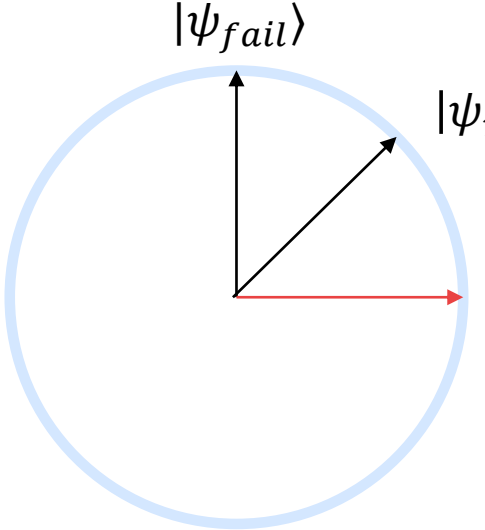


$b \neq b'$の場合
$|\psi_{mid}\rangle$に対して折り返して$|\psi_{suc}\rangle$に持っていく
$\Delta \coloneqq I \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|$ とすると、

$$(UT)\Delta(UT)^*|\psi_{fail}\rangle = \frac{1}{\sqrt{2}}|\psi_{mid}\rangle$$

$$\rightarrow \quad (UT)(2\Delta - I)(UT)^*|\psi_{fail}\rangle = |\psi_{suc}\rangle$$

Watrousのシミュレータ[Watrous09]



$|\psi_{mid}\rangle = UT|\psi_{inp}\rangle|0\rangle|0\rangle$

$|\psi_{suc}\rangle = (UT)(2\Delta - I)(UT)^*|\psi_{fail}\rangle$

$b \neq b'$の場合
$|\psi_{mid}\rangle$に対して折り返して$|\psi_{suc}\rangle$に持っていく
$\Delta := I \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|$ とすると、

$$(UT)\Delta(UT)^*|\psi_{fail}\rangle = \frac{1}{\sqrt{2}}|\psi_{mid}\rangle$$

$$\rightarrow \quad (UT)(2\Delta - I)(UT)^*|\psi_{fail}\rangle = |\psi_{suc}\rangle$$

$(UT)\Delta(UT)^*\left|\psi_{fail}\right\rangle = \frac{1}{\sqrt{2}}|\psi_{mid}\rangle$の証明

$\Delta \coloneqq I \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|$, $\Pi \coloneqq |0,1\rangle\langle 0,1|_{b,b'} + |1,0\rangle\langle 1,0|_{b,b'}$ ($b \neq b'$なる状態への*projection*)

$b \neq b'$となる確率は初期状態$|\psi_{inp}\rangle$によらず$\frac{1}{2}$、つまり

$$|\Pi UT\left|\psi_{inp}\right\rangle|0\rangle|0\rangle|^2 = \frac{1}{2} \rightarrow \langle\psi_{inp}|\langle 0|\langle 0|(UT)^*\Pi UT\left|\psi_{inp}\right\rangle|0\rangle|0\rangle = \frac{1}{2}$$

したがって、任意の$|\psi_{inp}\rangle$に対して

$$\langle\psi_{inp}|(I \otimes \langle 0|\langle 0|)(UT)^*\Pi UT(I \otimes |0\rangle|0\rangle)|\psi_{inp}\rangle = \frac{1}{2}$$

したがって

$$(I \otimes \langle 0|\langle 0|)(UT)^*\Pi UT(I \otimes |0\rangle|0\rangle) = \frac{I}{2} \quad \rightarrow \quad \Delta(UT)^*\Pi UT\Delta = \frac{\Delta}{2}$$

以上より

$$(UT)\Delta(UT)^*\left|\psi_{fail}\right\rangle = UT\Delta(UT)^*\sqrt{2}\Pi UT\Delta\left|\psi_{inp}\right\rangle|0\rangle|0\rangle$$

$$= \frac{1}{\sqrt{2}}UT\Delta\left|\psi_{inp}\right\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}|\psi_{mid}\rangle$$

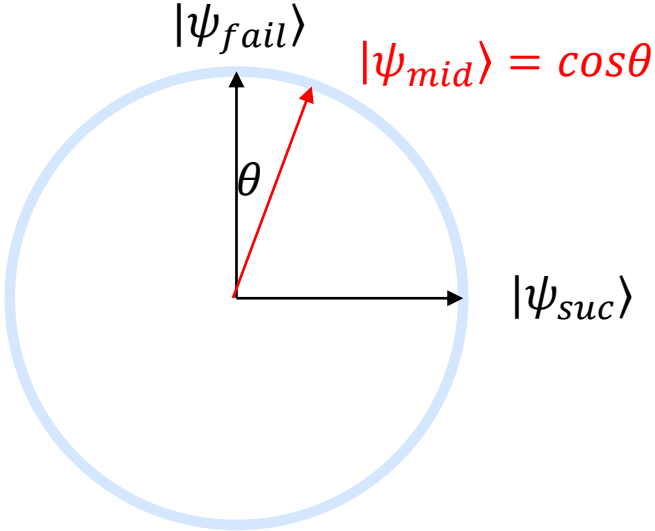
ここまでのまとめ

- 古典のゼロ知識性の証明は巻き戻し(rewinding)というテクニックをよく使う
- 検証者が量子だと巻き戻しが自明には出来ない
- Watrousは量子でも**特定の場合**に巻き戻し可能であることを示した

初期状態によらず「成功確率」が$\frac{1}{2}$
（½でなくても1/polyなら同様に出来る）

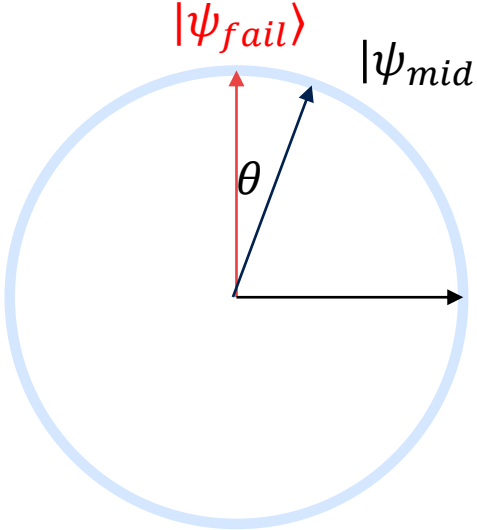
- これにより、グラフ同型問題に対する古典ゼロ知識証明は耐量子ゼロ知識でもあることを示した

WatrousのRewinding for 成功率≠1/2



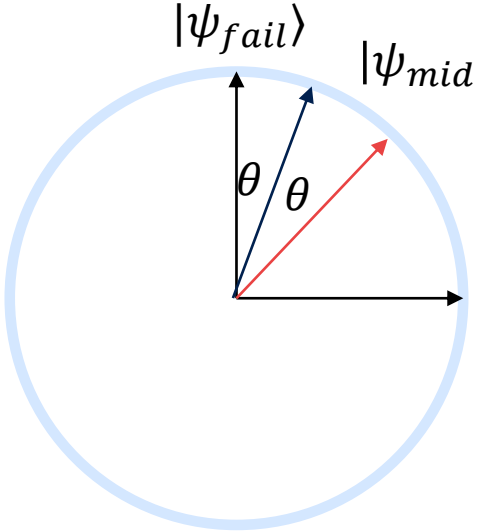
$|\psi_{mid}\rangle = cos\theta|\psi_{fail}\rangle + sin\theta|\psi_{suc}\rangle$

WatrousのRewinding for 成功率≠1/2



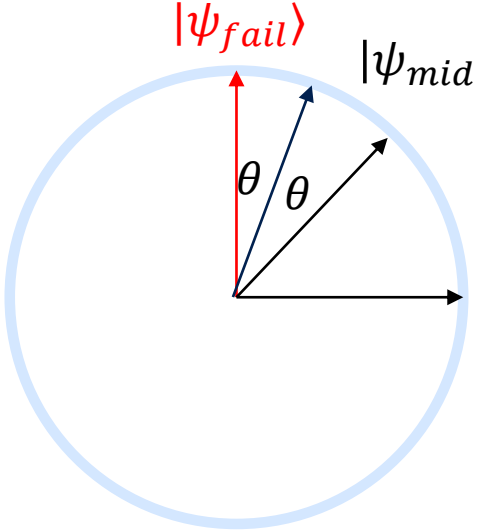
$$|\psi_{mid}\rangle = cos\theta|\psi_{fail}\rangle + sin\theta|\psi_{suc}\rangle$$

WatrousのRewinding for 成功率≠1/2



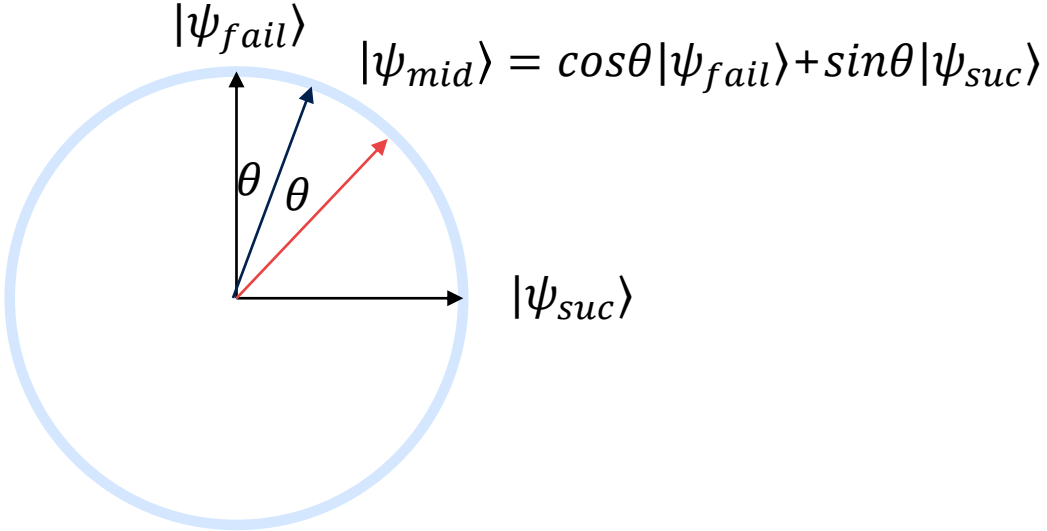
$$|\psi_{mid}\rangle = cos\theta|\psi_{fail}\rangle + sin\theta|\psi_{suc}\rangle$$

WatrousのRewinding for 成功率≠1/2



$$|\psi_{mid}\rangle = cos\theta|\psi_{fail}\rangle + sin\theta|\psi_{suc}\rangle$$

WatrousのRewinding for 成功率≠1/2



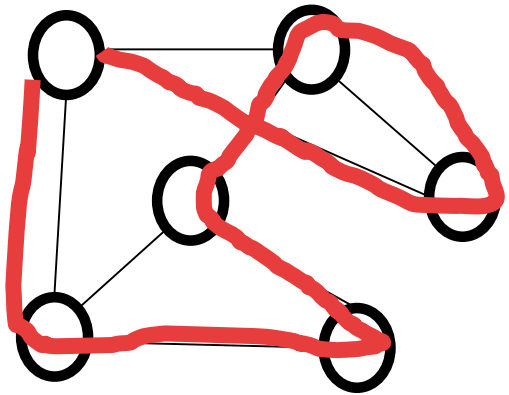
$|\psi_{suc}\rangle$へのprojectionが失敗して$|\psi_{fail}\rangle$にprojectionされてしまっても、
何回でも繰り返せる
→一回当たりの成功率が1/polyなら（期待値）poly回の繰り返しで成功
→log回のparallel repetitionバージョンならそのまま量子ゼロ知識が証明可能

目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

ハミルトニアン閉路問題

- 全ての頂点を一度ずつ通って元の頂点に戻る閉路は存在するか？



- NP完全問題であることが知られている

→ハミルトニアン閉路問題に対するゼロ知識証明が出来れば、
任意のNP言語に対するゼロ知識証明が出来たことになる！

（耐量子）コミットメント

- メッセージを秘匿したままメッセージを後から変えられないようにする暗号プロトコル

コミットフェイズ：
メッセージmへのコミットメントcomを生成
オープンフェイズ：
comの中身がmであるという証拠を生成

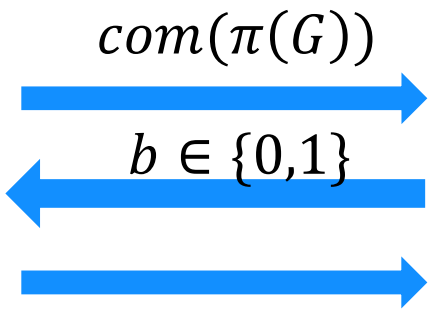
完全性：正しく実行すれば常に証拠を生成できる
完全拘束性：二通りのmに証拠が作成できるcomは存在しない
（耐量子）計算量的秘匿性：任意のm_0, m_1について、それらのコミットメントは（量子）多項式時間攻撃者に対して識別不能

- LWEを含む標準的仮定から耐量子コミットメントの構成が知られている
  - 例えば、IND-CPA安全な公開鍵暗号をそのまま使えば良い

ハミルトン閉路問題に対するゼロ知識証明[Blum86]

証明者P
入力:
$x = G$
$w =$ Gのハミルトン閉路

検証者V
入力: $x = G$



$b = 0$の時：comを$\pi(G)$にオープンし、
その証拠とπを送る

証拠とπの正当性をチェック

$b = 1$の時：comをハミルトン**閉路部分**だけ
オープンし、その証拠を送る

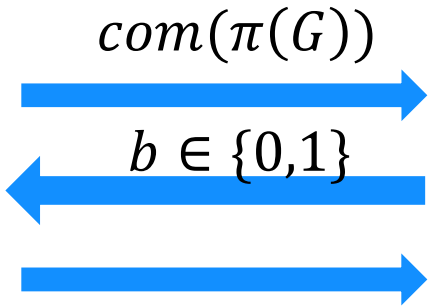
証拠の正当性をチェック

健全性:
Gがハミルトン閉路を持たないとき、$\pi(G)$もハミルトン閉路を持たない
更に、コミットメントの拘束性から、*com*の中身を*b=0*と*b=1*のときで変更できない
→*b=0*に答えられるなら、*b=1*には答えが存在しない
→検証の通れる確率高々*1/2*

ハミルトン閉路問題に対するゼロ知識証明[Blum86]

証明者P
入力:
$x = G$
$w =$ Gのハミルトン閉路

検証者V
入力: $x = G$



$b = 0$の時：comを$\pi(G)$にオープンし、
その証拠とπを送る

証拠とπの正当性をチェック

$b = 1$の時：comをハミルトン**閉路部分**だけ
オープンし、その証拠を送る

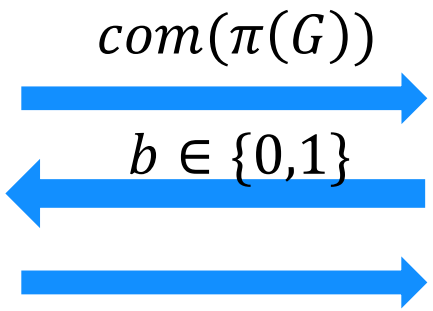
証拠の正当性をチェック

ゼロ知識性:
*b=0*の時、*G*のランダム置換を見るだけ、*b=1*の時ランダムな閉路を見るだけ
（それ以外の部分はコミットメントの秘匿性により隠されている）
→どちらも自分でシミュレーション出来る！

ハミルトン閉路問題に対するゼロ知識証明[Blum86]

証明者P
入力:
$x = G$
w = Gのハミルトン閉路

検証者V
入力: $x = G$



$b = 0$の時：comを$\pi(G)$にオープンし、その証拠とπを送る

証拠とπの正当性をチェック

$b = 1$の時：comを<u>ハミルトン**閉路部分**</u>だけオープンし、その証拠を送る

証拠の正当性をチェック

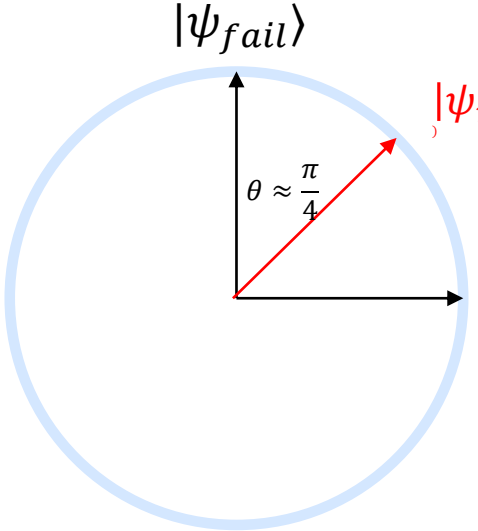
（古典）シミュレータ:

1. $b' \in \{0,1\}$をランダムに取る。b′ = 0 なら$com(\pi(G))$を送る。b'=1なら、ランダムな閉路のみからなるグラフHを取ってcom(H)を送る（Hに相当しない部分は全部0をコミットしておく）。
2. 検証者が$b \in \{0,1\}$を返す。***<u>$b \neq b'$ならステップ1に戻る</u>***。さもなくば次へ
3. b=0ならcomを$\pi(G)$にオープンし、その証拠とπを送る。 b=1ならHの部分だけオープンしてその証拠を送る。
4. 検証者の出力を出力する

耐量子ゼロ知識性

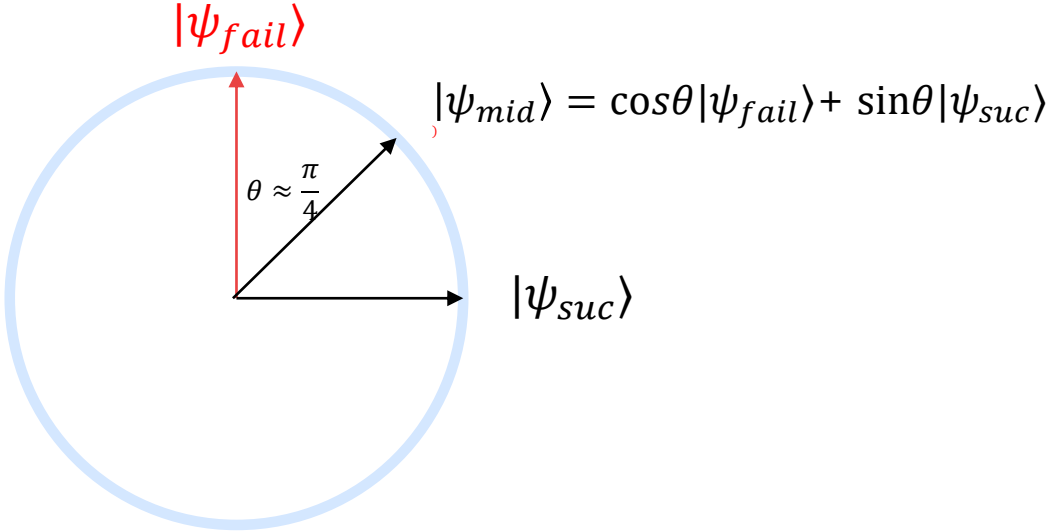
- グラフ同型問題の時と同様、単純には巻き戻し出来ない問題
- 今回もWatrousのテクニックで解決できる
- 違い：$b' = 0$の時と$b' = 1$の時のシミュレータの1メッセージ目の分布が完全に同一ではない
  →検証者の2メッセージ目の分布がそれぞれのケースで異なる可能性
  → 初期状態によらず$\Pr[b = b']$が一定とは言えない
- しかし、コミットメントの秘匿性より、その違いは**無視可能**であり、この場合にもWatrousの巻き戻し手法は拡張可能
- したがって耐量子ゼロ知識性が証明できる

Watrousのシミュレータ for Blum's protocol



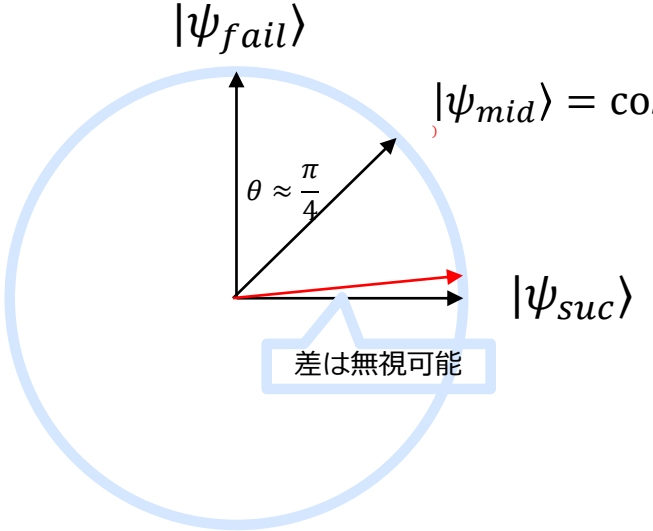
$|\psi_{mid}\rangle = \cos\theta|\psi_{fail}\rangle + \sin\theta|\psi_{suc}\rangle$

Watrousのシミュレータ for Blum's protocol



$$|\psi_{mid}\rangle = \cos\theta|\psi_{fail}\rangle + \sin\theta|\psi_{suc}\rangle$$

Watrousのシミュレータ for Blum's protocol



$$|\psi_{mid}\rangle = \cos\theta|\psi_{fail}\rangle + \sin\theta|\psi_{suc}\rangle$$

ここまでのまとめ

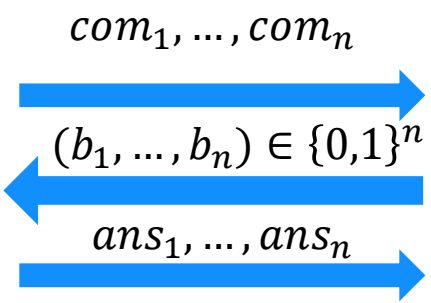
- グラフ同型問題に対する耐量子（情報理論的）ゼロ知識証明
- 任意のNP言語に対する耐量子（計算量的）ゼロ知識証明
  - 耐量子コミットメントを使う
- どちらも3ラウンド、健全性エラー1/2

  →直列にn回繰り返せば健全性エラー$\left(\frac{1}{2}\right)^n$に低減可能
- 何故並列に繰り返せないのか？
  →ゼロ知識性が保たれないため

ハミルトン閉路に対するゼロ知識証明の並列実行

証明者P
入力:
$x = G$
$w =$ Gのハミルトン閉路

検証者V
入力: $x = G$



ゼロ知識性の証明の肝：
「シミュレーターは検証者の2メッセージ目を予めランダムに予想し、当たるまで繰り返す」
並列実行版の場合当たる確率：$\frac{1}{2^n}$

指数的に小さいのでこのシミュレーションが上手くいかない！

注：**Honest Verifierゼロ知識性**は満たす。
VerifierがHonestな時$(b_1, \dots, b_n)$の分布はランダム→シミュレータが勝手に選べば良い

目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

定数ラウンドゼロ知識証明

- 単純な繰り返しで健全性エラーを指数的に低減するには、多項式回直列に繰り返さなければならない
  →多項式ラウンドプロトコルとなる
- 定数ラウンドで健全性エラーを指数的に低減出来るか？
- 古典の場合：YES [GK96] etc.
- 量子の場合：YES [BS20]
  - ただし健全性が計算量的安全性になってしまう
  - [GK96]とは全く異なるプロトコル

（古典）計算量的拘束・情報理論的秘匿コミットメント

コミットフェイズ：
メッセージmへのコミットメントcomを生成
オープンフェイズ：
comの中身がmであるという証拠を生成

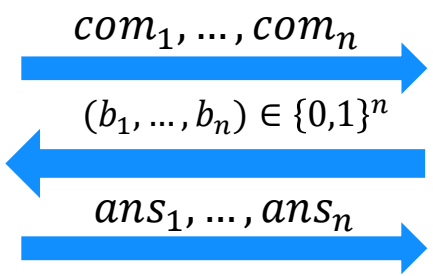
完全性：正しく実行すれば常に証拠を生成できる
（古典）計算量的拘束性：（古典）多項式時間アルゴリズムは一つのcomに
二通りのmへの証拠を作成できない
情報理論的秘匿性：任意のm_0, m_1について、それらのコミットメントは
任意の攻撃者に対して識別不能

- LWEを含む標準的仮定からこれらを満たすコミットメントの構成が知られている

定数ラウンド（古典）ゼロ知識証明[GK96]

証明者P
入力:
$x = G$
w = Gのハミルトン閉路

検証者V
入力: $x = G$



定数ラウンド（古典）ゼロ知識証明[GK96]

証明者P
入力:
$x = G$
w = Gのハミルトン閉路

検証者V
入力: $x = G$

情報理論的秘匿・計算量的拘束

$com(b_1), \dots, com(b_n)$

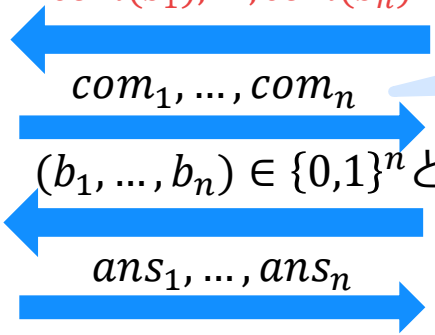
$com_1, \dots, com_n$

計算量的秘匿・完全拘束

$(b_1, \dots, b_n) \in \{0,1\}^n$とその証拠

もし証拠がinvalidなら
この時点でプロトコルを中断

$ans_1, \dots, ans_n$

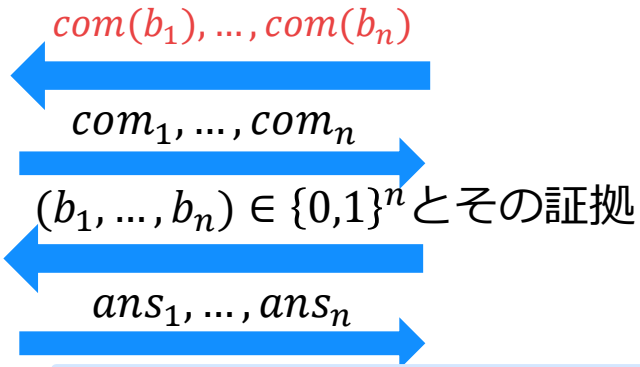


健全性：
コミットメントの情報理論的秘匿性より、証明者は1ラウンド目で、$(b_1, \dots, b_n)$の情報をほぼ何も得ていない
→元々のBlum's protocolのparallel版と同等のsoundness $\frac{1}{2^n}$を達成する

定数ラウンド（古典）ゼロ知識証明[GK96]

証明者P
入力:
$x = G$
$w =$ Gのハミルトン閉路

検証者V
入力: $x = G$



もし証拠がinvalidなら
この時点でプロトコルを中断

量子で出来るかは非自明！
Watrousの手法は使えない（rewindingなしで「成功率」1/polyな方法がないため）
→[GK96]プロトコルが耐量子ゼロ知識かは知られていない

古典ゼロ知識性：
シミュレーター（概略）

1. まず3ラウンド目まで走らせ
2. 2ラウンド目直前まで巻き戻す
3. $(b_1, \dots, b_n)$に答えられるように$com_1, \dots, com_n$を生成
4. コミットメントの計算量的理論的拘束性より、Vの3ラウンド目のメッセージは必ず$(b_1, \dots, b_n)$かまたはinvalid
   →シミュレーション可能

定数ラウンド耐量子ゼロ知識証明[BS20]

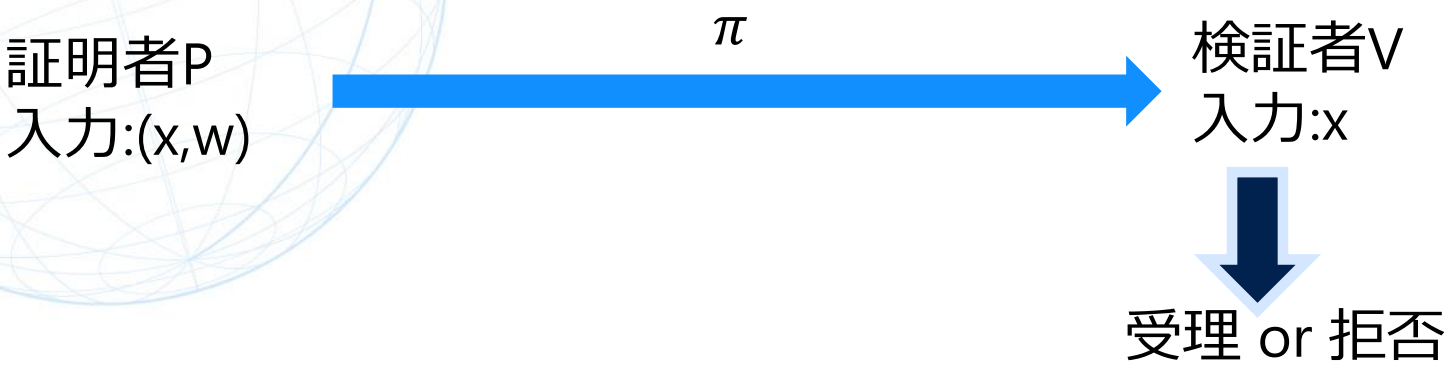
NTT

- [GK96]プロトコルが耐量子ゼロ知識かは知られていない
  - WatrousのRewindingが使えないため
- 最近定数ラウンド耐量子ゼロ知識証明が提案された[BS20]
  - Rewindingは上手くいかないので、Rewindingを避けたい
    →Non-Black-Boxシミュレーション[Barak01,BKP19 etc.]
- シミュレータはNo instanceに対してもvalidなtranscriptを生成
  →実際の証明者にはない何らかの能力が必要
  - Rewinding: 検証者を巻き戻す（耐量子では使用が限定的）
  - Non-Black-Box Simulation:**検証者の回路としての記述を知っている**
    ことを使用して証明者には出来ないことをする
- [BS20]のアイディア：検証者の出力した量子完全準同型暗号の暗号文に対して、**検証者自身を記述する量子回路**で準同型演算する
  →検証者のコミットしたチャレンジが得られる
  - 詳細は[BS20]参照

目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

非対話ゼロ知識証明[BFM88]



- セットアップなしの非対話ゼロ知識証明は自明な言語にしか存在しない

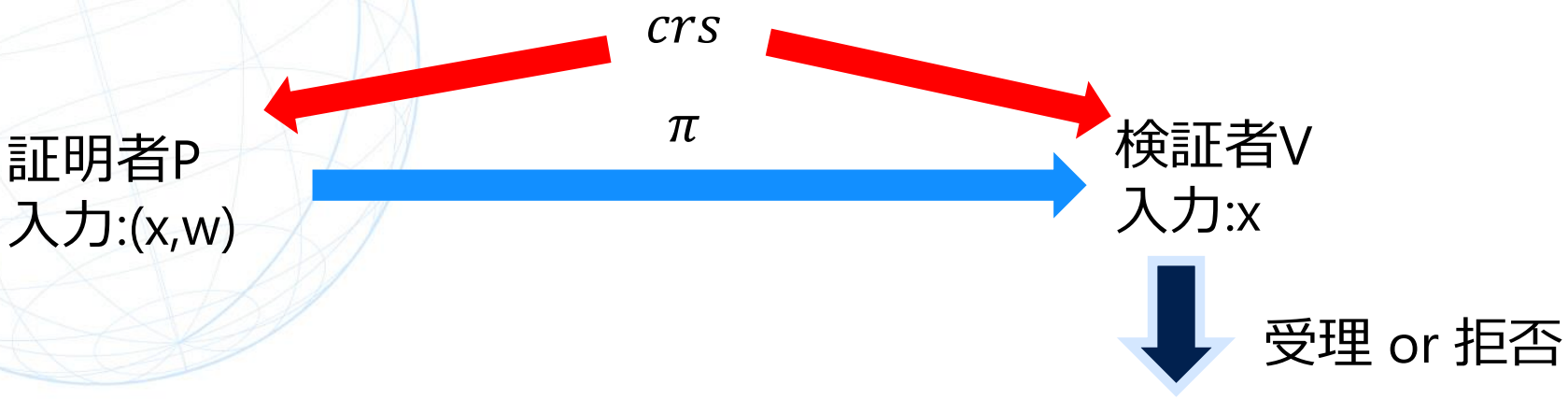
∵ xが与えられた時、シミュレータを使ってxに対する証明πを生成

$x \in L$の時：ゼロ知識性よりVはπを受理

$x \notin L$の時：健全性よりVはπを拒否

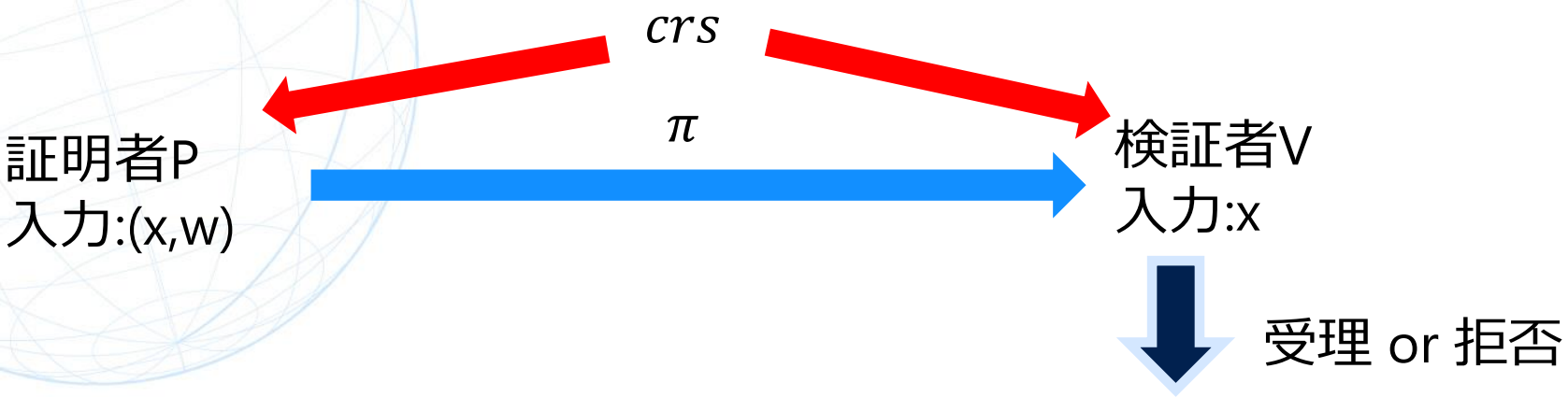
→$x \in L$か$x \notin L$か効率的に判定できる

非対話ゼロ知識証明[BFM88]



- セットアップとしてtrusted partyがcommon reference string (crs)を生成するモデルを考える
- 完全性：$x \in L$ の時正しく実行すれば（無視可能な確率を除いて）受理
- （計算量的）健全性：$x \notin L$の時Pが量子多項式時間なら受理確率は無視可能
- （計算量的）ゼロ知識性：$x \in L$ でPが正直に動くとき、Vはどんなずるをしても「$x \in L$ である」という以上の"知識"を得られない

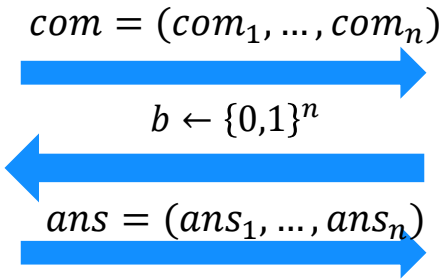
非対話ゼロ知識証明[BFM88]



- セットアップとしてtrusted partyがcommon reference string (crs)を生成するモデルを考える
- 完全性： $x \in L$ の時正しく実行すれば（無視可能な確率を除いて）受理
- （計算量的）健全性： $x \notin L$の時Pが量子多項式時間なら受理確率は無視可能
- （計算量的）ゼロ知識性：あるシミュレータSが存在して、xだけを入力にとって(crs, π)の分布と計算量的識別不能なものをシミュレート出来る:

$$\{(crs,\pi): crs \leftarrow Setup, \pi \leftarrow Prove(crs,(x,w))\} \approx_{comp} \{(crs,\pi) \leftarrow S(x)\}$$

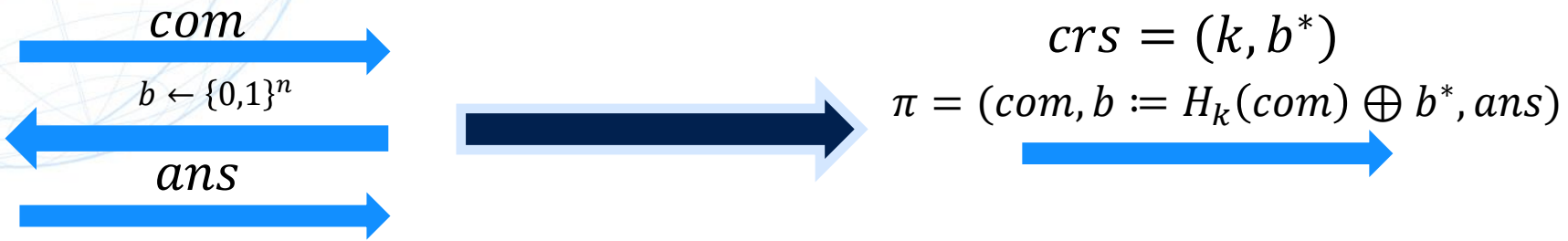
Fiat-Shamir変換[FS86]



- 証明者が自分でbを選ぶことにすれば非対話プロトコルになる
- しかしそれだと健全性が崩れる
  - bを先に決めたらそれに答えられるようなcomが作れるため
- アイディア：ハッシュ関数Hを使って$b := H(com)$とする
- 直感：comを決めると自動的にbが決まる
  →bを決めてからcomを作る攻撃が出来ない

Fiat-Shamir変換[FS86]

- **Honest Verifierゼロ知識性**を持つ3ラウンド**Public Coin**プロトコルから非対話ゼロ知識証明へのハッシュ関数を使った変換
- H_kを$k \in K$でインデックス付けされたcom空間から$\{0,1\}^n$への
ハッシュ関数とする

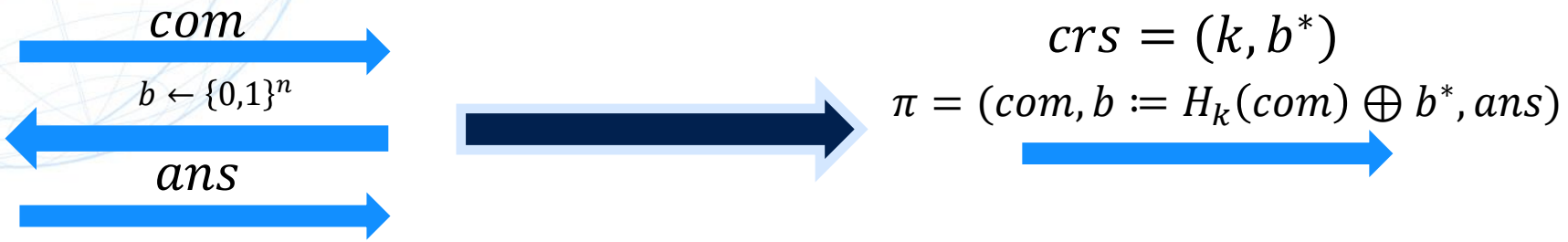


- 元々の3ラウンドプロトコルがHonest Verifierゼロ知識
→変換後の非対話方式はゼロ知識
∵Sはまず3ラウンドプロトコルのシミュレータを使って(com, b, ans)
をシミュレートし、その後$b=H_k(com) \oplus b^*$となるようにb^*を設定
→bもb^*もランダムなので取る順を逆にしても分布不変

Fiat-Shamir変換[FS86]

NTT

- **Honest Verifierゼロ知識性**を持つ3ラウンド**Public Coin**プロトコルから非対話ゼロ知識証明へのハッシュ関数を使った変換
- H_kを$k \in K$でインデックス付けされたcom空間から$\{0,1\}^n$へのハッシュ関数とする



- 健全性は保たれるか？
- 元方式が計算量的健全性しか満たさないとき:
  - ある元方式が存在して、どんなH_kを使っても変換後の方式は健全性を満たさない[GK03]
  - H_kを（量子）ランダムオラクルとすると健全性証明可能。古典：[PS96] 量子: [DFMS19,LZ19
- 元の方式が情報理論的健全性を満たすとき:
  Hが**Correlation Intractable Hash (CIH)**ならば変換後の健全性が証明可能

Correlation Intractable Hash[CGH98]

- ハッシュ関数族$\{H_k : X \to Y\}_{k \in K}$が（耐量子）CIHであるとは、任意のRelation $R \subseteq X \times Y$について、もしRがsparse、すなわち

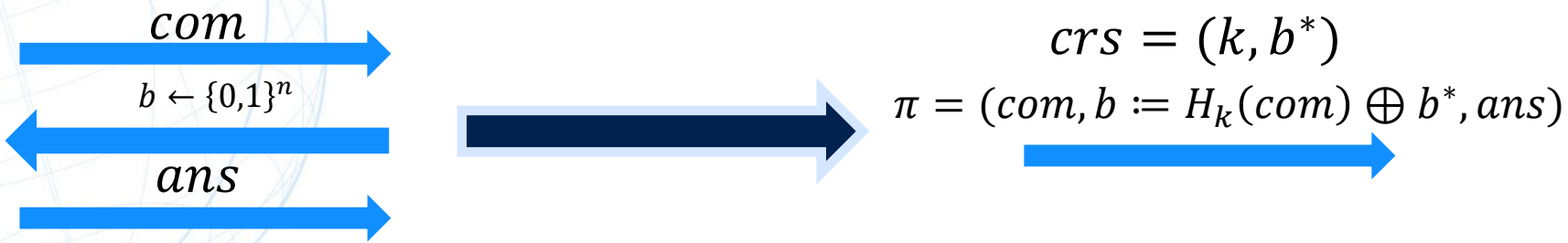
  「任意の$x \in X$に対して $\Pr_{y \leftarrow Y}[(x, y) \in R]$が無視可能」

  ならば、任意の（量子）多項式時間アルゴリズムAに対して、

  $$\Pr_{k \leftarrow K, x \leftarrow A(k)}[(x, H_k(x)) \in R]$$は無視可能。

- "（量子）ランダムオラクルはCIHである"
  - 古典の場合：仮定からどのxについても$\Pr(x, H(x)) \in R$は無視可能
    →各クエリに対して答えが見つけられる確率は無視可能
    →多項式回のクエリで答えが見つけられる確率は無視可能
  - 量子の場合：One-Way-to-Hidingの証明と同様のhybrid argumentを行う

Fiat-Shamir変換 from CIH



- $COM \times \{0,1\}^n$上のRelation Rを以下のように定義（COMはcomの属する集合）

$$(com, b') \in R \Leftrightarrow \exists\, ans\ s.t.\ (com, b' \oplus b^*, ans)\text{は検証に通る}$$

- 情報理論的健全性が成り立つ時、 $x \notin L$の時、任意のcomに対して

$$\Pr_{b' \leftarrow \{0,1\}^n}[\exists\, ans\ s.t.\ (com, b' \oplus b^*, ans)\text{は検証に通る}] = \text{無視可能}$$

- CIHの安全性より、

$$\Pr_{k \leftarrow K, com \leftarrow A(k)}[\exists\, ans\ s.t.\ (com, H_k(com) \oplus b^*, ans)\text{は検証に通る}] = \text{無視可能}$$

CIHの構成

- 先述の定義を満たすCIHの標準的仮定からの構成は知られていない
- Relation Rをsearchableなものに限定した場合LWE仮定からの構成が存在 [PS19]
  - $R \subseteq X \times Y$がsearcheableとは、ある多項式時間計算可能なfが存在して、

$$(x, y) \in R \Rightarrow y = f(x)$$

- Fiat-Shamir変換前のプロトコルを工夫すればCIH for searcheable relationsで十分
  - アイディア：コミットメントを公開鍵暗号で実装しておくと、 $x \notin L$の時、各comに対して”bad challenge”(=validなansが存在するb)が復号アルゴリズムを使うことで多項式時間で計算可能（詳細は[CCH+19,PS19]等参照）
- LWE→CIH for searchable relations→非対話ゼロ知識証明 for all NP言語
- 以下では簡単のため、LWEよりもやや強い仮定である**Circular Secure FHE**に基づく構成を紹介[CCH+19]

CIH from FHEのアイディア

NTT

- CIH for searcheable relationsとは、ハッシュ関数族$\{H_k\}$で任意の（bounded）多項式時間で計算可能なfに対してkが与えられた時
$$H_k(x) = f(x)$$
となるxを見つけるのは困難というものであった。
- もし、H_kが特定のfに依存して良いとすれば自明に達成可能
  - $H_k(x) := f(x) \oplus 1$とすればよい
- 単一のH_kで全てのfに対応しなければならないのが難しい
- アイディア：**完全準同型暗号**を使って"fの暗号文"を公開し、"$H_k(x) := f(x) \oplus 1$"を"暗号化されたまま"行う
  - 完全準同型暗号の安全性から、"fの暗号文"と"f'の暗号文"は見分けつかない

→すべてのfに対して同時に示したい性質を満たしている

完全準同型暗号（FHE）

- FHEは以下のアルゴリズムからなる

KeyGen()→(PK,SK)
Enc(PK,M)→C
Dec(SK,C)→M
Eval(PK,f,C)→f(M)

- 準同型性：Dec(SK, Eval(PK,f,Enc(PK,M)))=f(M)
- IND-CPA安全性:$(\mathrm{PK}, \mathrm{Enc}(\mathrm{PK}, \mathrm{M}_0)) \approx (\mathrm{PK}, \mathrm{Enc}(\mathrm{PK}, \mathrm{M}_1))$
- Circular安全性：”秘密鍵を暗号化しても安全”

$$(\mathrm{PK}, \mathrm{Enc}(\mathrm{PK}, \mathrm{SK})) \approx (\mathrm{PK}, \mathrm{Enc}(\mathrm{PK}, 0^{|\mathrm{SK}|}))$$

  - 準同型性と組み合わせると次が言える：任意のf (with output length L)に対して

$$(\mathrm{PK}, \mathrm{Enc}(\mathrm{PK}, \mathrm{f}(\mathrm{SK}))) \approx (\mathrm{PK}, \mathrm{Enc}(\mathrm{PK}, 0^{\mathrm{L}}))$$

- IND-CPA安全な(leveled) FHEはLWEからの構成が知られている [GSW13 etc]
- それらの構成はCircular安全性も満たすと信じられている

CIH for Searchable Relations from Circular Secure FHE

- $k := (pk, ct)$ ただし、$\mathrm{C} = Enc(pk, 0^L)$
- $H_k(x) := Eval(pk, U_x, ct)$
  ただし、U_x はユニバーサル回路、つまり i.e., $U_x(g) = g(x)$
- 証明したい事：任意の効率的計算可能なfに対して、
  $$\Pr[H_k(x) = f(x) : x \leftarrow A(k)] = \text{無視可能}$$
- 証明ステップ1：$C = Enc(pk, g_{sk})$に置き換える。ここで、
  $$g_{sk}(x) := Dec\big(sk, f(x)\big) \oplus 1$$
  - Circular securityより、こうしても攻撃者の成功確率の変化は無視可能
- $H_k(x) = Eval(pk, U_x, C = Enc(pk, g_{sk}))$
  $= Enc\big(pk, g_{sk}(x)\big) = Enc(pk, Dec\big(sk, f(x)\big) \oplus 1)$

$\rightarrow Dec\big(sk, H_k(x)\big) = Dec\big(sk, f(x)\big) \oplus 1$

$\rightarrow$ **$H_k(x) = f(x)$にはなりえない**

目次

- イントロダクション
- グラフ同型問題に対するゼロ知識証明
- NP完全問題（ハミルトニアン閉路問題）に対するゼロ知識証明
- 定数ラウンドゼロ知識証明
- 非対話ゼロ知識証明
- IND-CCA公開鍵暗号への応用

復習：公開鍵暗号

- 公開鍵暗号は以下のアルゴリズムからなる

KeyGen()→(PK,SK)

Enc(PK,M)→C

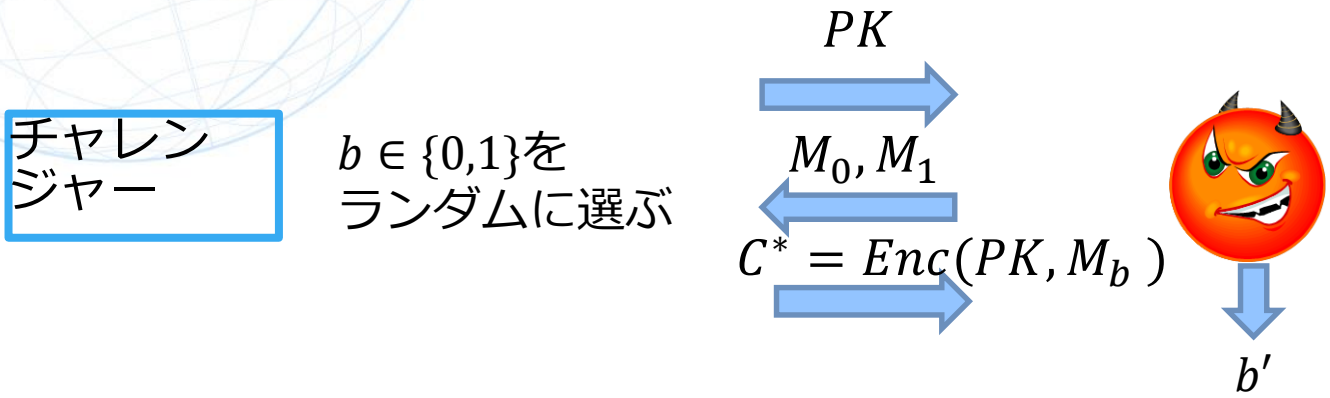
Dec(SK,C)→M

- 正当性：”暗号化して復号したらもとに戻る”

$$Dec(SK, Enc(PK,M))=M$$

復習：IND-CPA安全性

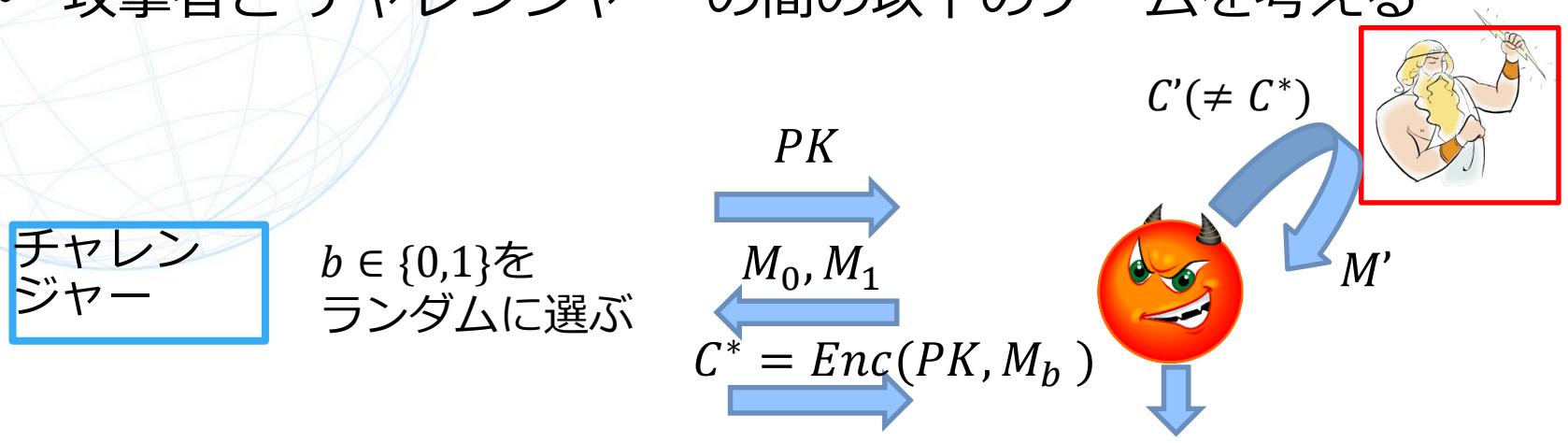
- 「攻撃者がMの情報を一切得られない」ことの数学的定義がIND-CPA安全性（選択平文攻撃に対する識別不可能性）
- 攻撃者と"チャレンジャー"の間の以下のゲームを考える



- 任意の（量子）多項式時間攻撃者に対して$|\Pr[b = b'] - 1/2|$が**無視可能**な時、公開鍵暗号方式は（耐量子）IND-CPA安全と言う。

復習：IND-CCA安全性

- 選択暗号文攻撃に対する識別不可能性）
- 攻撃者と"チャレンジャー"の間の以下のゲームを考える



- 任意の（量子）多項式時間攻撃者に対して$|\Pr[b = b'] - 1/2|$が**無視可能**な時、公開鍵暗号方式は（耐量子）IND-CCA安全と言う。
  - 復号オラクルがC^*を得る前に限定されている時IND-CCA1安全といい、これと区別するために、IND-CCA安全のことをIND-CCA2安全ともいう。

IND-CPA→IND-CCA変換

- IND-CPA→IND-CCA安全への（量子）ランダムオラクルを用いた一般的変換として藤崎岡本変換がある（昨日紹介した）
- ランダムオラクルも追加の仮定も一切使用しない一般的変換は未だ知られていない
- NaorとYung[NY90]は追加で非対話ゼロ知識証明を仮定すればIND-CPA→IND-CCA1安全への一般的変換が出来ることを示した

Naor-Yung変換

- (CPA.Gen,CPA.Enc,CPA.Dec)をIND-CPA安全な公開鍵暗号方式として、IND-CCA1安全な公開鍵暗号方式を以下のようにして構成

CCA.KeyGen(): CPA.Genを二回走らせて$\{(PK_b, SK_b)\}_{b\in\{0,1\}}$を生成、
$PK := (PK_0, PK_1), SK := (SK_0, SK_1)$を出力

CCA.Enc(PK,M): $C_0 \leftarrow$ CCA.Enc(PK_0,M), $C_1 \leftarrow$ CCA.Enc(PK_1,M),
“C_0とC_1が同じ平文の暗号化”であることの非対話ゼロ知識証明πを
生成し、暗号文$C := (C_0, C_1, \pi)$を出力

CCA.Dec(SK,C): もしπが正しい証明でなければエラーを返す。さもなくば、
$M \leftarrow$ CCA.Enc(SK_0, C_0) を出力

- 直感：検証に通るπを作るには、Mを知りながら正しく(C_0, C_1)を作るしかなさそう→復号オラクルの無意味化

Naor-Yung変換のIND-CCA1安全性証明

NTT

- 攻撃者は$C^* := (C_0^* = CPA.Enc(PK_0, M_0), C_1^* = CPA.Enc(PK_1, M_0), \pi^*)$と復号オラクルが与えられているとする
  - 目標はM_0をM_1に取り換えること

上記ゲームに以下のような変形を順に施していく

1. π^*を正直に作る代わりにシミュレータで作る　ゼロ知識性
2. $C_1^* = CPA.Enc(PK_1, M_1)$とする　IND-CPA
3. 復号オラクルはC_0側ではなくC_1側を復号する　健全性
4. $C_1^* = CPA.Enc(PK_1, M_1)$とする　IND-CPA
5. π^*を正直に作る　ゼロ知識性

- この時点で攻撃者はM_1の暗号文を与えられたのと同じこと

→攻撃者は復号オラクルを与えられてもM_0の暗号文とM_1の暗号文を識別出来ない

IND-CCA2達成のために

- 非対話ゼロ知識証明の健全性はシミュレータが生成した証明を見たあとには保証されない
  - シミュレータの生成した偽証明を微妙に変形して新たな偽証明を作れる可能性がある
- このような攻撃を防ぐためには(ワンタイム)シミュレーション健全性と呼ばれる安全性を満たすことが必要
  - 一つシミュレータが作った偽証明を見ても新たな偽証明を作れない
  - 任意の非対話ゼロ知識証明とワンタイム署名を組み合わせて(ワンタイム)シミュレーション健全性を満たすように出来る[Lindell03]
- (ワンタイム)シミュレーション健全性を持つ非対話ゼロ知識証明を使うことでIND-CCA2安全性が達成できる

まとめ

- ゼロ知識証明とは追加の知識を一切与えずに何かを証明すること
- ゼロ知識性の証明の典型的手法は巻き戻し(rewinding)
  - 耐量子性を考えると巻き戻しはそのままでは上手くいかない
  - Watrousは特定の場合には上手くいくことを示した
- 信頼されたcrsを導入することで非対話ゼロ知識証明が構成できる
- 3ラウンド方式を非対話化する方法としてFiat-Shamir変換を紹介した
  - Correlation Intractable Hashを使って実現可能
  - Correlation Intractable HashはLWE仮定から構成可能（ただし今日はより強い仮定であるCircular安全FHEを用いた構成を紹介した）
- 非対話ゼロ知識証明の応用としてNaor-Yung変換と呼ばれるIND-CCA安全な公開鍵暗号の構成を紹介した

参考文献

- [GMR89]: Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. SIAM J. Comput.,
- [Babai16]:László Babai, Graph Isomorphism in Quasipolynomial Time. STOC16
- [GMW91]:O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. Journal of the ACM
- [Watrous09]:John Watrous. Zero-knowledge against quantum attacks.SIAM J. Comput
- [Blum86]:Manuel Blum. How to prove a theorem so no one else can claim it. InProceedings ofthe International Congress of Mathematicians
- [GK96]:Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledgeproof systems for NP.
- [BS20]:Nir Bitansky and Omri Shmueli. Post-quantum zero knowledge in constant rounds. STOC20
- [Barak01]: Boaz Barak. How to go beyond the black-box simulation barrier FOCS01
- [BKP19]: Nir Bitansky, Dakshita Khurana, and Omer Paneth. Weak zero-knowledge beyond the black-box barrier STOC19
- [BFM88]:Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). STOC88
- [FS86]:Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. CRYPTO86
- [GK03]:Shafi Goldwasser and Yael Tauman Kalai, On the (in) security of the Fiat-Shamir paradigm,FOCS03
- [PS96]:David Pointcheval and Jacques Stern. Provably secure blind signature schemes.Asiacrypt96
- [DFMS19]: Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model CRYPTO19
- [LZ19]:Qipeng Liu and Mark Zhandry. Revisiting post-quantum fiat-shamir CRYPTO19
- [CGH98]:Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited STOC 98
- [PS19]:Chris Peikert and Sina Shiehian, Noninteractive zero knowledge for np from (plain) learning with errors CRYPTO19
- [CCH+19]:Fiat-Shamir: from practice to theory. STOC 2019
- [GSW13]:Craig Gentry and Amit Sahai and Brent Waters, Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, CRYPTO 13
- [NY90]:Moni Naor, Moti Yung, Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks STOC90