# 耐量子暗号について(2)：量子解析と耐量子鍵共有


## 富士通株式会社　データ&セキュリティ研究所

### 福岡 尊


純粋数学者のためのデータサイエンス入門2025@名古屋大学
2025/3/23（日）

# 昨日のおさらい

- 鍵共有（i.e.秘密の共有）：暗号を使う上で大事なプロセス
- 有限体Diffie-Hellman・楕円曲線Diffie-Hellman.
- これらが安全であるには，以下の問題が安全でないといけない：

$G$をアーベル群，$0 \neq g \in G$を位数$n$の元とする.

$$\mathrm{DE}_g \colon \mathbb{Z}/n\mathbb{Z} \ni a \mapsto g^a \in G$$

の像を$\langle g \rangle$，逆写像を$\mathrm{DL}_g \colon \langle g \rangle \to \mathbb{Z}/n\mathbb{Z}$とする.
このとき，$h \in \langle g \rangle$について，$\mathrm{DL}_g(h)$を計算せよ.

- しかし上は量子アルゴリズムで解くことができてしまう！
- 今日：どう上の問題が解かれるか．そして量子計算機でも解けないと思われているDiffie-Hellmanを紹介.

# 参考：Table Of Contents (Day 1)

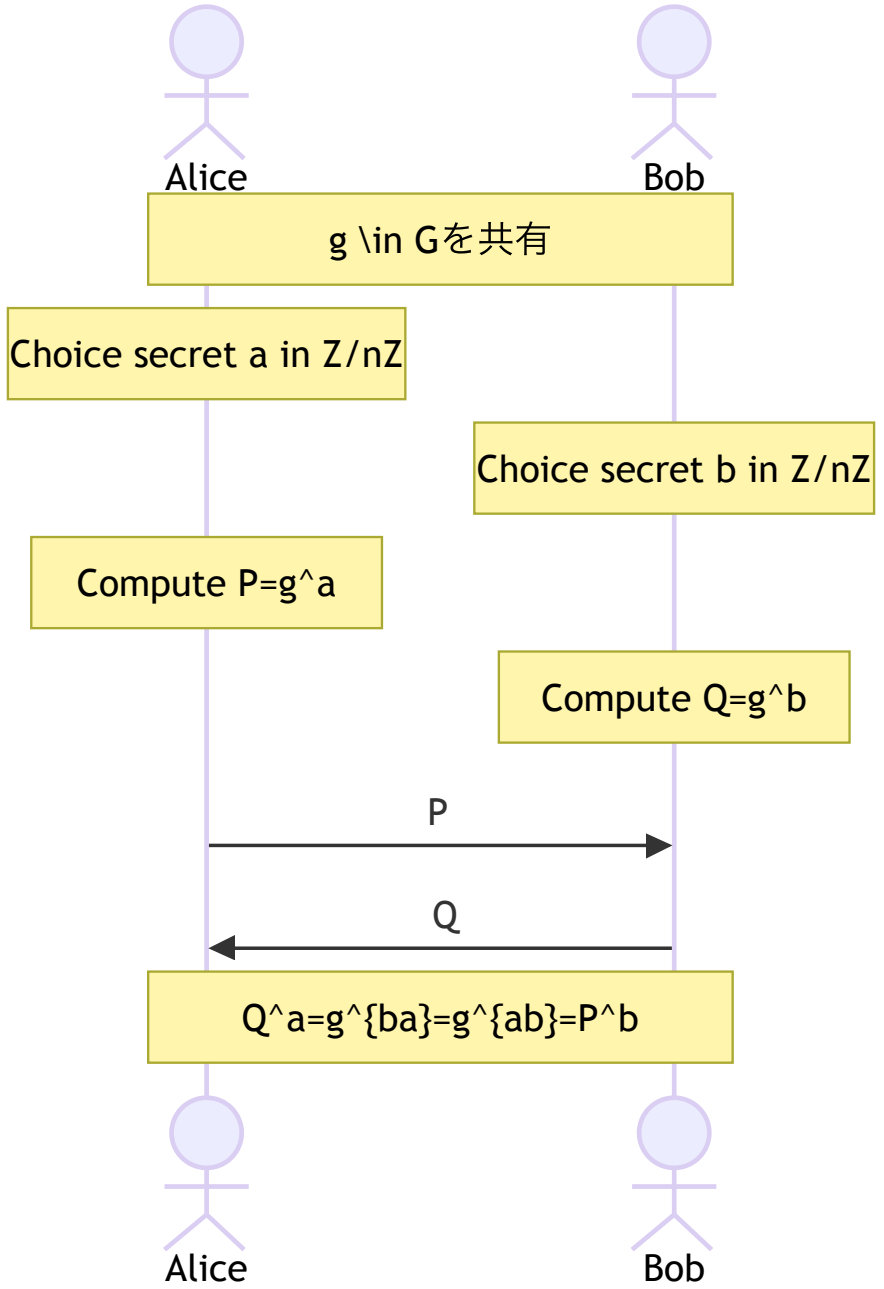
# Table Of Contents (Day 2)

# 3. 量子暗号解読とは

# アーベル群Diffie-Hellman (AbDH)

- $G$：アーベル群.
- $g \in G$：位数$n$.

- Alice：秘密$a \in \mathbb{Z}/n$, $P = g^a$を公開, $R = Q^a$を共有
- Bob：秘密$b \in \mathbb{Z}/n$, $Q = g^b$を公開, $R = P^b$を共有
- $Q^a = g^{ba} = g^{ab} = P^b$



# 復習：AbDHの困難性

**アーベル群離散対数問題**

$G$をアーベル群，$0 \neq g \in G$を位数$n$の元とする．

$$\mathrm{DE}_g \colon \mathbb{Z}/n\mathbb{Z} \ni a \mapsto g^a \in G$$

の像を$\langle g \rangle$，逆写像を$\mathrm{DL}_g \colon \langle g \rangle \to \mathbb{Z}/n\mathbb{Z}$とする．
このとき，$h \in \langle g \rangle$について，$\mathrm{DL}_g(h)$を計算せよ．

- $G = \mathbb{F}_p^\times$の場合が有限体Diffie-Hellman
- $G$が有限体上の楕円曲線の有理点の場合が楕円曲線Diffie-Hellman

# 離散対数問題の求解アプローチ

- $g, h \in G$とする.
- $s \in \mathbb{Z}$で$h = g^s$なるものを求めたい.
- 以下の群準同型を考える：

$$f\colon (\mathbb{Z}/n\mathbb{Z})^2 \ni (a, b) \mapsto g^a h^b \in G.$$

- $f$は準同型写像で，核は$(s, -1)$で生成される：

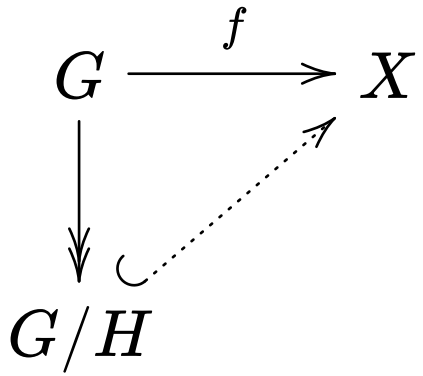
$$\mathrm{Ker}(f) = (\mathbb{Z}/n\mathbb{Z}) \cdot (s, -1) = \{(ks, -k) \mid k \in \mathbb{Z}/n\mathbb{Z}\}$$

→実質的に，準同型写像の核を計算する問題に入れ替わる

# Hidden Subgroup Problem

**Definition.** $G$をアーベル群，$f\colon G \to X$を写像，$H < G$を部分群とする．

$f$が$H$を**隠す**とは，以下を可換にする単射$G/H \to X$が存在することを言う：




（$f$が群準同型なら$H = \mathrm{Ker}(f)$と同値）

**Hidden Subgroup Problem（HSP，隠れ部分群問題）**

$G$を有限アーベル群，$X$を有限集合，$f\colon G \to X$を写像とする．このとき，$f$で隠された部分群$H$の生成元を求めよ．

# 簡単に解けるケース

- $G = \bigoplus_{i=1}^{k} (\mathbb{Z}/m_i\mathbb{Z})$とする.
- $X = \bigoplus_{j=1}^{l} (\mathbb{Z}/n_j\mathbb{Z})$であり，$f\colon G \to X$が行列で与えられているなら：

$$f = (f_{ij}) \in \bigoplus_{i,j} \mathrm{Hom}(\mathbb{Z}/m_i, \mathbb{Z}/n_j) \simeq \bigoplus_{i,j} \mathbb{Z}/\gcd(m_i, n_j)$$

- $g = (g_i) \in G$について

$$g \in \mathrm{Ker}(f) \iff \sum_i a_{ij} g_i \equiv 0 \pmod{n_j}$$

- →掃き出し法（計算時間はだいたい$O(k^3) \approx O(\mathrm{poly}(\log |G|))$）
- しかし$f$の表現行列がわからないときは非自明．総当たりは$O(|G|)$時間かかる.
  - $X = \mathbb{F}_p^{\times}$，$X = E[n](\mathbb{F}_p)$など

# 隠れ部分群問題の量子解析

- 現代社会を支えるDiffie-Hellmanプロトコルは，群準同型の核を具体的に計算できれば破れる.
- しかし，今まで実際に破られてはいない.
- その一方，**量子計算機**というアイデアが物理学から生まれた（量子系を用いた計算プロセス）
- **量子アルゴリズム**：量子計算機でできるアルゴリズム

**Theorem** [EHK04]. $G = \bigoplus_{j=1}^{l} (\mathbb{Z}/t_j\mathbb{Z})$とする．任意の有限集合への写像$f\colon G \to X$に対し，ある量子アルゴリズムで，時間計算量$O(\log |G|)$で，非常に高い確率で，隠れ部分群問題を解くものがある.

# そもそも量子計算機ってなに？

## 古典計算機

- 古典回路で$\{0,1\}^n$の元（ビット列）から$\{0,1\}^m$の元（ビット列）を計算.
- 古典回路はAND素子，OR素子，NOT素子を組み合わせて作られる.
- （任意の関数$\{0,1\}^n \to \{0,1\}^m$は$O(m2^n)$以下の素子数で実現できる）

## 量子計算機

- 量子回路により，$(\mathbb{C}^2)^{\otimes n}$から$(\mathbb{C}^2)^{\otimes n}$の元を計算.
- 量子回路はいくつかのユニタリ変換を組み合わせて作られる（よって可逆）.
- （任意のユニタリ変換$(\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$は，$O(n^2 2^{2n})$以下の$2 \times 2$のユニタリ行列とCNOT素子で実現できる）.

# 古典回路におけるビット列 vs 量子ビット

- 古典回路：長さ$n$のビット列$\vec{b} = (b_1 \dots b_n)$を取り扱う.
- 量子回路：ビット列は$(\mathbb{C}^2)^{\otimes n}$の基底に対応.
- $\mathbb{C}^2$の基底を$e_0, e_1$とする.
- ビット列$b = (b_1 \dots b_n)$に対応する基底は$e_{b_1} \otimes \cdots \otimes e_{b_n}$.
- この基底のことを$|b_1 \cdots b_n\rangle$と書く. **計算基底状態**と呼ぶ.
- Notation: 長さ$n$の計算基底状態$|b_1 \cdots b_n\rangle$を$|\sum_i 2^i b_i\rangle$で表す.
  - 例（$n = 5$）：$|3\rangle = |00011\rangle$, $|28\rangle = |11100\rangle$.

**Definition (量子ビット).** $n$量子ビットとは以下で表せる$(\mathbb{C}^2)^{\otimes m}$の元：

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \text{ with } \sum_j |x_j|^2 = 1. \quad (\text{"Probability of } j\text{"} = |x_j|^2)$$

# ユニタリ変換の例(1)：古典回路の量子回路化

**Definition.** $f\colon \{0,1\}^n \to \{0,1\}^m$について，ユニタリ変換$U_f$が$f$に付随するとは以下：

$$U_f\colon (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes m} \ni |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle \in (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes m}.$$

**Remark.** $f$の論理回路がわかっているなら，$(\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes k}$におけるユニタリ変換で

$$|x\rangle|0\rangle|z\rangle \mapsto |x\rangle|f(x)\rangle|G(z)\rangle$$

を満たすものが作れることが知られている．ここで残っている補助ビット$|z\rangle$はゴミ情報と呼ばれる．

# ユニタリ変換の例(2)：重ね合わせ

- $I \subset \{0, \ldots, N-1\}$を部分集合とする.
- $\mathbb{C}^N$の正規直行基底$U_I = (u_1, \ldots, u_N)$で，$u_1 = \frac{1}{\sqrt{\#I}} \sum_{j \in I} e_j$なるものを取る（グラム・シュミット）.
- この$U_I \colon \mathbb{C}^N \to \mathbb{C}^N$は以下を満たす.

$$U \colon |0\rangle \mapsto \frac{1}{\sqrt{\#I}} \sum_{j \in I} |j\rangle$$

- つまり，$I$に属する部分のみを平均的に重ね合わせた状態を作ることができる.
- $I = \{0,1\}^N, N = 2^n$であるときは，Hadamard変換というものが上記を満たすものとして知られている．とても大事だが今回は省略.

# ユニタリ変換の例(3)：量子フーリエ（逆）変換

**Definition.** 以下で決まる変換$\mathbb{C}^N \to \mathbb{C}^N$をQFTと呼ぶ：

$$\mathrm{QFT}: \sum_{j=0}^{N-1} x_j |j\rangle \mapsto \sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i kj/N} |k\rangle.$$

これはユニタリ変換である：

$$\begin{aligned}\langle \sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i kj/N} |k\rangle, \sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} y_j e^{2\pi i kj/N} |k\rangle \rangle &= \frac{1}{N} \sum_k \left( \sum_j x_j e^{2\pi i kj/N} \right) \left( \sum_l \overline{y_l} e^{-2\pi i kl/N} \right) \\ &= \frac{1}{N} \sum_k \left( \sum_{j,l} x_j \overline{y_l} e^{2\pi i k(j-l)/N} \right) \\ &= \sum_j x_j \overline{y_j} = \langle \sum_j x_j |j\rangle, \sum_j y_j |j\rangle \rangle.\end{aligned}$$

# 有限アーベル群とQFT

- $G$：有限アーベル群，$\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$.
- $\mathbb{C}^G$：$\{|g\rangle \mid g \in G\}$を基底とする$\mathbb{C}$-線形空間.
- $G = \mathbb{Z}/N\mathbb{Z}$であれば，
  - $\hat{G} = \{\chi_k \mid 0 \leq k < N\}$ where $\chi_k \colon \mathbb{Z}/n\mathbb{Z} \ni j \mapsto e^{2\pi i k j/n} \in S^1$.
  - $\mathrm{QFT}(|j\rangle) = \sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} \chi_k(j)|k\rangle$.

一般の有限アーベル群$G$についても，$\mathrm{QFT} \colon \mathbb{C}^G \to \mathbb{C}^{\hat{G}}$が決まる：

$$|g\rangle \mapsto \frac{1}{\sqrt{\#G}} \sum_{\chi \in \hat{G}} \chi(g)|\chi\rangle$$

- $\mathbb{C}^G \ni |g\rangle \mapsto \mathrm{ev}_{|g\rangle} \in \mathbb{C}[\hat{G}]$が自然に同型なので，逆変換のほうが都合がよい.

# Sketch of Proof [EHK04]

- 量子アルゴリズムを具体的に作るには，今言ったものを量子回路の組み合わせで書き下すことも大事.
  - パーツ：Pauli行列，Hadamard変換，CNOTゲート，Toffoliゲートなど
- 今回は細かいところには目を瞑り，実際に隠れ部分群問題を解いてみよう.

**HSP for $G = \bigoplus_j \mathbb{Z}/t_j\mathbb{Z}$**

$G := \bigoplus_j \mathbb{Z}/t_j\mathbb{Z}$，$X$：有限集合，$f\colon G \to X$：写像．$U_f$：$f$のユニタリ変換 on $\mathbb{C}^G \otimes \mathbb{C}^X$.
このとき，$f$で隠された部分群$H$の生成元を求めよ.

# Step 1. Extract information of $f$ using the oracle

- $\mathbb{C}^G \otimes \mathbb{C}^X$において初期ベクトル$|0\rangle|0\rangle$を取る.

1. 第一レジスタを重ね合わせる（変換(2)）：$|0\rangle|0\rangle \mapsto \frac{1}{\sqrt{\#G}} \sum_{g\in G} |g\rangle|0\rangle$.
2. $U_f$を噛ませる（変換(1)）：$U_f$: $|g\rangle|0\rangle \mapsto |g\rangle|f(g)\rangle$.

- ここで$\frac{1}{\sqrt{\#G}} \sum_{g\in G} |g\rangle|f(g)\rangle$は，$f(g) = f(gh)$ for every $h \in H$であることから，以下の値と一致する：

$$\frac{1}{\sqrt{\#G}} \sum_{s\in G/H} \sum_{h\in H} |s+h\rangle|f(s)\rangle.$$

3. 右側のレジスタのみ観測：ある$s \in G$で$|f(s)\rangle$が観測され，残った状態は$\frac{1}{\sqrt{\#H}} \sum_{h\in H} |s+h\rangle$となる.

# Step 2. Random picking from $H^{\perp}$.

4. $\frac{1}{\sqrt{\#H}} \sum_{h \in H} |s+h\rangle \in \mathbb{C}^G$にQFTを施す（変換(3)）：
   $\frac{1}{\sqrt{\#H}} \sum_{h \in H} \mathrm{QFT}(|s+h\rangle)$.

これを計算すると以下になる：

$$\sqrt{\frac{1}{\#H^{\perp}}} \sum_{\chi \in H^{\perp}} \chi(s)|\chi\rangle \cdots (\bigstar) \text{ where } H^{\perp} := \{g \in \widehat{G} \mid g(h) = 1 \text{ for any } h \in H\}$$

5. 第一レジスタを測定すると，必ず$H^{\perp}$の元$\chi$が出力される．さらに各$\chi \in H^{\perp}$についてそれが出力される確率は同様に確からしい．

**Claim.** $\chi \in \hat{G}$について$\sum_{h\in H}\chi(h) = \begin{cases} \#H & \text{if } \chi \in H^\perp \\ 0 & \text{if } \chi \notin H^\perp \end{cases}$.

Proof. $\chi \in H^\perp$の場合は自明である．そうでない場合ある$a \in H$で$\chi(a) \neq 1$である．
$\chi(a)\sum_{h\in H}\chi(h) = \sum_{h\in H}\chi(h)$だが，$\chi(a) \neq 1$より$\sum_{h\in H}\chi(h) = 0$. $\square$

*Proof of* $(\bigstar)$.

$$\begin{aligned}
\mathrm{QFT}\left(\frac{1}{\sqrt{\#H}}\sum_{h\in H}|s+h\rangle\right) &= \frac{1}{\sqrt{\#G\#H}}\sum_{h\in H}\sum_{\chi\in\hat{G}}\chi(s+h)|\chi\rangle \\
&= \frac{1}{\sqrt{\#G\#H}}\sum_{\chi\in\hat{G}}\chi(s)\sum_{h\in H}\chi(h)|\chi\rangle \\
&= \sqrt{\frac{\#H}{\#G}}\sum_{\chi\in H^\perp}\chi(s)|\chi\rangle \square.
\end{aligned}$$

# Step 3. あとは古典アルゴリズム

- 上の1~5を$N$回繰り返す→$\chi^1, \ldots, \chi^N \in H^\perp$が得られる.
- $N = O(\lceil \log_2 \#G \rceil)$なら，高い確率で$H^\perp$を生成する.
- ここで$G = \bigoplus_{j=1}^{l} (\mathbb{Z}/t_j\mathbb{Z})$とすれば
  $\hat{G} = \prod_{j=1}^{l} \widehat{\mathbb{Z}/t_j\mathbb{Z}} = \{(\chi_{1,k_1}, \ldots, \chi_{l,k_l}) \mid 0 \leq k_i < t_i\}$.
- この下で$\chi^p = (\chi_{1,k_1^p}, \ldots, \chi_{l,k_l^p})$と書く．$g = (g_j) \in G$について,

$$g \in H \iff \forall p, 1 = \chi^p(g) = \prod_{j=1}^{l} \chi_{j,k_j^p}(g_j) = \prod_{j=1}^{l} e^{\frac{2\pi i k_j^p g_j}{t_j}} \iff \sum_{j=1}^{l} \frac{k_j^p g_j}{t_j} \equiv 0 \pmod{\mathbb{Z}}.$$

- $e := \mathrm{lcm}(t_1, \ldots, t_l), a_j^p := e k_j^p / t_j \in \mathbb{Z}$とすれば，$\forall p, \sum_{j=1}^{l} a_j^p g_j \equiv 0 \pmod{e}$
  と同値．これは解くことができるので，HSPが解けた．□

# まとめ

- 有限体Diffie-Hellmanと楕円曲線Diffie-Hellmanは，アーベル群$G$におけるDiffie-Hellmanの特別な例である.
- アーベル群Diffie-Hellmanは，$f\colon (\mathbb{Z}/n\mathbb{Z})^{\oplus 2} \to G$なる群準同型の核を求める問題に帰着される.
- 量子アルゴリズムと$f$の量子オラクルを用いると，$(\mathbb{Z}/n\mathbb{Z})^{\oplus 2} \to (\mathbb{Z}/n\mathbb{Z})^{\oplus N}$の表現行列の核を計算する問題に帰着できる.

**→アーベル群Diffie-Hellmanは量子アルゴリズムで安全ではない**

# 現状の量子計算機

- 量子アルゴリズムを実現できる計算機を量子計算機という.
- 量子計算機にはいろんな実現方法があるらしいが，「量子ビット数を増やすことが難しい」，「物理的影響で生じる計算誤差」が目下の課題とのこと.
  - 今のところ量子ビット数はIBMの1121が最大と思われるが，誤差付きの計算結果となる
- 一方，隠れ部分群問題は$\mathbb{C}^G \otimes \mathbb{C}^X$というレジスタを使うので，少なくとも$\log_2 \#G$の量子ビットが必要であり，さらに計算も正確である必要がある
  - 例：ffdhe2048/3072/4096なら2048/3072/4096量子ビットが必要
- 隠れ部分群問題の効率化などの研究も行われているが，まだ実用的なものはない

**ソフトウェアはあるが，ハードウェアがない.**

**→有限体DH，楕円曲線DHは未だに社会で使われている**

# 復習：群作用Diffie-Hellman

アーベル群Diffie-Hellmanはだめだったが，群作用ではどうか？

**群作用離散対数問題**

$A$をアーベル群，$x \in X$を点付き対象，$A \curvearrowright X$を忠実な作用とする．

$$\mathrm{DE}_x \colon A \ni a \mapsto a.x \in X$$

の像を$\mathrm{Orb}(x)$，逆写像を$\mathrm{DL}_x \colon \mathrm{Orb}(x) \to A$とする．

このとき，$y \in \mathrm{Orb}(x)$について，$\mathrm{DL}_x(y)$を計算せよ．

# 群作用離散対数問題の求解アプローチ

- $x, y \in X$とする．ある$s \in A$で$y = s.x$だったとしよう．
- 以下の関数を考える：

$$f\colon A \ni a \mapsto a.x \in X$$
$$g\colon A \ni b \mapsto b.y \in X$$

- $f, g$はどちらも単射，$f(A) = g(A)$であり，$f(a) = g(b) \iff b = a - s$.

**Abelian Hidden Shift Problem（AHSP，アーベル群隠れシフト問題）**

$A$をアーベル群，$X$を集合，$f, g\colon A \to X$を単射とする．$f(A) = g(A)$のとき，任意の$a$について$f(a) = g(a - s)$なる$s$を見つけよ．

AHSPが解ければ，離散対数問題も解けることになる．

# 一般化二面体群

- $\mu_2 = \{1, -1\} \subset \mathbb{C}^\times$とする．アーベル群$A$について，一般化二面体群$D_A = A \rtimes \mu_2$を以下で定める：

$$(g, i) * (h, j) = (g + ih, ij) \text{ where } i, j \in \{-1, 1\}$$

- For given $f, g$: $A \to X$, let $h$: $A \rtimes \mu_2 \to X$ be

$$h\colon A \rtimes \mu_2 \ni (a, i) \mapsto \begin{cases} f(a) & i = 1 \\ g(a) & i = -1 \end{cases} \in X$$

- $h(a, 1) = h(b, -1) \iff f(a) = g(b) \iff b = a - s$.
- よって$K_a := \{(a, 1), (a - s, -1)\}$として，$K_0$が$h$の隠れ部分群.

結局$K_0 = \{(0, 1), (-s, -1)\}$がわかればよい.

# Dihedral Hidden Subgroup Problem

**Dihedral Hidden Subgroup Problem（DHSP，二面体群隠れ部分群問題）**

有限アーベル群$A$，$X$を集合，$f\colon A \rtimes \mu_2 \to X$を写像とする．このとき，$f$で隠された部分群$H$の生成元を求めよ．

- 上の問題は，量子アルゴリズムで，劣指数時間で解ける[Reg04], [Kup14].
  - 多項式時間ではないが，指数時間よりは高速.
- 現状，群作用Diffie-Hellmanは，量子計算機に対して耐性があると言える.
- しかし，DHSPとアーベル群作用離散対数問題が同値なのかは未だに未解決である[MZ22].

# まとめ

- 現状の鍵共有プロトコル（⊂ AbDH）は，量子アルゴリズムで解読可.
  - アーベル群離散対数問題=アーベル群の隠れ部分群問題（HSP）.
  - アーベル群HSPは量子アルゴリズムで効率的に解ける.
    - 他の量子アルゴリズムとしては，素因数分解（Shorのアルゴリズム）や高速探索（Groverのアルゴリズム）なども有名
  - しかし量子計算機はまだ実現されてない（ソフトは◯，ハードは×）
- 群作用Diffie-Hellmanは，量子アルゴリズムで劣指数時間の解法がある（DHSP）
  - 多項式時間ではないが，指数時間よりは高速.

**量子計算機でも解読できない鍵共有はないものか？**

# →耐量子暗号

# 4. 耐量子暗号

# より一般化された設定

以下の写像たちを考える：

- $f_A \colon S_A \times X \to Y_A$.
- $g_A \colon S_A \times Y_B \to Z$.
- $f_B \colon X \times S_B \to Y_B$.
- $g_B \colon Y_A \times S_B \to Z$.
- $x \in X$：セットアップで固定

以下が可換とする：

$$\begin{array}{ccc} S_A \times X \times S_B & \xrightarrow{\mathrm{id}_{S_A} \times f_B} & S_A \times Y_B \\ \downarrow{\scriptstyle f_A \times \mathrm{id}_{S_B}} & & \downarrow{\scriptstyle g_A} \\ Y_A \times S_B & \xrightarrow[g_B]{} & Z. \end{array}$$

- $S_*$：secret，$Y_*$：public，$X, Z$：common.
- Alice：$s_A \in S_A$を秘密，$y_A := f_A(s_A, x)$を公開，$z := g_A(s_A, y_B)$を共有
- Bob：$s_B \in S_B$を秘密，$y_B := f_B(x, s_B)$を公開．$z := g_B(y_A, s_B)$を共有

# 例：群作用鍵共有

以下の写像たちを考える：

- $f_A = g_A : G_A \times X \to X$：左作用
- $f_B = g_B : X \times G_B \to X$：右作用
- $x \in X$：セットアップで固定.

$$
\begin{array}{ccc}
G_A \times X \times G_B & \longrightarrow & G_A \times X \\
\downarrow & & \downarrow \\
X \times G_B & \longrightarrow & Z
\end{array}
$$

$$
\begin{array}{ccc}
(s_A, x, s_B) & \longmapsto & (s_A, x.s_B) \\
\downarrow & & \downarrow \\
(s_A.x, s_B) & \longmapsto & s_A.x.s_B
\end{array}
$$

$G_A = G_B$がアーベル群なら今までの群作用DH

# 例：二次形式

- $f_A \colon \mathbb{F}^n \times \mathrm{M}_n(\mathbb{F}) \to \mathbb{F}^n;$
  $(s_A, M) \mapsto s_A \cdot M$
- $f_B \colon \mathrm{M}_n(\mathbb{F}) \times \mathbb{F}^n \to \mathbb{F}^n;$
  $(s_B, M) \mapsto s_B \cdot M^{\mathsf{T}}$
- $g_A = g_B \colon \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F};$
  $(v, w) \mapsto v \cdot w^{\mathsf{T}}$
- $M \in \mathrm{M}_n(\mathbb{F})$：セットアップで固定.

$$
\begin{array}{ccc}
\mathbb{F}^n \times \mathrm{M}_n(\mathbb{F}) \times \mathbb{F}^n & \longrightarrow & \mathbb{F}^n \times \mathbb{F}^n \\
\downarrow & & \downarrow \\
\mathbb{F}^n \times \mathbb{F}^n & \longrightarrow & \mathbb{F}. \\
\\
(s_A, M, s_B) & \longmapsto & (s_A, s_B \cdot M^{\mathsf{T}}) \\
\downarrow & & \downarrow \\
(s_A . M, s_B) & \longrightarrow & s_A . M . s_B^{\mathsf{T}}
\end{array}
$$

- これは簡単に解けてしまう：$M$の逆行列を計算し，公開情報$y_A = M . s_A$について$M^{-1} y_A$をすれば良い.

# 誤差付きで考えてみる

- $M \in \mathrm{M}_n(\mathbb{F})$：固定
- $f_A \colon \mathbb{F}^n \times \mathbb{F}^n \times \mathrm{M}_n(\mathbb{F}) \to \mathbb{F}^n ; (\boldsymbol{s}_A, \underbrace{e_A}_{\text{error}}, M) \mapsto p_A := \boldsymbol{s}_A \cdot M + e_A.$
- $f_B \colon \mathrm{M}_n(\mathbb{F}) \times \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^n ; (\boldsymbol{s}_B, \underbrace{e_B}_{\text{error}}, M) \mapsto p_B := \boldsymbol{s}_B \cdot M^{\mathsf{T}} + e_B.$

もちろんこれは可換ではなく，誤差が発生する：

- Aliceさんが得るもの：$K_A := \boldsymbol{s}_A . p_B^{\mathsf{T}} = \boldsymbol{s}_A . M . \boldsymbol{s}_B^{\mathsf{T}} + \langle \boldsymbol{s}_A, e_B \rangle .$
- Bobさんが得るもの：$K_B := p_A . \boldsymbol{s}_B^{\mathsf{T}} = \boldsymbol{s}_A . M . \boldsymbol{s}_B^{\mathsf{T}} + \langle e_A, \boldsymbol{s}_B \rangle .$

ただ，誤差$e$を小さくすれば，情報を取り出せるのでは？

# Regevの発想：ビットの取り出し [Reg05]

- $p$を奇素数，$\mathbb{F} = \mathbb{F}_p$を$\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$と同一視する.
- エラーが$2e_A, 2e_B$だったとする：
  - Alice：$K_A := s_A . M . s_B^{\mathsf{T}} + \langle s_A, 2e_B \rangle \in \mathbb{F}_p$.
  - Bob：$K_B := s_A . M . s_B^{\mathsf{T}} + \langle 2e_A, s_B \rangle \in \mathbb{F}_p$.
- 通常，$\mathbb{F}_p$の元には偶奇は定まらない（$1 = p + 1 = 2p + 1 = \ldots$）.
- しかしエラーベクトル$e$と秘密ベクトル$s$を十分"小さく"取れれば，$\langle s, 2e \rangle$がオーバーフローせず，$[-\frac{p-1}{2}, \frac{p-1}{2}] \cap \mathbb{Z}$内での計算で収まる.
- →エラーが十分小さいならビットを取り出せるのでは？

# Robust Extractor [DXL12]（簡略版）

Suppose $|\langle e_A, s_B\rangle - \langle s_A, e_B\rangle| \leq \frac{p-1}{8}$. $(\mathbb{F}_p = [-\frac{p-1}{2}, \frac{p-1}{2}] \cap \mathbb{Z})$

- Alice: $K_A = s_A.M.s_B^{\mathsf{T}} + \langle s_A, 2e_B\rangle$.
- Bob: $K_B := s_A.M.s_B^{\mathsf{T}} + \langle 2e_A, s_B\rangle$.
- Alice: let $\sigma := 0$ if $K_A \in [-\frac{p-1}{4}, \frac{p-1}{4}], \sigma := 1$ o.w.
- Alice: put $E_A := K_A + \sigma \cdot \frac{p-1}{2}$. Then $E_A \in [-\frac{p-1}{4}, \frac{p-1}{4}]$.
- Alice->>Bob：$\sigma$を伝達
- Bob：$E_B := K_B + \sigma m$：これはオーバーフローせずに計算できる

$$E_B = E_A + (K_B - K_A) = \underbrace{E_A}_{\in[-\frac{p-1}{4}, \frac{p-1}{4}]} + \underbrace{2(\langle e_A, s_B\rangle - \langle s_A, e_B\rangle)}_{\in[-\frac{p-1}{4}, \frac{p-1}{4}]}.$$

**→$E_A$と$E_B$の2で割った余りは一致する！**

# $e, s$を取るための離散ガウシアン分布

急峻な"$\mathbb{Z}^n$上の正規分布"に従って$e, s \in \mathbb{Z}^n$をピックできれば，非常に高い確率で

- $e, s$の各成分を$[-\frac{p-1}{2}, \frac{p-1}{2}] \cap \mathbb{Z}$に入るようにでき，
- $\langle e, s \rangle_{\mathbb{Z}} \in [-\frac{p-1}{16}, \frac{p-1}{16}]$と十分小さく取れる．

実際には，$16r^2n + 1 < p$なる状況で，以下の確率密度$\sigma_r$から定まる離散ガウシアン分布$D_{L,r}$から取ってくる．

$$\rho_{\mathbb{R}^n,r} \colon \mathbb{R}^n \ni x \mapsto \exp\left(-\pi \frac{\|x\|^2}{r^2}\right) \in \mathbb{R}_{>0}$$

$$\rho_r(\mathbb{Z}^n) := \sum_{v \in \mathbb{Z}^n} \rho_r(v)$$

$$\sigma_r(v) := \rho_r(v) / \rho_r(L)$$

# 参考：通常の正規分布の復習

- 関数の定義：$s > 0$, $n \in \mathbb{Z}_{>0}$, $c \in \mathbb{R}^n$について, $\rho_{s,c}$を以下で置く：

$$\rho_{s,c}\colon \mathbb{R}^n \ni x \mapsto \exp\left(-\pi \frac{\|x-c\|^2}{s^2}\right) \in \mathbb{R}_{>0}$$

- 積分：この積分はガウス積分としてよく知られていて,

$$\int_{x \in \mathbb{R}^n} \rho_{s,c}(x)\, dx = s^n$$

- よって

$$\nu_{s,c} := \rho_{s,c} / s^n$$

とすることで, $\mathbb{R}^n$上の確率密度関数が定まる.

- 記号として, $\rho_s := \rho_{s,0}$, $\nu_s := \nu_{s,0}$と書く.

# 参考：離散ガウシアン分布 $D_{L,s}$

- $\mathbb{Z}^n \simeq L \subset \mathbb{R}^n$をフルランク格子とする
- （つまり$L$は$\mathbb{R}^n$の離散な加法部分群かつ$L$を含む最小の線形部分空間が$\mathbb{R}^n$自身）
- $\rho_s$は急減少関数だから，以下の無限和は収束する：

$$\rho_s(L) := \sum_{v \in L} \rho_s(v)$$

- よって以下の$L$上の確率密度関数$\sigma_s$が決まる：

$$\sigma_s(v) := \rho_s(v)/\rho_s(L)$$

**Definition.** フルランク格子$L \subset \mathbb{R}^n$について，$D_{L,s}$を$\sigma_s$に従う$L$上の確率分布とする.

# 参考：内積評価 on $\mathbb{Z}^n$.

$v \leftarrow D_{\mathbb{Z}^n,r}$を取ったとき，そのノルムはほぼ$r\sqrt{n}$で抑えられる．すなわち：

**Fact [Ban93].**

$$\Pr_{v \leftarrow D_{\mathbb{Z}^n,r}}(\|v\| > r\sqrt{n}) \leq 2^{-2n} \cdot r^n \cdot \rho(\mathbb{Z}^n). \blacksquare$$

特に$s, e \leftarrow D_{\mathbb{Z}^n,r}$をとったとき，$2^{-2n} r^n 2\rho(\mathbb{Z}^n)$の確率を除き，

- $s, e \in [-r\sqrt{n}, r\sqrt{n}]^n$であり，
- $|\langle s, e \rangle| \leq r^2 n$（Cauchy-Schwartz）.

# 参考：内積評価 on $\mathbb{F}_p^n$.

素数$p$について，$\mathbb{F}_p$を$\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$と同一視する．$r^2 n < \frac{p-1}{16}$であれば，$s_A, e_A, s_B, e_B \leftarrow D_{\mathbb{Z}^n, r}$は無視できる確率を除いて

- $s_A, e_A, s_B, e_B \in \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}^n$.
- $|\langle s_A, e_B \rangle_{\mathbb{Z}}| \leq r^2 n$, $|\langle e_A, s_B \rangle_{\mathbb{Z}}| \leq r^2 n$.
- $|\langle s_A, e_B \rangle_{\mathbb{Z}} - \langle e_A, s_B \rangle_{\mathbb{Z}}| \leq 2r^2 n < \frac{p-1}{8}$.

# 安全性とLWE問題

- Aliceの公開情報：$p_A = s_A \cdot M + e_A$
- $e_A$というエラー項を付け加えただけ…秘密$s_A$を求められるのでは？

**Learning with Error問題（LWE問題）** ：$1 \leq n \leq m$を整数，$p$を素数，
$M \in \mathrm{M}_{m,n}(\mathbb{F})$：フルランク，$\chi$：$\mathbb{F}^n$上の確率分布とする（エラー分布）
以下のアルゴリズム$\mathcal{A}$を考える：

- 入力：$s \in \mathbb{F}^m$．出力：$v \in \mathbb{F}^n$．

1. $e \in \mathbb{F}^n$: 確率分布$\chi$に従って選ぶ．
2. $v := s \cdot M + e$とし，$v$を出力．

$\mathcal{A}$の出力$v$が与えられたとき，入力$s$を求めよ．

# 素朴なobservation(1)：LWE問題

$n = m$のLWE問題を考えよう.

$n \in \mathbb{Z}_{\geq 1}, M \in \mathrm{GL}_n(\mathbb{F})$. 入力$s \in \mathbb{F}^n$について$v \leftarrow \mathcal{A}(s)$を以下で出力：
$e \xleftarrow{\chi} \mathbb{F}^n$, $v := s \cdot M + e$.

$s$を素朴に求める方法として，以下を計算する：$s' \leftarrow v \cdot M^{-1} = s + e \cdot M^{-1}$.

- $v$と$s$. $M$の"距離"は$\|e\|$であり，非常に小さい.
- $s$と$s'$の"距離"は$\|e \cdot M^{-1}\| = \|e\|\|M^{-1}\|$：大きくなってしまう.
- →素朴に解こうとしても中々難しい.

**LWE問題は量子アルゴリズムですら解く方法が見つかっていない**

# 素朴なobservation(2)：LWE問題

では，共通されるビット$b \in \{0,1\}$は割り出されるのか？

- 攻撃者が素数$p$，行列$M$に加え，通信経路に乗る全データを得たとしよう：
  - $p_A = s_A \cdot M + 2e_A$,
  - $p_B = s_B \cdot M^{\mathsf{T}} + 2e_B$,
  - $\sigma \in \{0,1\}$：$K_A := s_A \cdot p_B^{\mathsf{T}} \in [-\frac{p-1}{4}, \frac{p-1}{4}]$なら$0$，それ以外は$1$.
- 攻撃者が割り出したいデータ
  - $K_A + \sigma \cdot \frac{p-1}{2}$を$2$で割った余りを求めたい
  - $\sigma$はわかってる$\Rightarrow$ $K_A = s_A \cdot p_B^{\mathsf{T}}$を$2$で割った余りがわかることと同値
  - しかし$s_A$はランダムなので，$s_A \cdot p_B^{\mathsf{T}}$の偶奇はわからない

**→LWE問題さえ解けなければかなり安全→耐量子暗号として有力**

# ML-KEMとNISTの標準化

- NIST PQC Standardization
  - 米国立標準技術研究所（NIST）により開催されている，耐量子暗号の標準化を目的としたコンペティション．2016年より開始.
- 2024/8/13：耐量子鍵カプセル化方式FIPS203として**ML-KEM**が標準化.
  - ML-KEM = Module-Lattice based Key-Encapsulation Mechanism
  - 採択されたのは**Crystal-Kyber**[CrystalKyber]．上で見たものがベース.
- 現在TLS通信でも使えるようにドラフトが作られている：[KyberTLSDraft]

**→近い将来，量子計算機にも耐える（かもしれない）安全な通信が実現する**

# 参考）TLSで使えるようになるであろう鍵の比較

| 鍵共有方式 | 公開鍵長 | 秘密鍵長 | セキュリティ |
|---|---|---|---|
| ffdhe3072 | 3072 | 275~1536 | 125 |
| ffdhe4096 | 4096 | 325~2048 | 150 |
| secp256r1 | 512 | 256 | 128 |
| secp384r1 | 768 | 384 | 192 |
| secp521r1 | 1042 | 521 | 260 |
| x25519 | 510 | 255 | 127 |
| x448 | 896 | 448 | 224 |
| Kyber512 | 800 | 1632 | 128 |
| Kyber768 | 1184 | 2400 | 192 |
| Kyber1024 | 1568 | 3168 | 256 |

- 有限体DH：公開鍵・秘密鍵ともに長く，セキュリティも微妙.
- 楕円曲線DH：公開鍵・秘密鍵が短い．こちらも古くから使われている. 最近のアプリケーションはこれを使うイメージがある.
- Kyber：秘密鍵長がボトルネック．これから使われていく予定.

**正直量子計算機よりも怖いのは**
**人間のヒューマンエラーです.**
**気をつけて使おう！**

# まとめ

- LWEを使った耐量子鍵共有方式：「二次形式の値をエラー付きで共有する」
  - キモ：エラーが十分小さいなら$\langle s_A, s_B \rangle_M + \langle s_A, 2e_B \rangle$の偶奇は一意的
- 解読するにはLWE問題を解く必要があり，それは難しそう
  - LWE問題：誤差付きの線形方程式を解くこと.
- LWE問題を基礎とした暗号方式ML-KEMが標準化された

**LWE問題の困難性は今も盛んに研究が行われている.**

（「解かれないこと」が示される日が来るのでしょうか…）

# おわりに

- **現代暗号の大目標：解読不能な鍵共有方式をつくる**

| 鍵共有法 | 解読する問題 | 古典計算解読の現状 | 量子計算解読の現状 |
|---|---|---|---|
| 有限体DH | $\mathbb{F}_p^\times$の離散対数問題 | 劣指数時間 | 多項式時間（HSP） |
| ECDH | 楕円曲線の離散対数問題 | 劣指数時間 | 多項式時間（HSP） |
| GADH | 群作用 | 指数時間 | 劣指数時間（DHSP） |
| Kyber | Module-LWE | 指数時間 | 指数時間 |

- これらの方式は全て純粋数学が支えている→社会で純粋数学はとっても有用！
- それでいてこれらのアイデアは，**別に暗号のために作られたわけじゃない**.

**→自由に研究することで今までにないアイデアが生まれる．純粋数学は大事ですね！**

# 5.（おまけ） 現代の暗号解読：同種写像と暗号解析

# SIKE：Supersingular Isogeny Key Encapsulation

- かつて耐量子暗号として期待されていた方式として**SIKE**があった.
- NIST PQC Standardizationでも最終ラウンド（2022）まで候補として残った
- しかし2022年，SIKEは解読された[CD23].
- 解読は「**古典計算機**」で行える.
- 解読アイデアは純粋数学をフルに使う.

  **みんなが「耐量子性がありそう」と言っていても，真実はどうかわからない.**

- この解読のお話と，同種写像についてお話します.

# 同種写像問題

- $\mathbb{F}$を有限体とする.
- $E$を$\mathbb{F}$上の楕円曲線とする.
- $G \subset E(\mathbb{F}_p)$を巡回群とする.
- このとき，$E \to E/G$という同種が得られる.

**同種写像問題**

二つの楕円曲線$E, E'$が同種であったとき，同種$E \to E'$を求めよ.

- $E$がordinaryのときは，準指数時間で量子アルゴリズムで解ける [AJS14]

**→supersingularのときが重要**

# SIDH (Supersingular Isogeny Diffie Hellman) [JdF11]

**設定**

- $p = 2^{e_A}3^{e_B}f - 1$：素数.
- $E_0 := (y^2 = x^3 + x)/\mathbb{F}_p$.
- $P_A, Q_A \in E[2^{e_A}]$：生成元
- $P_B, Q_B \in E[2^{e_B}]$：生成元

**秘密**

- Alice：秘密$k_A \in (\mathbb{Z}/2^{e_A})^\times$
- Bob：秘密$k_B \in (\mathbb{Z}/3^{e_B})^\times$

**公開**

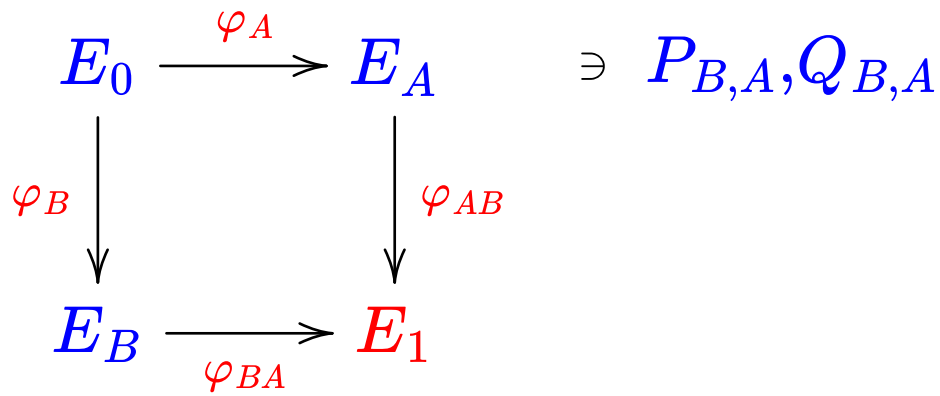
- Alice: $E_A := E_0/\langle R_A \rangle$, $P_B, Q_B$の像$P_{BA}, Q_{BA} \in E_A$を公開
- Bob: $E_B := E_0/\langle R_B \rangle$, $P_A, Q_A$の像$P_{AB}, Q_{AB} \in E_B$を公開

**共有**

- Alice:$E_{BA} := E_B/\langle P_{AB} + k_A Q_{AB} \rangle$.
- Bob:$E_{AB} := E_A/\langle P_{BA} + k_B Q_{BA} \rangle$.

$E_{AB} \simeq E_{BA}$なので，$j$-不変量を共有可能

# SIDHは破るには：同種問題の亜種




青は公開，赤が秘密，横は$N_A = 2^{e_A}$-同種，縦は$N_B = 3^{e_B}$-同種．これを破るには：

**SuperSingular Isogeny problem with Torsions**

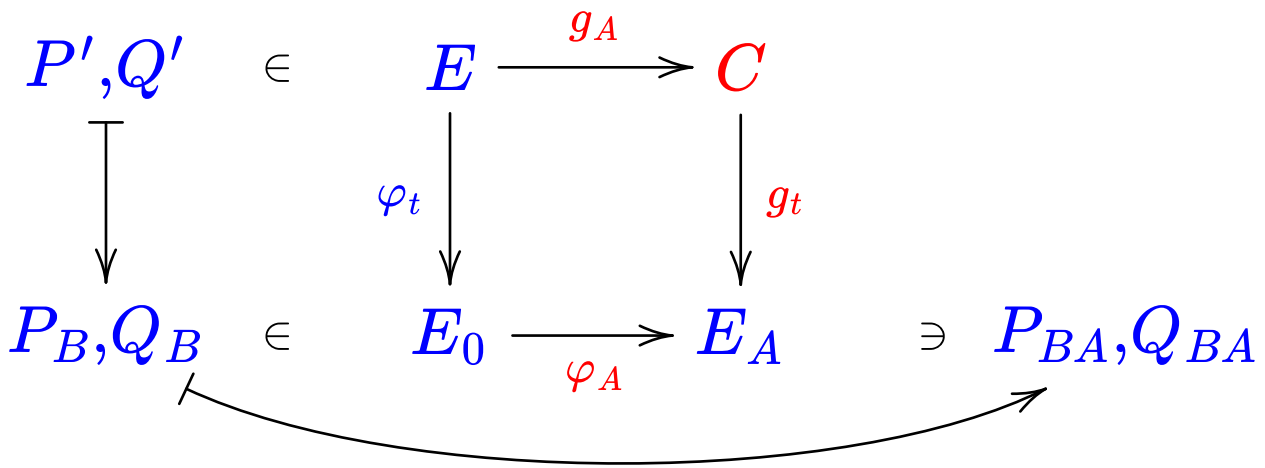
$N_A, N_B$：互いに素な整数，$E_0$：超特異楕円曲線．
$\varphi_A : E_0 \to E_A$という$N_A$-同種が存在したとする．
このとき，$\varphi_B(E_A[N_B])$を用いて，$\mathrm{Ker}\,\varphi_A$を計算せよ．

# Direct Key Recovery Attack [MMPPW23]

- Generate $\varphi_t : E \to E_0$：degree $N_B - N_A$.
- $P', Q' \in E$：点$P, Q$のリフト
- Write $E \xrightarrow{g_A} C := E/\widehat{\varphi_t}(\mathrm{Ker}\,\varphi_A)$
- $C$は$E_A$を支配する.

$$\Phi = \begin{pmatrix} \varphi_t & -\widehat{\varphi_A} \\ g_A & \widehat{g_t} \end{pmatrix} : E \times E_A \to E_0 \times C$$

- **Kaniの定理と捻れ点を使うと計算可**
- $\Phi(0, x) = (\widehat{\varphi_A}(x), x_C)$.
- →$\widehat{\varphi_A}$がわかる→$\varphi_A$がわかる



# SIDHのざっくりとした経緯

- 2011年：SIDHができた[JdF11]
- 2022年：Castryck–Decru [CD23]によりSIDHが破られた
  - 同種の計算問題を，同種の"存在"問題に帰着する.
  - 同種の存在判定にKaniの結果[Kan97]（1997年の定理）を使う.
- 2022年：Maino-Martindale-Panny-Pope-Wesolowski[MMPPW23]により改良（上の形）
  - $\mathrm{Ker}\,\Phi$の公式が本質的，これもKaniの定理と現在では言われる.

破るための定理は，生まれた時点ですでにあった→純粋数学は"金脈"のようなもの?!

# CSIDH (Commutative SIDH)

- この攻撃はインパクトがかなりあり，他のいくつかの同種写像鍵共有も（古典計算機で）解読された
- →同種写像を使った鍵共有の中で，攻撃耐性がある例として，CSIDHを簡単に紹介する.
  - Kaniの定理で用いた捻れ点の情報がない.
  - 同種写像ベースの鍵共有方式として，現在最も有力.
  - 群作用Diffie-Hellmanである.
  - オリジナルはCouveignes[Cou06], Rostovtsev–Stolbunov[RS06]による提案.

# 考える群作用 (1/2)

- $p$：素数，$E$：$\mathbb{F}_p$上の楕円曲線.
- $t := (p+1) - \#E(\mathbb{F}_p)$.
- $\mathcal{O} := \mathrm{End}_p(E)$：$\mathbb{F}_p$上の自己準同型環.
- $\pi$: $E \to E$：Frobenius
  - $\pi^2 - t\pi + p = 0$（Waterhouse）
  - $t^2 - 4p \leq 0$（Hasse-Weil）
  - $t = 0 \iff E$: supersingular
- $\pi \in \mathcal{O} \subset \mathbb{Q}(\sqrt{t^2-4p})$

$\mathfrak{a} \subset \mathcal{O}$を分数イデアルとしたとき，同種

$$E \to E/\mathfrak{a}$$

が次のように定まる[Wat69].

- $\mathfrak{a} = (\pi)^r \cdot \mathfrak{a}_s$と分解できる.
- $G := \bigcap_{\alpha \in \mathfrak{a}_s} \mathrm{Ker}\,\alpha$
- $E/G$に$r$回Frobeniusを作用
- 注意：$\mathfrak{a}$が単項なら同型.

# 考える群作用 (2/2)

$E/\mathfrak{a}$の$\mathbb{F}_p$-エンド環は$\mathrm{End}_p(E) \simeq \mathrm{End}_p(E/\mathfrak{a})$を満たす．そこで，

- For $d \geq 0$，$\mathcal{O}$：$\mathbb{Q}(\sqrt{-d})$のmaximal order，$\pi \in \mathcal{O}$，
- let $\mathcal{E}ll_p(\mathcal{O}, \pi)$：$\mathrm{End}_p(E) = \mathcal{O}$かつ$\pi$がFrobeniusに対応する楕円曲線全体

とし，$\mathrm{Cl}(\mathcal{O}) \curvearrowright \mathcal{E}ll_p(\mathcal{O}, \pi)$を考える：

$$(\mathfrak{a}, E) \mapsto E/\mathfrak{a}$$

**Theorem [Wat69],[Sch87].** これはfully faithful.

# CSIDH Protocol [CSIDH]

**CSIDH**

- $p = 4l_1 \cdots l_n - 1$：素数 s.t. $l_1, \ldots, l_n$：奇素数.
- $\mathcal{O} := \mathbb{Z}[\pi]$ where $\pi := \sqrt{-p}$.

$\mathrm{Cl}(\mathcal{O}) \curvearrowright \mathcal{E}ll_p(\mathcal{O}, \pi)$の作用によるDiffie-HellmanをCSIDHと呼ぶ.

- Alice：$\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$を秘密，$E_A := E/\mathfrak{a}$を公開，$E_A/\mathfrak{b}$を共有
- Bob：$\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$を秘密，$E_B := E/\mathfrak{b}$を公開，$E_B/\mathfrak{a}$を共有

# CSIDHの安全性

次の問題が安全性の根拠となる

- (DL): For given $E, C \in \mathcal{E}ll_p(\mathcal{O}, \pi)$, find $\mathfrak{a}$ s.t. $C \simeq E/\mathfrak{a}$.
- (CDH): For given $E, E/\mathfrak{a}_1, E/\mathfrak{a}_2 \in \mathcal{E}ll_p(\mathcal{O}, \pi)$, find $E/\mathfrak{a}_1\mathfrak{a}_2$.
- (DDH) Distinguish the following two distributions:
  - $(E/\mathfrak{a}, E/\mathfrak{b}, E/\mathfrak{a}\mathfrak{b})$, where $\mathfrak{a}$, $\mathfrak{b}$ are uniform.
  - $(E/\mathfrak{a}, E/\mathfrak{b}, E/\mathfrak{c})$, where $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are uniform.

- 群作用離散対数問題なので，Dihedral hidden subgroup problemが解ければ良い．これは劣指数時間．
- $\mathrm{Cl}(\mathcal{O})[2] \neq 0$のときは，DDHが解かれている．

# まとめ

- 同種写像を使った鍵共有：かつてはSIDH，今はCSIDH.
  - どちらも楕円曲線を共有する
  - SIDH：楕円曲線の同種を，捻れ点集合をもちいて計算
  - CSIDH：楕円曲線の同種を，群作用を用いて計算.
- SIDHの解読（Castryck–Decru攻撃）は純粋数学に基づく.
- Castryck–Decru攻撃を使った，新しい方式の高速化研究も進んでいる
  - FESTA，SQIsign2D–West

暗号を作るのも数学であり，解読するのも数学であり，解読を活用するのも数学

**→純粋数学は過去・現在・未来の社会を支えに支えまくっている**

# 早見表

| 鍵共有法 | 解読する問題 | 古典計算解読の現状 | 量子計算解読の現状 |
|---|---|---|---|
| 有限体DH | $\mathbb{F}_p^\times$の離散対数問題 | 劣指数時間 | 多項式時間（HSP） |
| ECDH | 楕円曲線の離散対数問題 | 劣指数時間 | 多項式時間（HSP） |
| CSIDH | 虚二次体整環イデアル類群の楕円曲線のモジュライへの群作用離散対数問題 | 指数時間 | 劣指数時間（DHSP） |
| Kyber | Module-LWE | 指数時間 | 指数時間 |

# References for hidden subgroup problem


- [EHK04]: M.Ettinger, P.Hoyer, and E.Knill, "The quantum query complexity of the hidden subgroup problem is polynomial". *Inf. Process. Lett.*, 91, 43–48, 2004
- [Reg04] O.Regev. “A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space”, *arXiv preprint*, 2004. https://arxiv.org/abs/quant-ph/0406151.
- [Kup14] G.Kuperberg. “A subexponential-time quantum algorithm for the Dihedral Hidden Subgroup Problem”. *SIAM J. Comput.*, 35(1):170–188, 2005. https://arxiv.org/abs/quant-ph/0302112
- [MZ22]: H.Montgomery and M.Zhandry, "Full quantum equivalence of group action DLog and CDH, and more", *J. Cryptol.*, 37.4: 39, 2024.
- 石坂 智，小川 朋宏，河内 亮周，木村 元，林 正人，"量子情報科学入門"，共立出版，2012.

# References for LWE


- [Reg05]: O.Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography", *STOC*, ACM (2005) 84–93.
- [DXL12]: J.Ding, X.Xie, and X.Lin, "A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem", *IACR Cryptology ePrint Archive* 2012/688, (2012). https://ia.cr/2012/688.
- [Ban93]: W. Banaszczyk. "New bounds in some transference theorems in the geometry of numbers". *Math. Ann.*, 296(4):625–635, (1993).
- [CrystalKyber]: J.Bos, L.Ducas, E.Kiltz, T.Lepoint, V.Lyubashevsky, J.M.Schanck, P.Schwabe, G.Seiler, and D.Stehle, "CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM", *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 353-367, (2018). https://ieeexplore.ieee.org/abstract/document/8406610/
- [KyberTLSDraft] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

# References for SIDH


- [CD23]: W.Castryck and T.Decru. "An efficient key recovery attack on SIDH." *Advances in Cryptology - EUROCRYPT 2023*, 423–447, 2023.
- [AJS14]: A.Childs, D.Jao, and V.Soukharev, "Constructing elliptic curve isogenies in quantum subexponential time." *J. Math. Cryptol.*, 8.1 (2014): 1-29.
- [MMPPW23]: L.Maino, C.Martindale, L.Panny, G.Pope, and B.Wesolowski, "A direct key recovery attack on SIDH." *Advances in Cryptology - EUROCRYPT 2023*, 448–471, 2023.
- [JdF11]: D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". *In B. Yang, editor, PQCrypto 2011, volume 7071 of LNCS*, 19–34, 2011.
- [Kan97]: E.Kani, "The number of curves of genus two with elliptic differentials". *J. fur Reine Angew. Math.* 1997(485), 93–122 (1997).

# References for CSIDH


- [Cou06]: J-M.Couveignes. "Hard Homogeneous Spaces" *IACR Cryptology ePrint Archive* 2006/291, (2006). https://ia.cr/2006/291
- [RS06]: A.Rostovtsev and A.Stolbunov, "Public-key cryptosystem based on isogenies", *IACR Cryptology ePrint Archive* 2006/145, (2006). https://ia.cr/2006/145
- [Wat69]: W.C. Waterhouse. "Abelian varieties over finite fields", *Ann. Sci. Éc. Norm. Supér.*, 2:521–560, 1969.
- [Sch87]: R.Schoof. "Nonsingular plane cubic curves over finite fields", *J. Comb. Theory, Ser. A*, 46(2):183–211, 1987.
- [CSIDH]: W.Castryck, T.Lange, C.Martindale, L.Panny, and J.Renes, "CSIDH: an efficient post-quantum commutative group action", *Advances in Cryptology - ASIACRYPT 2018*, LCNS 11274, 395-427, 2018. https://csidh.isogeny.org

# おわり

お問い合わせはこちら：fukuoka.takeru@fujitsu.com