MITSUBISHI ELECTRIC
Changes for the Better

格子と同種写像に関するアルゴリズムの耐量子暗号への応用

数学協働ﾌﾟﾛｸﾞﾗﾑ:
情報ｾｷｭﾘﾃｨにおける数学的方法とその実践

2016年 12月 20日

高島克幸

三菱電機株式会社

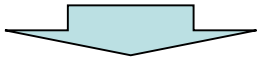
アジェンダ

- 研究の背景
  - 耐量子 公開鍵暗号 に関する 動向
- 格子暗号
  - 概要
  - 安全性評価に関する我々の成果 [高島-高安15]
- 同種写像暗号
  - 概要
  - 複数人 間 鍵共有 [古川-國廣-高島16]
  - ペアリング と 同種写像 を共に利用した暗号構成法
    [小柴-高島16]

研究の背景:
量子計算機　と　公開鍵暗号

NIST（米国立標準技術研究所）主催の新しい暗号ｺﾝﾍﾟﾃｨｼｮﾝ

- 量子計算機に対するデータ安全性の危殆化は、未来だけでなく現在の 暗号化データ に関しても考慮する必要がある
- NIST は、これまでも必要に応じて、暗号ｱﾙｺﾞﾘｽﾞﾑの公募を行い、公開評価を経て、標準・推奨ｱﾙｺﾞﾘｽﾞﾑ の選定を行ってきた



- 2016年、NIST は、量子計算機攻撃に耐性をもつ公開鍵暗号ｱﾙｺﾞﾘｽﾞﾑ の公募・ｺﾝﾍﾟﾃｨｼｮﾝ を呼びかけた
  - ディジタル署名
  - 暗号化　／　鍵共有
  - 決して、一つに絞り込むことを目指すわけでなく、ユーザにとっての “複数の妥当な選択肢” を提示することを目指す
  - ただし、先には、その中から ｱﾙｺﾞﾘｽﾞﾑ標準化 を見据える

NIST 主催の Post-Quantum 暗号 ｺﾝﾍﾟﾃｨｼｮﾝ

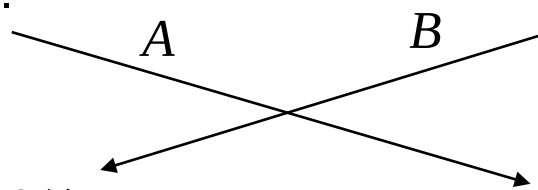
- スケジュール
  - 2016.02：耐量子(公開鍵)暗号に関する国際会議 PQCrypto 2016
    において、NIST が 公募ｺﾝﾍﾟﾃｨｼｮﾝ を行うことを ｱﾅｳﾝｽ した
    （例年の PQCrypto の倍以上の参加者を集めた）
  - 2016.12：ｱﾙｺﾞﾘｽﾞﾑ提案に関する正式な募集告知
  - 2017.11：ｱﾙｺﾞﾘｽﾞﾑ提案 受け付け終了
  - その後、3-5 年かけて、評価作業を進めて、結果をまとめる
  - 更に、2年後に、可能であれば、標準化ﾄﾞﾗﾌﾄ の作成を視野に入れる
  - その間、専用のﾜｰｸｼｮｯﾌﾟ も適宜開催して、評価・認識を共有

最も基本的な 公開鍵暗号： Diffie-Hellman 鍵共有

- 公開パラメータ：素数 p（例：500桁），$\mathbb{F}_p^\times$（$\cong \{1,..,p-1\}$）の生成元 g

  記法：$x \xleftarrow{\cup} X \iff x$ を集合 X から一様ランダムに選ぶ

Alice	Bob
$\alpha \xleftarrow{\cup} \mathbb{Z}/(p-1)\mathbb{Z}$ ：Alice の秘密鍵	$\beta \xleftarrow{\cup} \mathbb{Z}/(p-1)\mathbb{Z}$ ：Bob の秘密鍵
$A = g^\alpha \bmod p$ を計算.	$B = g^\beta \bmod p$ を計算.
$K_{\text{Alice}} = B^\alpha \bmod p$ を計算.	$K_{\text{Bob}} = A^\beta \bmod p$ を計算.



- 共有鍵： $K_{\text{Alice}} = B^\alpha = (g^\beta)^\alpha = g^{\beta\alpha} = g^{\alpha\beta} = (g^\alpha)^\beta = A^\beta = K_{\text{Bob}}$
- 安全性：(g, g^α) から α を計算する問題（離散対数問題: DLP ）の困難性を根拠とする.

残念ながら、耐量子でないので、これに置き換わる 耐量子鍵共有を探す必要

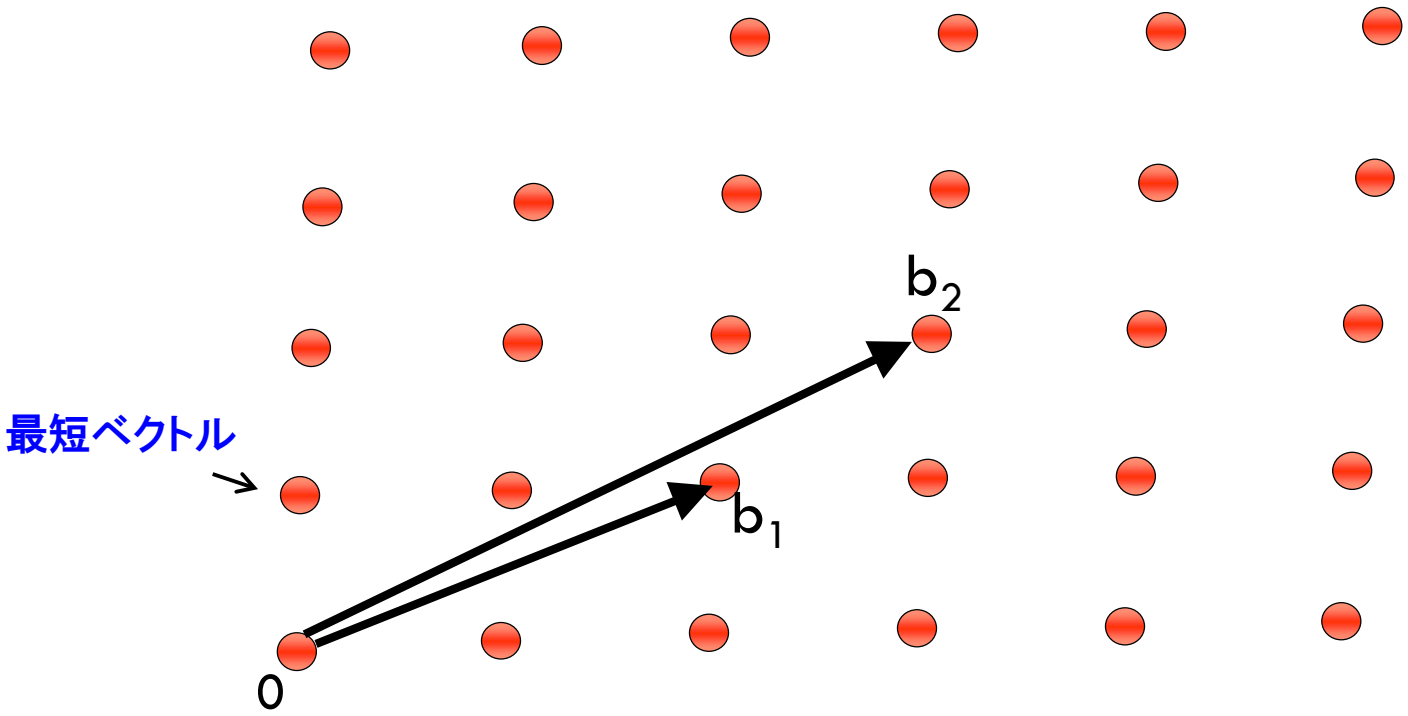
耐量子計算機 公開鍵暗号 の候補

- 量子計算機を用いた Shor の 素因数分解, 離散対数計算 アルゴリズムによって 実用化されている公開鍵暗号, e.g., RSA, (EC)DH, ペアリング暗号 が破られる
- 耐量子計算機 公開鍵暗号 の候補
  - 格子暗号
  - 多変数公開鍵暗号
  - 符号ベース暗号
  - 同種写像暗号
- 量子計算機にも耐性をもつ 困難な数学問題
  - 格子暗号： 最短ベクトル探索問題（SVP）、最近ベクトル探索問題（CVP）
  - 同種写像暗号： 同種写像 核空間 計算問題

耐量子公開鍵暗号 その1
格子暗号

格子 と 最短ベクトル探索問題

線型独立な $b_1, \ldots, b_n \in R^n$ の整係数一次結合 全体(加群)



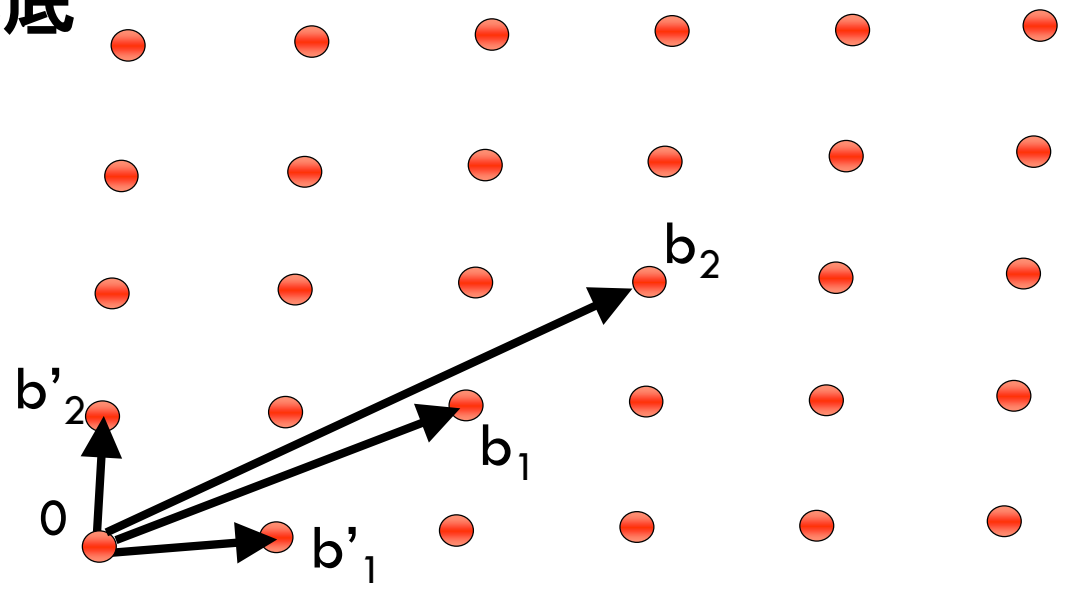
最短ベクトル探索問題 SVP (Shortest Vector Problem)

- 原点以外で**一番短い格子点**を探せ

(暗号使用上は、
$n > 400$ とか)

格子基底　と　基底簡約アルゴリズム

良い（短く直交に近い）基底に変換できれば SVP 計算に有効



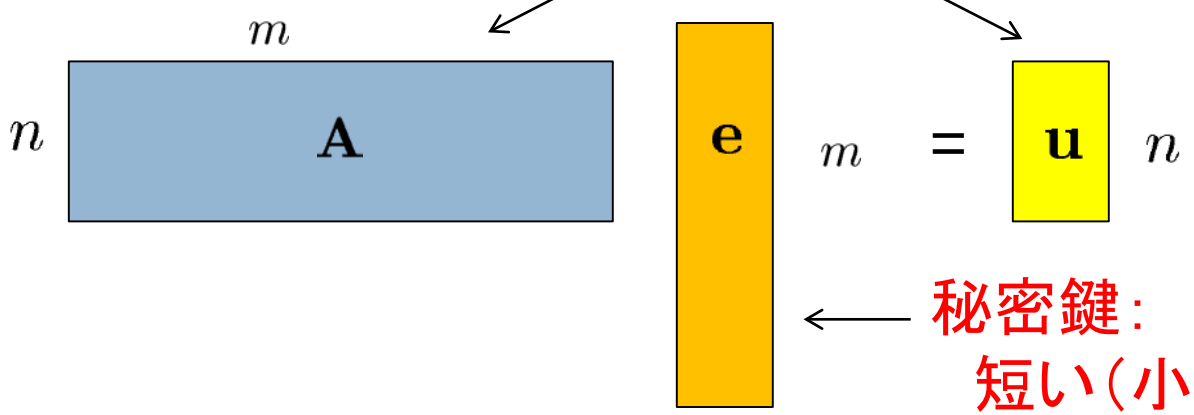
基底簡約アルゴリズム

- [Lenstra,Lenstra,Lovász ‘82]:
  n 次元格子 L に対し, LLL アルゴリズムは n の多項式時間で動き、L 内の 2^n-近似最短ベクトル (SV) を計算する .
- [Schnorr’87]: (概略) $2^{n/d}$ 時間で 2^d-近似 SV を出力.

SVP困難性　と　格子暗号

- SVP は、量子計算機によって効率的に解かれてない
- SVP 困難性に基づく（耐量子）暗号を格子暗号と呼ぶ
  （正確には、SVP 以外の格子問題困難性も考える）
- 以下では、整数 q を法とした $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ を成分とする ベクトル、行列を考える
- 長さを考慮した線型方程式

$$\mathbf{A} \cdot \mathbf{e} = \mathbf{u} \bmod q$$

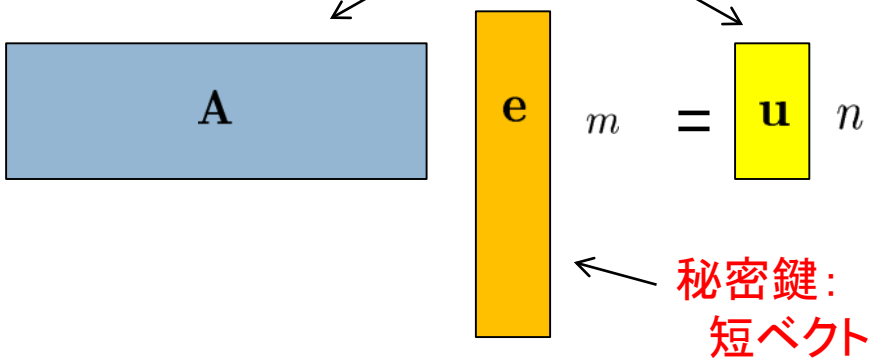


短整数解 (SIS: Short Integer Solution) 問題

- ランダムな $\mathbf{A}, \mathbf{u}$ が与えられて、短い $\mathbf{e}$ を答える

$\Leftrightarrow$ 公開鍵から秘密鍵がばれる！！

$$\mathbf{A} \cdot \mathbf{e} = \mathbf{u} \bmod q$$



- なぜ、これは安全か？

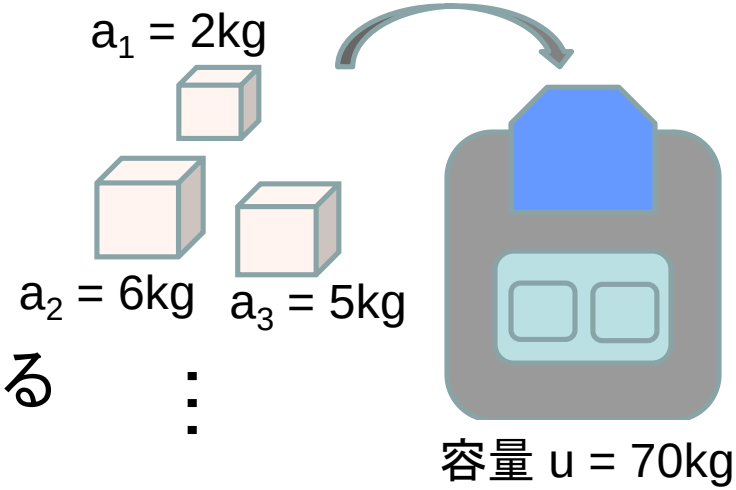
$$\mathcal{L}^{\perp}(\mathbf{A}) := \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{e} = \mathbf{0} \bmod q\}$$

は、格子になっており、$\mathcal{L}^{\perp}(\mathbf{A})$ に対する（近似）SVP 問題は、$\mathbf{A}$ に対する SIS 問題と呼ばれる

$\Rightarrow$ もし、上記の 秘密鍵復元攻撃が成功すれば、SIS 問題が解けるが、SIS 問題は困難なので、上記の秘密鍵は安全に秘匿される

SIS 問題　と　ナップザック問題

- よく知られた組み合わせ的問題の困難性とも関連付けてみる
- ナップザック問題：
  $A = \{ a_i \}, u$　が与えられて、
  $\Sigma\, e_i\, a_i = u$　となる $e_i = 0$ or 1
  を計算する問題

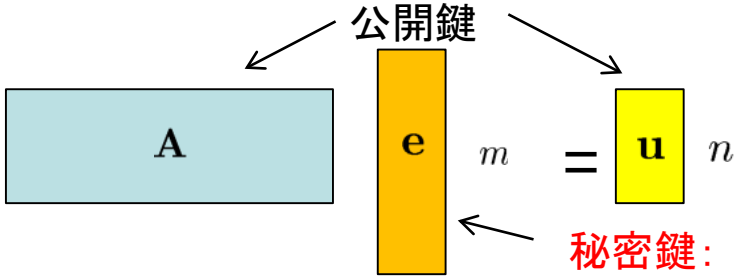


⇨　一般に困難と考えられている

- もし　$\mathbf{e} = (e_1, \ldots, e_m)^{\mathrm{T}}$

の要素が　$e_i \in \{0, 1\}$　なら、

$\mathbf{A} =$ $\mathbf{a}_1$ … $\mathbf{a}_m$　に対して、

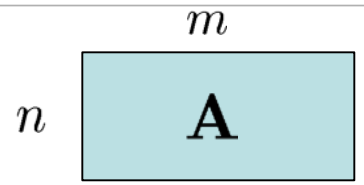


は $\sum_{i=1}^{m} \mathbf{a}_i e_i = \mathbf{u}$ となる $\mathbf{e}$ を計算するﾅｯﾌﾟｻﾞｯｸ問題

⇨　SIS は、その $\mathbf{e}$ に関する条件を緩和した問題とみなせる

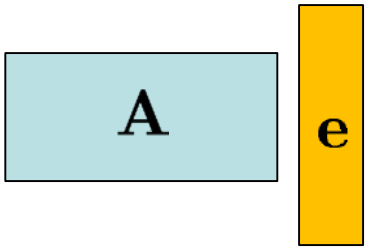
格子ベース 公開鍵暗号

- KeyGen　$\mathbf{A} \xleftarrow{\mathsf{U}} \mathbb{Z}_q^{n \times m}$



秘密鍵: $\mathbf{e} \xleftarrow{\mathsf{R}} D_{\mathbb{Z}^m,r} : \mathbb{Z}^m$ 内の短いベクトル

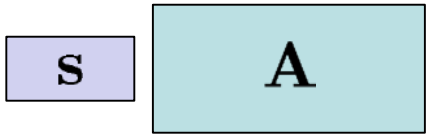
公開鍵: $\mathbf{u} := \mathbf{A} \cdot \mathbf{e} \bmod q$



- Enc($b \in \{0,1\}$)

$\mathbf{s} \xleftarrow{\mathsf{U}} \mathbb{Z}_q^n$　　$\mathbf{x}, x$: 短いベクトル（ノイズ）

$\mathbf{p} := \mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{x} \in \mathbb{Z}_q^m$　　$c := \mathbf{u}^\mathsf{T}\mathbf{s} + x + b\lfloor q/2 \rceil \in \mathbb{Z}_q$



暗号文: $(\mathbf{p}, c)$

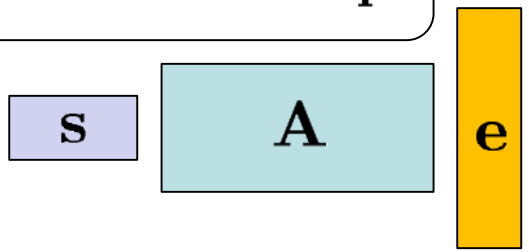
DH 型 近似等式

$\mathbf{u}^\mathsf{T}\mathbf{s} = \mathbf{e}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} \approx \mathbf{e}^\mathsf{T}\mathbf{p}$

- Dec($\mathbf{e}, (\mathbf{p}, c)$)

$b' := c - \mathbf{e}^\mathsf{T}\mathbf{p}$

もし、b' が $\lfloor q/2 \rceil$ より 0 に近ければ、
0 を出力. そうでなければ、1 を出力.



$\mathbf{e}^\mathsf{T}\mathbf{p} = \mathbf{e}^\mathsf{T}(\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{x}) = \mathbf{e}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e}^\mathsf{T}\mathbf{x} = \mathbf{u}^\mathsf{T}\mathbf{s} + \mathbf{e}^\mathsf{T}\mathbf{x}$ ← 短い！！

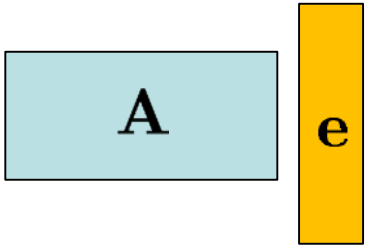
格子ベース 公開鍵暗号の 安全性 ポイント

- KeyGen　$\mathbf{A} \xleftarrow{\mathsf{U}} \mathbb{Z}_q^{n \times m}$

$(\mathbf{A}, \mathbf{u})$ から短 $\mathbf{e}$ の計算は困難

秘密鍵: $\mathbf{e} \xleftarrow{\mathsf{R}} D_{\mathbb{Z}^m, r} : \mathbb{Z}^m$ 内の短いベクトル

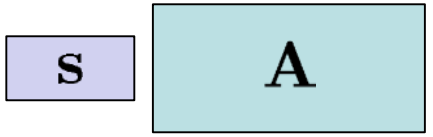
公開鍵: $\mathbf{u} := \mathbf{A} \cdot \mathbf{e} \bmod q$



- Enc(b)

$\mathbf{s} \xleftarrow{\mathsf{U}} \mathbb{Z}_q^n$　　$\mathbf{x}, x$: 短いベクトル(ノイズ)

$\mathbf{p} := \mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{x} \in \mathbb{Z}_q^m$　　$c := \mathbf{u}^\mathsf{T}\mathbf{s} + x + b\lfloor q/2 \rceil \in \mathbb{Z}_q$



暗号文: $(\mathbf{p}, c)$

$(\mathbf{A}, \mathbf{p})$ から $\mathbf{s}$ の計算は困難

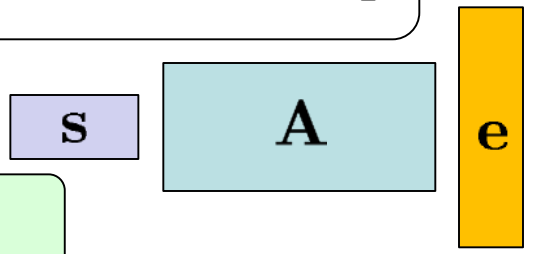
- Dec($\mathbf{e}$, $(\mathbf{p}, c)$)

DH 型 近似等式

$\mathbf{u}^\mathsf{T}\mathbf{s} = \mathbf{e}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} \approx \mathbf{e}^\mathsf{T}\mathbf{p}$

$b' := c - \mathbf{e}^\mathsf{T}\mathbf{p}$

$\mathbf{e}^\mathsf{T}\mathbf{p} = \mathbf{e}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e}^\mathsf{T}\mathbf{x} = \mathbf{u}^\mathsf{T}\mathbf{s} + \mathbf{e}^\mathsf{T}\mathbf{x}$



$\mathbf{e}, \mathbf{x}$ 短いので、 $\mathbf{e}^\mathsf{T}\mathbf{x}$ は十分小さい

格子暗号の新しい安全性向上法
[高島-高安15]

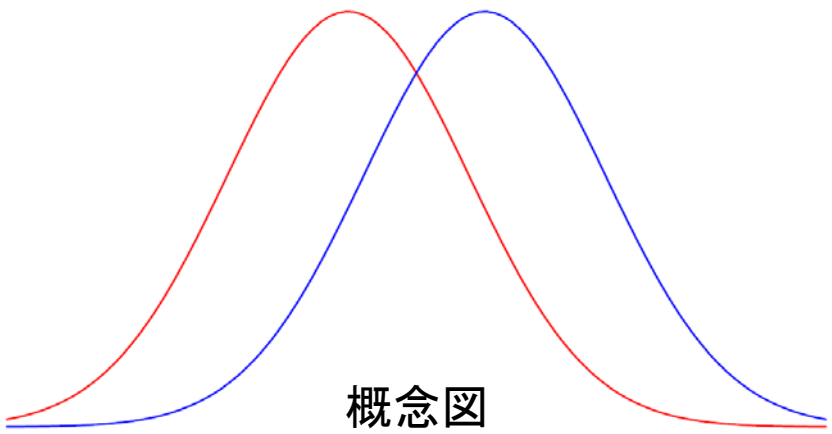
格子暗号の安全性 と ノイズ分布

- 格子暗号の安全性は、短いノイズベクトルをサンプリングする分布に大きく依存している
- その分布を “厳密に” 実装するのは効率が悪く，実用上は “近似的な” 方式で代用することがある.

- 厳密なノイズ分布 と 近似的なノイズ分布が統計的に近接していれば，実装した方式の安全性を証明できる.

我々の成果：ノイズ分布解析法の向上

- 統計的距離（SD）は暗号の安全性証明で、これまで広く用いられてきた.
- 近接度を測る別種の Renyi ﾀﾞｲﾊﾞｰｼﾞｪﾝｽ(RD) が、近年、格子暗号において利用されている.
- RD を用いることで、短いﾃﾞｰﾀｻｲｽﾞで、SD と同等以上の安全性を実現できた！



概念図

- RD は、次数 α というパラメタをもつが、
これまでは、多くの場合、α = 2　という 固定次数 が使われていた.

[高島-高安15]の成果

RD の次数を最適化することで 短いデータサイズ の下で、
高い安全性（タイトな安全性帰着）を達成できることを 示した.

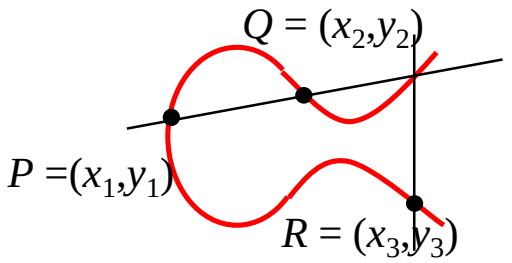
耐量子公開鍵暗号 その2
同種写像暗号

楕円曲線暗号

- DH鍵共有で、整数の乗算の代わりに，楕円曲線上の点の加算(足し算)を用いて暗号演算を定めたものを楕円曲線暗号という.

- 次式で与えられる有限体 $\mathbb{F}_{p^k}\ (p \geq 5)$ 上の楕円曲線 E を専ら考える $(4a^3 + 27b^2 \neq 0)$

$$E : y^2 = x^3 + ax + b \qquad a, b \in \mathbb{F}_{p^k}$$



- $R = P + Q,\ (x_3,y_3) = (x_1,y_1) + (x_2,y_2)$

$$x_3 = \{(y_2-y_1)/(x_2-x_1)\}^2 - x_1 - x_2$$
$$y_3 = \{(y_2-y_1)/(x_2-x_1)\}(x_1-x_3) - y_1$$

- $\alpha \cdot P = \underbrace{P + \ldots + P}_{\alpha}$ ⟷ Diffie-Hellman での g^α と対応

- ECDH (Elliptic Curve Diffie-Hellman):
(P , $\alpha \cdot P$) から α を計算する問題 (ECDLP)の困難性を安全性根拠とする.

しかし、耐量子ではない. 楕円曲線を使った耐量子方式はないか？

楕円曲線間の同種写像

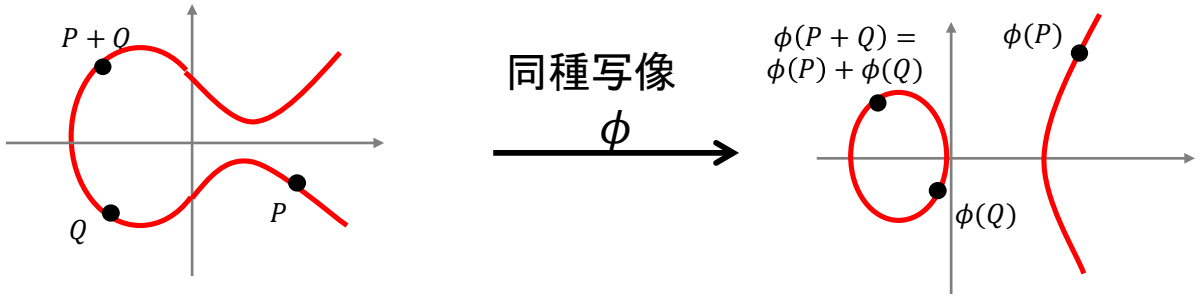
- 2つの楕円曲線 E, E' に対して、同種写像 $\phi: E \to E'$ は、E 上の点 $P = (x, y)$ に対して、有理関数 f, g を使って、

$$\phi(P) = (f(x, y), g(x, y))$$

と、代数的に定義される写像である

- 更に、2点 P, Q に対して、加算構造を保存する（ 線型性 ）

$$\phi(P + Q) = \phi(P) + \phi(Q).$$



- Vélu の公式: 楕円曲線 E とその上の点 R に対して、$< R >$ を核空間とする

同種写像 $\phi_R: E \to E/< R >=: E_R$

を効率的に計算する公式（アルゴリズム）

楕円曲線に関する３種の一方向性関数

○：容易
×：困難

- スカラー倍算

$$(P, \alpha) \quad \bigcirc\!\!\rightarrow \quad (P,\ \alpha P)$$

$$\times\!\!\leftarrow$$

- ペアリング

$$(P, Q) \quad \bigcirc\!\!\rightarrow \quad (P, e(P, Q))$$

$$\times\!\!\leftarrow$$

- 同種写像計算

$$(E, R) \quad \bigcirc\!\!\rightarrow \quad (E,\ E/\langle R \rangle)$$

$$\times\!\!\leftarrow$$

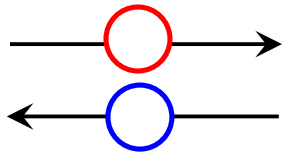
R は $\langle R \rangle$ を生成する点

楕円曲線に関する３種の一方向性関数

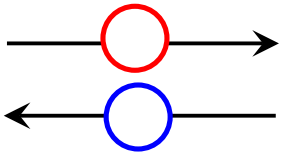
○：容易　　○：量子で容易

×：困難　　×：量子でも困難

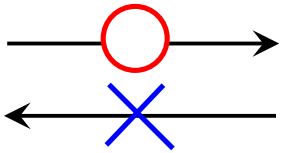
- スカラー倍算

(P, α)  $(P, \alpha P)$

- ペアリング

(P, Q)  $(P, e(P, Q))$

- 同種写像計算

(E, R)  $(E, E/\langle R \rangle)$

R は $\langle R \rangle$ を生成する点

同種写像 核計算 問題に対する解析(解読)アルゴリズム

同種写像核計算問題

2つの同種な楕円曲線 E, E' に対して、$E' = E/\langle R \rangle$ となる 同種写像の核空間生成点 R を計算せよ

	古典計算機による解読時間	量子計算機による解読時間
通常 楕円曲線	$\tilde{O}(\sqrt[4]{p})$	$L_p[1/2, \sqrt{3}/2]$
超特異 楕円曲線	$\tilde{O}(\sqrt{p})$	$\tilde{O}(\sqrt[4]{p})$

$\log p$ の準指数関数: $L_p[\alpha, c] := \exp\left((c + o(1))(\log p)^{\alpha}(\log\log p)^{1-\alpha}\right)$

- 以後は、高い安全性をもつ 超特異楕円曲線 を使った同種写像暗号（特に SIDH: Diffie–Hellman 型鍵共有）を中心に説明する

準指数時間 通常曲線同種写像問題 量子ｱﾙｺﾞﾘｽﾞﾑ [CJS14]

- 同種写像 $\star$ 作用素 [Wat69]

$$\begin{array}{ccccc} * : \mathrm{Cl}(\mathcal{O}_\Delta) & \times & \mathrm{Ell}_{q,n}(\mathcal{O}_\Delta) & \to & \mathrm{Ell}_{q,n}(\mathcal{O}_\Delta) \\ \cup & & \cup & & \cup \\ (\ [\mathfrak{b}], & & j(E) \ ) & \mapsto & j(E') = [\mathfrak{b}] * j(E) \end{array}$$

$\mathrm{Cl}(\mathcal{O}_\Delta)$: 判別式 $\Delta(<0)$ の虚 2 次 整環 (オーダー) のｲﾃﾞｱﾙ類群

$\mathrm{Ell}_{q,n}(\mathcal{O}_\Delta)$: $\mathcal{O}_\Delta$ を自己準同型環にもつ同種な楕円曲線 $/\mathbb{F}_q$ の同型類全体 with $n = \sharp E(\mathbb{F}_q)$

- アーベル群に対する 隠れシフト問題 (Hidden Shift Prob.) に帰着

単射な $f_0, f_1 : A \to S$ such that A : 有限アーベル群、S : 有限集合

$$f_1(x) = f_0(x + s) \quad \text{for some} \quad s \in A$$

にブラックボックスアクセスして、s を計算する問題

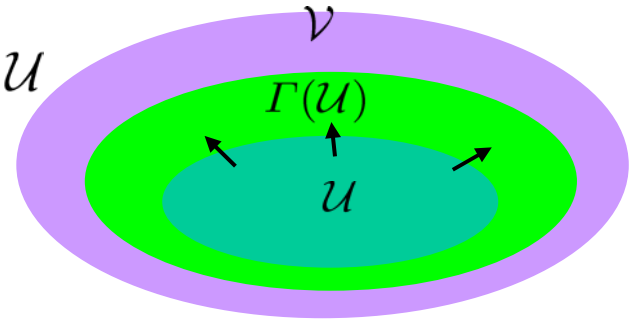
- その隠れシフト問題 を 二面体群 に関する 隠れ部分群問題 (DHSP) に帰着

DHSP には、準指数時間 量子ｱﾙｺﾞﾘｽﾞﾑが知られている (Kuperberg, Regev)

暗号に適した 同種写像グラフ

超特異楕円曲線とその ℓ- 同種写像のなすグラフ（同種写像グラフ）は，計算量理論、組み合わせ論、暗号理論等の応用上で有用な エクスパンダーグラフ になっている.

- $\mathcal{U}$ の境界 $\Gamma(\mathcal{U}) = \{v \in \mathcal{V} \mid \exists u \in \mathcal{U}, \{u, v\} \in \mathcal{E}\} - \mathcal{U}$ のサイズが $\sharp\Gamma(\mathcal{U}) \geq c \cdot \sharp\mathcal{U}$ である時，$G = (\mathcal{V}, \mathcal{E})$ を拡張率 $c > 0$ の エクスパンダーグラフという.



- エクスパンダーグラフ上のランダムウォークは，急速に一様分布に収束する.
  $O(\log(\sharp\mathcal{V}))$ ステップのランダムウォークをさせると、その終点の分布はグラフ上の一様分布を良い精度で近似する（急撹拌性定理）.

- 急撹拌性定理により，多くの頂点集合からの（ほぼ）一様なサンプリングが，少ないランダムネスで可能になる.

- 以後では、Velu の公式を使った同種写像計算を暗号演算に用いるが、その際、急撹拌定理による 効率的な一様サンプリング が安全性上重要である.

エクスパンダーグラフ 隣接行列の特徴

- 以下の特徴づけが，同種写像グラフとの関連では鍵となる．

エクスパンダーグラフの線形代数的な特徴

- G の隣接行列（実対称行列）の固有値を $k > \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{N-1}$ とすると，拡張率 c と次の関係がある．

$$c \geq \frac{2(k-\mu_1)}{3k-2\mu_1} =: f(\mu_1)$$

$f(\mu_1)$ は，$\mu_1 < k$ で μ_1 の狭義単調減少関数であるので，
μ_1 が小さいほど，c に対する大きい下限が得られ，応用上望ましい．

- 拡張率 $c > 0$ を有する k-正則 エクスパンダーグラフの族 $\{G_m\}$ $\mathrm{s.t.}\, \sharp\mathcal{V}(G_m) \to \infty$ が（十分多く）存在することは証明できるが，
それら族の具体的な構成は，Margulis によって始めてなされた (1973)．

Ramanujan グラフ

定理 [Alon-Boppana]

$\{G_m\}$　無限個の連結, k-正則 グラフ　$(\ \sharp\mathcal{V}(G_m) \to \infty\ )$

$\lambda = \max(|\mu_1|, |\mu_{N-1}|)$ とすると,　$\liminf \lambda(G_m) \geq 2\sqrt{k-1}$.

定義 : Ramanujan グラフ

$\lambda \leq 2\sqrt{k-1}$ である 連結 k-正則 グラフ を Ramanujan グラフという.

- Lubotzkey-Phillips-Sarnak, Margulis によって 独立に1988 年頃 Ramanujan グラフ族が具体的に構成された.

定理 [Lubotzkey-Phillips-Sarnak, Margulis, Morgenstern]

任意の素数ベキ q に対し, $k = q + 1$ 正則な Ramanujan グラフが無限個存在し, 具体的に構成できる.

- 最近、Marcus-Srivastava-Spielman により任意の k に対して、k-正則な Ramanujan グラフの存在が示されるなど、新たに進展している.

Pizer の Ramanujan グラフ

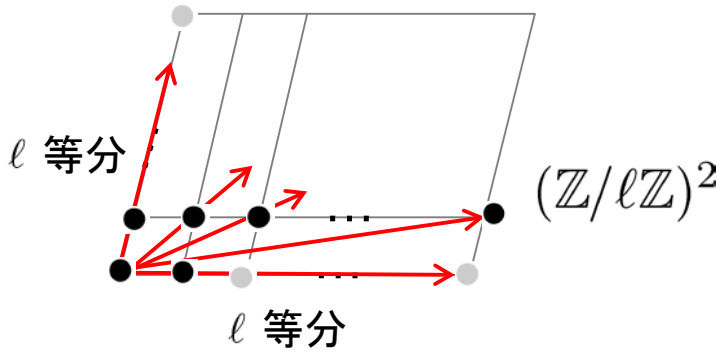
Pizer グラフ $G = G(p, \ell)$

p, ℓ : 2 つの異なる素数

$\mathcal{V}(G)$ は，$\mathbb{F}_{p^2}$ 上定義された超特異楕円曲線の $\overline{\mathbb{F}}_p$ 同型類全体.

$\mathcal{E}(G)$ は，ℓ- 同種写像全体で，双対同種写像を同一視して，
無向グラフとする. $(\ell + 1)$ 正則グラフ.

$$\sharp\mathcal{V}(G) = \lfloor \tfrac{p}{12} \rfloor + \epsilon,\ \epsilon \in \{0, 1, 2\}.$$



$G(p, \ell)$ の隣接行列（ ℓ-th Brandt 行列 ）

レベル p, 重さ 2 のカスプ形式の空間への ℓ-th Hecke 作用素
の表現行列

→ $G(p, \ell)$ は Ramanujan グラフ. 特に連結.

Ramanujan-Petersson予想
で証明済みの結果

（Eichler, Shimura）

Velú の公式

- 楕円曲線 E とその位数 ℓ の有限巡回部分群 C が与えられた時に，
  E/C の定義式と 同種写像 $E \ni (x,y) \mapsto (X,Y) \in E/C$ を与える公式．

$E : y^2 = x^3 + ax + b, \quad Q = (x_Q, y_Q) \neq O_E \in C$ に対し，

$$t_Q := \begin{cases} 2g_Q^x & \text{if } Q \in E[2] \\ g_Q^x & \text{otherwise} \end{cases}, \quad u_Q := (g_Q^y)^2,$$

ただし、

$g_Q^x := 3x_Q^2 + a_4, \quad g_Q^y := -2y_Q,$

$S := (C - \{O_E\}) / \pm 1$ とし，

$t := \sum_{Q \in S} t_Q, \quad w := \sum_{Q \in S} (u_Q + x_Q t_Q), \quad a' := a - 5t, \quad b' := b - 7u$ とする．

$$E/C : Y^2 = X^3 + a'X + b', \quad X = x + \sum_{Q \in S} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right),$$

$$Y = y - \sum_{Q \in S} \left(\frac{2u_Q y}{(x - x_Q)^3} + \frac{(t_Q(y - y_Q) - g_Q^x g_Q^y)}{(x - x_Q)^2} \right).$$

SIDH (Supersingular Isogeny Diffie-Hellman) アルゴリズム (1)

- 小素数 ℓ_A, ℓ_B; 例. $\ell_A = 2, \ell_B = 3$;
- $p+1 = f \cdot \ell_A^{e_A} \ell_B^{e_B}$ となる大素数 p
- $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2 \supseteq (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2$

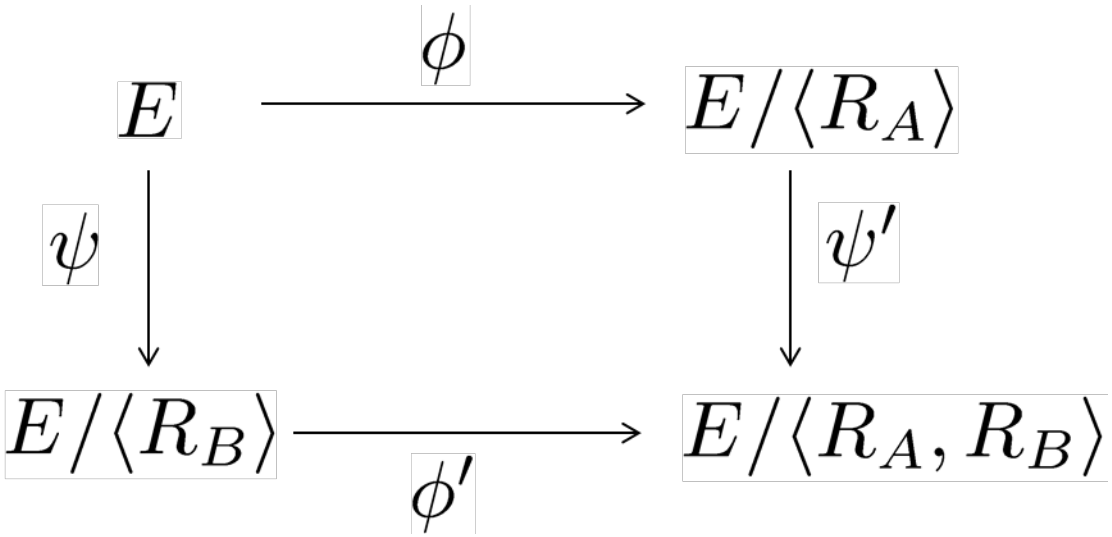
  となる超特異楕円曲線 $E/\mathbb{F}_{p^2}$
- 位数が $\ell_A^{e_A}$, $\ell_B^{e_B}$ の巡回群をそれぞれ核とする同種写像 ϕ, ψ を利用する.
- 下の 可換図式 を Alice と Bob の間の SIDH 鍵交換 に利用する.

$\ker \phi = \langle R_A \rangle \subset E[\ell_A^{e_A}]$

$\ker \psi = \langle R_B \rangle \subset E[\ell_B^{e_B}]$

$\ker \phi' = \langle \psi(R_A) \rangle$

$\ker \psi' = \langle \phi(R_B) \rangle$



SIDH アルゴリズム (2)

- 公開パラメータ: 素数 p （ s.t. $p+1 = f \cdot \ell_A^{e_A} \ell_B^{e_B}$ ），
  超特異楕円曲線, $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2 \supseteq (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2$
  生成元 $E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle$, $E[\ell_B^{e_B}] = \langle P_B, Q_B \rangle$,

Alice	Bob
$m_A, n_A \xleftarrow{\cup} (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^\times$,	$m_B, n_B \xleftarrow{\cup} (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^\times$,
$R_A := m_A P_A + n_A Q_A$,	$R_B := m_B P_B + n_B Q_B$,
$\phi : E \to E_A := E/\langle R_A \rangle$,	$\psi : E \to E_B := E/\langle R_B \rangle$,
$\phi(P_B), \phi(Q_B) \in E_A$	$\psi(P_A), \psi(Q_A) \in E_B$
$\psi(R_A) = m_A\psi(P_A) + n_A\psi(Q_A)$	$\phi(R_B) = m_B\phi(P_B) + n_B\phi(Q_B)$
$K_{\text{Alice}} := E_B/\langle \psi(R_A) \rangle$	$K_{\text{Bob}} := E_A/\langle \phi(R_B) \rangle$

$E_A, \phi(P_B), \phi(Q_B)$ →

← $E_B, \psi(P_A), \psi(Q_A)$

- 共有鍵: $K_{\text{Alice}} = E_B/\langle \psi(R_A) \rangle \simeq E/\langle R_A, R_B \rangle \simeq E_A/\langle \phi(R_B) \rangle = K_{\text{Bob}}$
- 安全性: $E, E_A, \phi(P_B), \phi(Q_B)$ から R_A を計算することの困難性に基づく

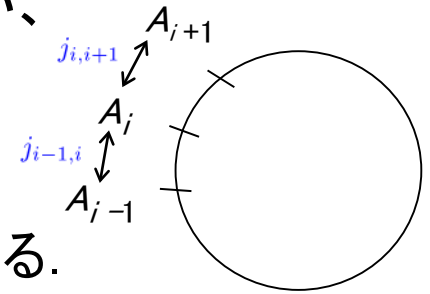
グループ(n 者間)鍵共有 [古川-國廣-高島16]

- n 者 $A_1,\cdots,A_n$ (n: 奇数) 間 の鍵共有
- 公開パラメータ: 素数 p (s.t. $p+1=f\cdot\ell_1^{e_1}\ell_2^{e_2}$),
  超特異楕円曲線, $E(\mathbb{F}_{p^2})\simeq(\mathbb{Z}/(p+1)\mathbb{Z})^2\supseteq(\mathbb{Z}/\ell_1^{e_1}\mathbb{Z})^2\oplus(\mathbb{Z}/\ell_2^{e_2}\mathbb{Z})^2$
  生成元 $E[\ell_1^{e_1}]=\langle P_1,Q_1\rangle,\quad E[\ell_2^{e_2}]=\langle P_2,Q_2\rangle,$

Step 1: 各 A_i はランダムに $m_i,n_i\in(\mathbb{Z}/\ell_\iota^{e_\iota}\mathbb{Z})^\times$ for $\iota=i \bmod 2$ を選び、
$R_i:=m_iP_\iota+n_iQ_\iota$ を計算する. そして $\phi_{A_i}:E\to E/\langle R_i\rangle$
を計算する. その後、A_{i-1}, A_{i+1} と 2者間鍵共有 を行い、

$j_{i-1,i}:=j(E/\langle R_{i-1},R_i\rangle),\quad j_{i,i+1}:=j(E/\langle R_i,R_{i+1}\rangle)$

を計算する. 但し、$j(E):=1728\frac{4a^3}{4a^3+27b^2}$



Step 2: 各 A_i は、 $X_i:=j_{i,i+1}\cdot j_{i-1,i}^{-1}$ を計算し、公開する.

Step 3: 各 A_i は、 $K_i:=j_{i-1,i}^n\cdot X_i^{n-1}\cdot X_{i+1}^{n-2}\cdots X_{i-2}$ を計算する.

- 共有鍵: $K:=K_i=j_{1,2}\cdot j_{2,3}\cdots j_{n-1,n}\cdot j_{n,1}$
  $=j(E/\langle R_1,R_2\rangle)\cdot j(E/\langle R_2,R_3\rangle)\cdots j(E/\langle R_{n-1},R_n\rangle)\cdot j(E/\langle R_n,R_1\rangle)$

MITSUBISHI ELECTRIC
Changes for the Better

ﾍﾟｱﾘﾝｸﾞと同種写像を利用する新しい暗号 [小柴-高島16]

ペアリング と 同種写像 を利用する 新しい暗号 [小柴-高島16]

- SIDH 鍵共有で使われている 超特異楕円曲線上では，効率的なペアリング演算も使えるので，両機能を取り入れた新しい暗号構成フレームワークを提案した.
- その「同種ペアリング群（IPG）」上で 暗号構成に必要な計算困難仮定を新しく定義した.
  - Isog−DBDH 仮定 = Isog−DBDH 問題の困難性
- IPG 上で，量子計算機にも部分的に耐性をもつ IDベース暗号，属性ベース暗号を構成した． Isog−DBDH 問題の困難性を仮定して，それら方式の安全性を証明した.
  - ペアリングだけを用いた暗号構成の時と遜色のない効率性

Weil ペアリング、Tate ペアリング

ペアリング逆計算が困難である双線型ペアリング i.e., $e(\alpha P, \beta Q) = e(P, Q)^{\alpha\beta}$

- 専ら、素数 r に関し、r-ねじれ点群 $E[r] := \{P \in E(\overline{\mathbb{F}}_p) \,|\, rP = O_E\}$ を考える
- 任意の素数 r に対して、*Weil ペアリング* $e_{r,\mathsf{weil}}$ は 位数 r の有理点対から $\overline{\mathbb{F}}_p$ 内の 1 の r 乗根のなす群 μ_r への双線型写像である

$$e_{r,\mathsf{weil}} : E[r] \times E[r] \to \mu_r.$$

Tate ペアリング $e_{r,\mathsf{tate}} : E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \to \overline{\mathbb{F}}^{\times}/(\overline{\mathbb{F}}^{\times})^r.$

μ_r を含む最小の体が $\mathbb{F}_{p^k}$ であるなら、両ペアリング共に、$\mathbb{F}_{p^k}$ に値を取る.

- $P, Q \in E[r]$ に対し、$(f_{r,P}) = r((P) - (\mathcal{O})),\ (f_{r,Q}) = r((Q) - (\mathcal{O}))$ となる有理関数 $f_{r,P}$, $f_{r,Q}$ が存在し、それを使って

$$e_{r,\mathsf{weil}}(P, Q) = f_{r,P}(D_Q)/f_{r,Q}(D_P) \quad \text{となる.}$$

ここで、 $D_P \sim (P) - \mathcal{O},\ D_Q \sim (Q) - \mathcal{O}$ （線形同値）

かつ $\mathrm{Supp}(D_P) \cap (f_{r,Q}) = \mathrm{Supp}(D_Q) \cap (f_{r,P}) = \emptyset.$

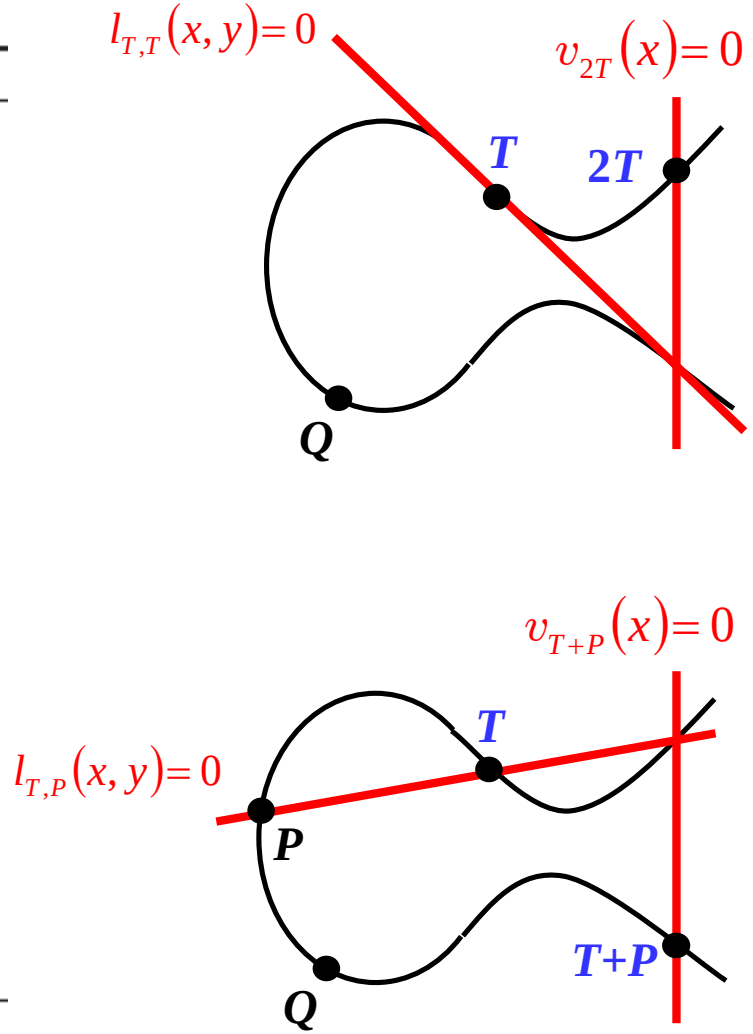
Miller アルゴリズム ($f_{r,P}(Q)$ 計算)

アルゴリズム 1　Miller アルゴリズム

入力：　整数 r　(r の 2 進展開 $= \sum_{j=0}^{L} r_j 2^j, r_L = 1$),
$rP = \mathcal{O}_E, rQ = \mathcal{O}_E$ となる
楕円曲線 E 上の点 P, Q.

出力：　Miller 変数値 $f_{r,P}(Q)$.

$T \leftarrow P, f \leftarrow 1$.
for $j = L - 1$ downto 0 **do**
　T を 2 倍するための直線 $l_{T,T}$ と v_{2T} を計算.
　$f \leftarrow f^2 \cdot l_{T,T}(Q)/v_{2T}(Q)$.
　$T \leftarrow 2T$.
　if r の j 番目のビット r_j が 1 **then**
　　T と P を加算するための直線 $l_{T,P}$ と v_{T+P} を計算.
　　$f \leftarrow f \cdot l_{T,P}(Q)/v_{T+P}(Q)$.
　　$T \leftarrow T + P$.
　end if
end for
f を出力.



- Tate ペアリングを基に効率化された Optimal Ate ペアリング が
より高速に計算できて、通常よく使用される.

暗号学的“ペアリング群”上の DBDH 仮定

- ペアリング演算を有する素数位数 q の群： $(\mathbb{G}, \widehat{\mathbb{G}}, \mathbb{G}_T)$
  - 暗号記述では，しばしば 全て 乗法群 で記述される
  - $e : \mathbb{G} \times \widehat{\mathbb{G}} \to \mathbb{G}_T, \quad g \neq 1 \in \mathbb{G},\ \hat{g} \neq 1 \in \widehat{\mathbb{G}}$
    1. 双線形性： $\forall a, b \in \mathbb{F}_q,\ e\left(g^a, \hat{g}^b\right) = e(g, \hat{g})^{ab}$
    2. 非退化性： $e(g, \hat{g}) \neq 1 \in \mathbb{G}_T$

ランダム $\alpha, \beta, \gamma, \delta \leftarrow \mathbb{F}_q$ に対して，確率的多項式時間チューリング（ppt）マシン $\mathcal{B}$ はランダム $b \leftarrow \{0,1\}$ に対する $\mathcal{X}_b$ を受け取る．ここで，

$$\mathcal{X}_0 := (\, g^{\alpha}, \hat{g}^{\beta}, \hat{g}^{\gamma}, g_T^{\alpha\beta\gamma} \,), \qquad \mathcal{X}_1 := (\, g^{\alpha}, \hat{g}^{\beta}, \hat{g}^{\gamma}, g_T^{\delta} \,).$$

但し， $g_T := e(g, \hat{g})$.

DBDH（Decisional Bilinear Diffie-Hellman）仮定

どんな $\mathcal{B}$ も，b の推測に関して高々無視できる 優位性しか もたない．

同種写像 と ペアリング の適合性

- 同種写像 $\phi: E_0 \to E_1$ と E_0, E_1 上の（Weil）ペアリング $e_{W,0}, e_{W,1}$ の間の適合性（compatibility）が IPG 上の暗号構成の鍵である

$$e_{W,0}(g,h)^{\deg(\phi)} = e_{W,1}(\phi(g),\phi(h)) \quad \text{for } g,h \in E_0$$

- 改めて，$e_0(\cdot,\cdot) \coloneqq e_{W,0}(\cdot,\cdot)^{\deg(\phi)}, e_1(\cdot,\cdot) \coloneqq e_{W,1}(\cdot,\cdot)$ と置くことで，

$$e_0(g,h) = e_1(\phi(g),\phi(h)) \quad \text{for} \quad g \in \mathbb{G}_0, h \in \widehat{\mathbb{G}}_0$$

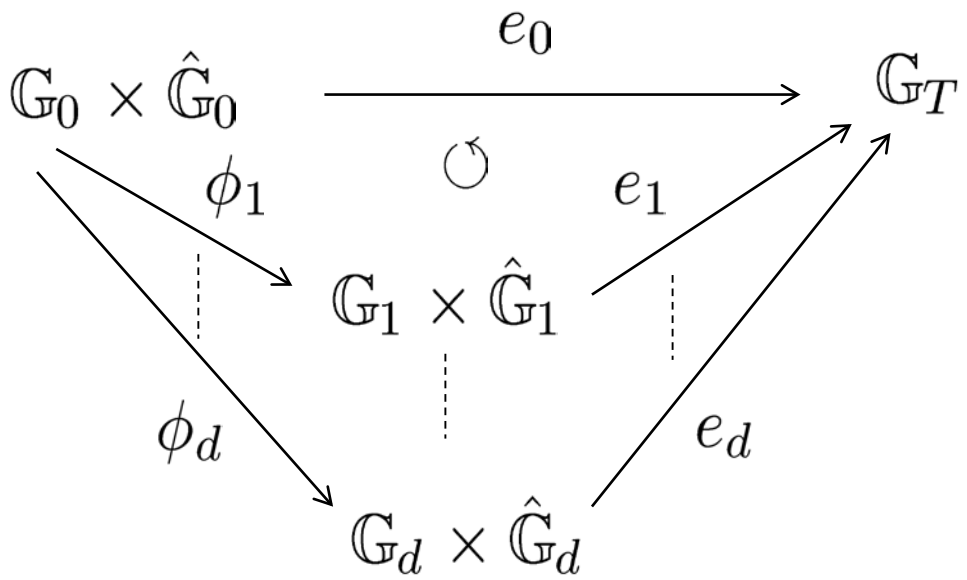
と書ける．ここで，$\mathbb{G}_0 \coloneqq \langle g \rangle, \widehat{\mathbb{G}}_0 \coloneqq \langle h \rangle$は，素数位数巡回群 $\mathbb{G}_0, \widehat{\mathbb{G}}_0 \subset E_0$.

“ 同種ペアリング群（IPG）”

- 同種ペアリング群（IPG）は，適合性（compatibility）を満たす

適合性： 任意の $t \in [d] := \{1, \ldots, d\}$ に対して

$$e_0(g_0, \hat{g}_0) = e_t(g_t, \hat{g}_t) = e_t(\phi_t(g_0), \hat{g}_t)$$



$$e_0(g_0, \hat{g}_0) =$$
$$e_1(g_1, \hat{g}_1) =$$
$$e_1(\phi_1(g_0), \hat{g}_1) =$$
$$\vdots$$
$$e_d(g_d, \hat{g}_d) =$$
$$e_d(\phi_d(g_0), \hat{g}_d)$$
$$= g_T \in \mathbb{G}_T$$

IPG上の Isog-DBDH 仮定

$$\left(\mathrm{pk}^{\mathrm{IPG}} := \left(\left(\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t\right)_{t=0,1}, \mathbb{G}_T\right), \quad \mathrm{sk}^{\mathrm{IPG}} := \phi_1\right) \xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}(1^\lambda, d = 1)$$

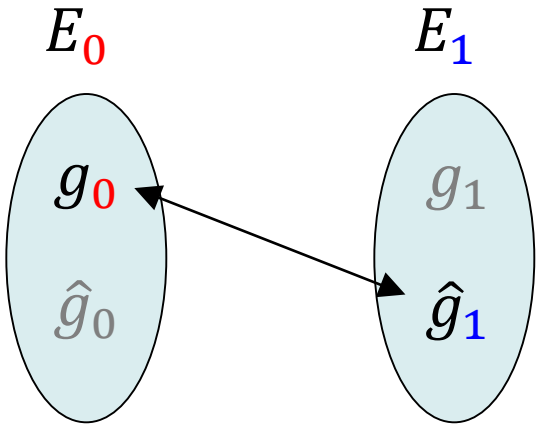
と $\alpha, \beta, \delta \leftarrow \mathbb{F}_q$に対して，ppt マシン $\mathcal{B}$ は ﾗﾝﾀﾞﾑ $b \leftarrow \{0,1\}$ に対する $\mathcal{X}_b$ を受け取る．ここで，

$$\mathcal{X}_0 := (\mathrm{pk}^{\mathrm{IPG}}, g_0^\alpha, \hat{g}_1^\beta, g_T^{\alpha\beta}),$$

$$\mathcal{X}_1 := (\mathrm{pk}^{\mathrm{IPG}}, g_0^\alpha, \hat{g}_1^\beta, g_T^\delta).$$

但し，$g_T = e_0(g_0, \hat{g}_0) = e_1(g_1, \hat{g}_1)$.

$\mathcal{B}$ は，b の推測に関して高々無視できる優位性しか もたない．



異なる楕円曲線上なので
ペアリングできない！

IPG上の qIsog-DBDH 仮定

$\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$: $\mathcal{B}_1$は多項式時間量子攻撃者，$\mathcal{B}_2$は ppt 攻撃者，

$$\left(\begin{array}{c}\mathrm{pk}^{\mathrm{IPG}} := \left((\mathbb{G}_t, \widehat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T\right), \\ \mathrm{sk}^{\mathrm{IPG}} := \phi_1\end{array}\right) \xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}(1^\lambda, 1)$$

state $\leftarrow \mathcal{B}_1\left(\mathrm{pk}^{\mathrm{IPG}}\right)$,

$\alpha, \beta, \delta \leftarrow \mathbb{F}_q$に対して，ppt マシン $\mathcal{B}_2$ は 引継ぎ情報 state と

$b \leftarrow \{0,1\}$ に対する $\mathcal{X}_b$ を受け取る．ここで，

$$\mathcal{X}_0 := (\ \mathrm{pk}^{\mathrm{IPG}},\ g_0^{\alpha},\ \hat{g}_1^{\beta},\ g_T^{\alpha\beta}\ ),$$

$$\mathcal{X}_1 := (\ \mathrm{pk}^{\mathrm{IPG}},\ g_0^{\alpha},\ \hat{g}_1^{\beta},\ g_T^{\delta}\ ).$$

$\mathcal{B}_2$ は，b の推測に関して高々無視できる優位性しか もたない．

IDベース暗号 (IBE)

マスタ公開鍵: pk
マスタ秘密鍵: msk

マスタ公開鍵

公開

pk

鍵発行センタ

ダウンロード

ID に関する
秘密鍵 (sk_{ID})

ID

Bob

Alice

c = Enc(pk, ***ID'***, m)
(***ID'*** と 平文 m に
対する 暗号文)

c

m = Dec(sk_{ID}, c)
(復号可能
iff *ID= ID'*)

（匿名）IDベース暗号

Setup(1^λ): $\left(\mathrm{pk}^{\mathrm{IPG}},\ \mathrm{sk}^{\mathrm{IPG}}\right) \xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}\left(1^\lambda, 1\right)$,

$\mathbb{F}_q$ を id 空間とするハッシュ関数 $H\colon \mathbb{F}_q \to \mathbb{G}_0$ を生成

return 公開鍵 $\mathrm{pk} = \left(\left(\mathbb{G}_t, \widehat{\mathbb{G}}_t, \hat{g}_t, e_t\right)_{t=0,1}, \mathbb{G}_T, H\right)$,

マスタ秘密鍵 $\mathrm{sk} := \phi_1$.

KeyGen(pk, sk, ID): $h_0 := H(\mathrm{ID}) \in \mathbb{G}_0,\ h_1 := \phi_1(h_0)$,

return ID秘密鍵 $\mathrm{sk}_{\mathrm{ID}} := h_1$.

Enc(pk, m, ID): $h_0 := H(\mathrm{ID}) \in \mathbb{G}_0\ \zeta \leftarrow \mathbb{F}_q^\times, c := \hat{g}_1^\zeta$,

$z := e_0(h_0, \hat{g}_0)^\zeta,\ c_T := z \cdot m,$ return 暗号文 $\mathrm{ct}_{\mathrm{ID}} := (c, c_T)$.

Dec(pk, $\mathrm{sk}_{\mathrm{ID}} := h_1,\ \mathrm{ct}_{\mathrm{ID}'} := (c, c_T)$):

if $\mathrm{ID} = \mathrm{ID}'$, $z' := e_1(h_1, c),\ m' := c_T \cdot (z')^{-1},$ return 平文 m'.

匿名 IBE：復号の正しさと安全性

$\mathrm{ID} = \mathrm{ID}'$ の時は,

$$z' = e_1(h_1, c) = e_1(\phi_1(h_0), \hat{g}_1^{\zeta}) = e_1(\phi_1(h_0), \hat{g}_1)^{\zeta}$$

$$= e_0\,(h_0, \hat{g}_0)^{\zeta} = z$$

適合性　$e_1(\phi_1(h_0), \hat{g}_1) = e_0(h_0, \hat{g}_0)$

定理1　提案 IBE は，量子ランダムオラクルモデルで，qIsog-DBDH 仮定の下で，プレチャレンジ量子攻撃者に対して，匿名 ID 安全である.

MITSUBISHI ELECTRIC
Changes for the Better

まとめ

- 量子計算機攻撃に耐性がある暗号 の必要性、
  耐量子 公開鍵暗号 に対する動向（NISTｺﾝﾍﾟﾃｨｼｮﾝ）を説明した.
- その代表的な候補として、次の2つを紹介した.
  - 格子暗号
    - 概要、我々の成果 [高島-高安15]
  - 同種写像暗号
    - 概要、
      我々の成果 [古川-國廣-高島16], [小柴-高島16]

参考文献

- 格子暗号

K. Takashima, A. Takayasu,
“ Tighter Security for Efficient Lattice Cryptography via the Renyi Divergence of Optimized Orders ”, ProvSec 2015

- 同種写像暗号

高島克幸,「 楕円曲線暗号の進展 」
日本応用数理学会論文誌 第25巻 第2号 (2015.6), 117-133
（ 日本数学会ﾋﾞﾃﾞｵｱｰｶｲﾌﾞ： 2014年度 年会 企画特別講演 ）

古川悟、國廣昇、高島克幸、
同種写像を用いたグループ鍵共有、SCIS 2016

T. Koshiba, K. Takashima,
“ Pairing Cryptography Meets Isogeny: A New Framework of Isogenous Pairing Groups ”, ePrint Archive 2016/1138

ご清聴 ありがとうございました。