耐量子暗号について(1)：暗号と鍵共有

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
2025/3/22（土）

自己紹介

- 名前：福岡　尊（ふくおか　たける）
- 肩書
  - 富士通株式会社　データ&セキュリティ研究所　研究員
  - 独立行政法人情報処理推進機構（IPA）　非常勤研究員
- 経歴：ずーっと数学をやって博士をとった→色々あって社会に出た
  - 東工大(~2014)→東大(~2019)→富士通(2019~), IPA(2022~)
- 専門：代数幾何（Fanoとその周辺）
  - 特にdel Pezzoファイブレーションや弱Fano多様体に興味があります（D論 [Fukuoka20]）
- やっていること：**セキュリティに関する研究開発**
  - ブロックチェーン関係の研究開発
    - https://documents.research.global.fujitsu.com/zke
  - 機械学習セキュリティ（Ongoing）

なにを話そうか…

- 会社でやってる自分の研究はデータサイエンスっぽい話，数学も使ってはいる
- が，~~今んとこあんま進捗がない~~ちょっと話すのも手間
- →IPAでやっている内容がいいんじゃないかなと思い，それを話します
- **IPAで何をやってるの→CRYPTRECの事務局をやってます**
  - CRYPTRECとは：日本の暗号の諸々を頑張るプロジェクト
  - 福岡は「どんな暗号がどんな攻撃状況にあるのか」を調べています
- データサイエンス…じゃないかもしれないけど，純粋数学はめちゃくちゃ使う
- **ちょうどいいかなと思ったので暗号について話します．お気軽に聞いてください**

Table Of Contents (Day 1)

安全性を支える数学的問題，現実に使われる暗号たちも外観します

参考：Table Of Contents (Day 2)

3. **なんかすげえコンピュータはDH鍵共有を解くらしい**：量子暗号解読とは
    - 量子計算とは
    - Hidden Subgroup Problem
4. **もっと難しい暗号はないのか？**：耐量子計算機暗号
    - LWE
    - ML-KEM
5. （おまけ）現代の解読：同種写像ベースの暗号解析
    - SIDH
    - CSIDH

1. 暗号ってなに？

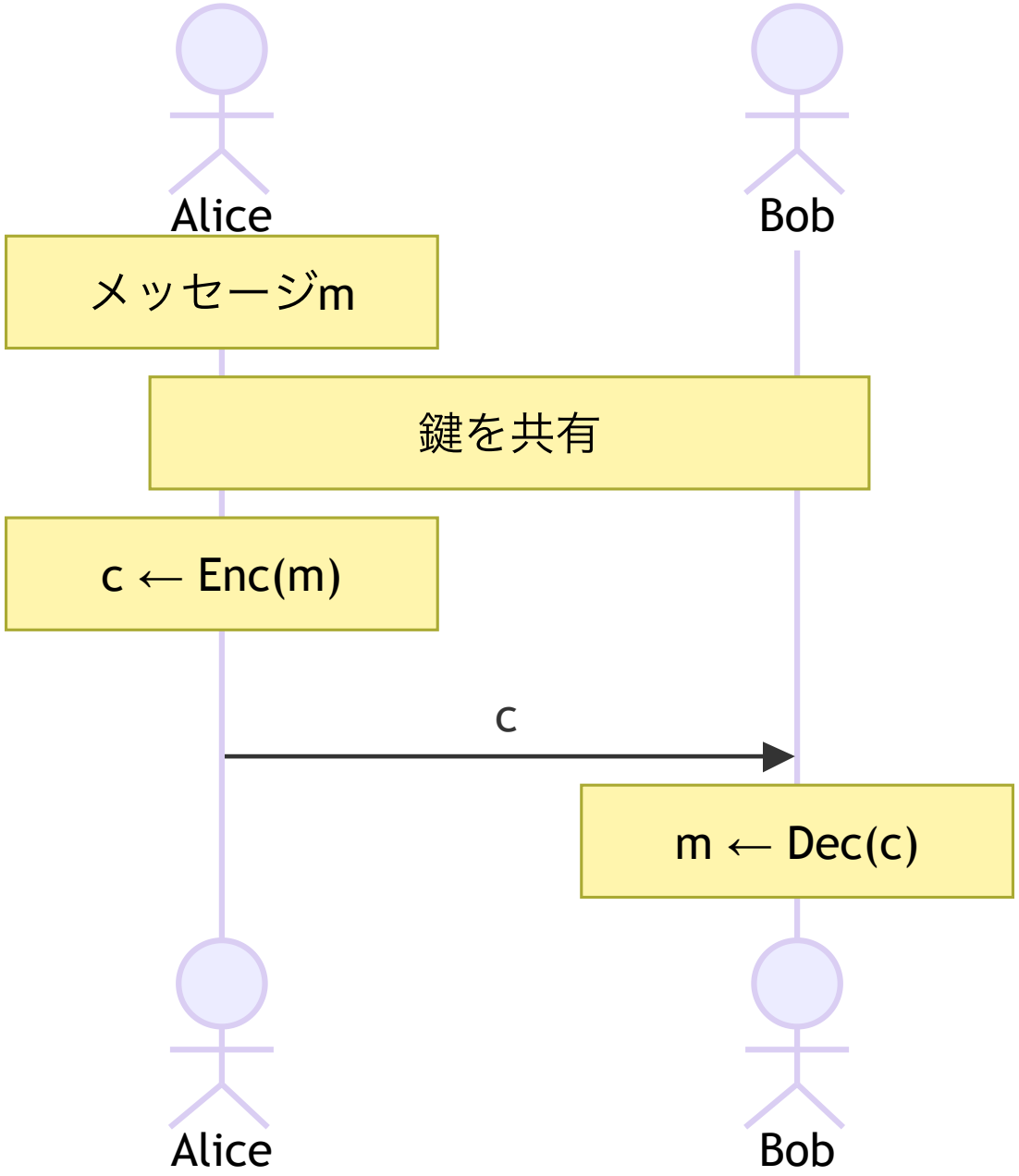
暗号：伝達における漏洩

- 古来から現代にかけて，いろんな機微情報が伝達されてきた.
  - 古代から近代：戦争作戦，政治の人事...
  - 現代：企業秘密，パーソナルデータ，データセット，パラメータ...
- しかし，どんな伝達方法にしろ，盗聴されるかもしれない
  - 古代から近代：会話，手紙，レコード，電話，無線...
  - 現代：インターネット
- →「**他人に漏洩したくない情報をどう伝達するか？**」という課題は昔からある
- 伝達における情報漏洩を防ぐには？

→暗号

暗号のモデル化

- シーン：AliceはBobに秘密のメッセージ m を送信したい.
- 暗号化の手順
  - Alice：m を暗号化：$c := \mathrm{Enc}(m)$.
  - AliceからBob：暗号文 c を送る.
  - Bob：cを復号：$m := \mathrm{Dec}(c)$.



古典暗号の例：シーザー暗号

- シーザー暗号：アルファベット列 m を暗号化する古典的方式
  - AさんとBさんで，"鍵"$k \in \{1, \ldots, 26\}$を共有
  - Aさんはメッセージmをアルファベットをk回ずらして暗号化
  - Bさんはアルファベットをk回戻して復号
  - （名前の由来はGaius Julius Caesar：共和政ローマ末期の執政官・独裁官）
- 例：$k = 1$，$m = \texttt{nagoya␣university}$なら，
- $$c = \mathrm{Enc}_1(m) = \texttt{obhpzb␣vojwfstjuz}$$
- *シーザー暗号の難点*：26 通りの総当たりで解けてしまう．

古典暗号の例：換字式暗号

- →自然な拡張として，置換を鍵とする**単一換字式暗号**も考えられた.
  - メッセージ：$m = (m_1, \ldots, m_l)$.，鍵：$\sigma \in \mathfrak{S}_{26}$
  - 暗号化：$\mathrm{Enc}_\sigma(m) := \sigma.m := (\sigma.m_1, \ldots, \sigma.m_l)$.
  - 復号化：$\mathrm{Dec}_\sigma(m) := \sigma^{-1}.m$.
  - 例：`i␣bake␣an␣apple␣pie` $\to$ `z␣ngpm␣gt␣gbbwm␣bzm`
- *単一換字式暗号の難点*：頻度分析などで解けてしまう
  - 例：「`gt` $\leftarrow$ `an`, `z` $\leftarrow$ `i`では？」「`b`が多い」→`i ?a?? an aXX?? Xi?`→ 💡
- 他の古典暗号：多表式換字（置換を周期的に変更），転置式（文字列の並替），それらの組み合わせなどが用いられたが，解かれたものも多い.
  - 有名な例：アナグラム，エニグマ等（PCで解読できる）

古典暗号の例：ワンタイムパッド（Vernam暗号）

- ワンタイムパッド：**最も安全な暗号の一つ**
- アイデア
  - 文字集合 Ω を $\mathbb{F}_2^k$ に埋め込む：$\Omega \hookrightarrow \mathbb{F}_2^k$.
  - 長さ l のメッセージ $m = (m_i) \in \Omega^l$ は $(\mathbb{F}_2^k)^l$ の元と見れる.
  - →ビット列を暗号化すれば良い.
- 手順：
  - メッセージ$m \in \mathbb{F}_2^n$：ビット列
  - AさんとBさんでランダムに鍵$k = (k_j) \in \mathbb{F}_2^n$を生成，共有.
  - Aさんは以下でメッセージを暗号化：$\mathrm{Enc}_k(m) := m + k \in \mathbb{F}_2^n$.
  - Bさんは以下でメッセージを復号化：$\mathrm{Dec}_k(c) := c + k \in \mathbb{F}_2^n$.

安全性についての理論整備が整っている点で重要

ワンタイムパッドの例

- Ωが小文字のアルファベットなら$b = 5$で埋め込める.
  - $\texttt{a} \mapsto 00001, \texttt{b} \mapsto 00010, \ldots, \texttt{z} \mapsto 11010, \texttt{␣} \mapsto 00000.$
  - 特殊文字として`?`,`!`,`(`,`)`を$11011, 11101, 11110, 11111$に対応させる
- $m := \texttt{nagoya} \mapsto 011100000100111011111010100001 \in \mathbb{F}_2^{30}.$
- 鍵$k := 010110111011010111011111000001 \in \mathbb{F}_2^{30}$
- $\mathrm{Enc}_k(m) = 001010111111101100010101100000.$
  - `io!qk␣`

ワンタイムパッドの安全性 [Shannon49]

- 「固定されたメッセージ$m \in \mathbb{F}_2^n$に対して，一様ランダムに鍵$k \in \mathbb{F}_2^n$を生成する」ならば，生成される暗号文$c := m + k \in \mathbb{F}_2^n$の確率分布は一様である.
  - $\because : \mathbb{F}_2^n \ni k \mapsto \mathrm{Enc}_k(m) \in \mathbb{F}_2^n$ が全単射だから.
- →送られる暗号文は，$\mathbb{F}_2^n$上で生成される乱数と見分けが全くつかない！
- 注意点：**「メッセージ毎に鍵を生成し共有する」必要あり（ワンタイム性）**
  - メッセージの取りうる空間$M \subset \mathbb{F}_2^n$が全体でないなら，
    $M \ni m \mapsto \mathrm{Enc}_k(m) \in \mathbb{F}_2^n$は一様ではない.
  - →複数のメッセージ$m_1, \ldots, m_N$について，
    - $(m_1 + k_1, m_2 + k_2, \ldots, m_N + k_N)$は一様乱数列だが
    - $(m_1 + k, m_2 + k \ldots, m_N + k)$は一様ではない.
  - →情報理論的な安全性は保てない

現代暗号の例：共通鍵暗号AES

- *ワンタイムパッドの難点*：鍵がメッセージと同じ大きさになる
  - 例：4GBの動画を暗号化するとき，パスワードも4GB必要
  - （最高の安全性を持つ方式なので，短い平文を安全に伝える際には使われる）
- **AES（Advanced Encryption Standard）**；現在最もよく使われている共通鍵暗号
  - 鍵の長さは128/192/256ビット
  - メッセージを128ビット事に区切って処理するブロック暗号の一種

まとめ

名前	暗号文	鍵	暗号・復号	安全？
換字式暗号・シーザー暗号	文字列	置換群の元	置換で作用	×
アナグラム	文字列	置換群の元	置換で並替え	×
ワンタイムパッド	ビット列	ビット列	排他的論理和	◯
AES	文字列	文字列	AES	◯（依然として解読研究は盛ん）

共通鍵暗号と鍵共有

- 今まで見てきた方式は，共通の鍵を使うので，**共通鍵暗号**と呼ばれる.
- 共通鍵暗号を使うには，**鍵を共有する必要がある**.
  - 例：ワンタイムパッドはメッセージと同じ大きさの鍵を共有する必要あり.
  - →そもそも「メッセージと同じ大きさの鍵を共有できる」なら，その伝達経路を使えばいいんじゃないの？
  - AESでも「どう鍵共有するか？」は別途考える必要ある
- 古くはあの手この手で鍵を手渡しし，物理的に共有してきた.
  - 直接手渡し，スキュタレー，復号機械...

現代では，どうやって秘密を共有するのか？

→鍵共有方式

2. 鍵共有ってなに？

2-1. 有限体Diffie-Hellman鍵共有

鍵を共有してみよう（セットアップ）

- 実際これから，講演者とあなたの間で鍵を共有してみます.
- まず，1から10の好きな数字 a を選んでください：
  - （小さい数字だとあとで計算が楽です）

$$a \in \{1, 2, \ldots, 10\}.$$

- aは誰にも教えてはいけません.
- 福岡も，好きな数字bを選びました.

鍵を共有してみよう（公開情報の生成）

- 選んだ数字aを使って，2^aを23で割った余りAを計算してください：

$$A \equiv 2^a \pmod{23}.$$

- Aは誰に教えてもらっても構いません.
- 福岡も同様に，余り$B \equiv 2^b$を計算したところ，$B = 3$となりました.

鍵を共有してみよう（秘密の共有）

- 福岡の余りは$B = 3$です．B^aを23で割った余りCを計算してみてください：

$$C \equiv B^a \pmod{23}.$$

- 福岡も同様に，あなたの余りAについて，$A^b \pmod{23}$を計算します：

$$C \equiv A^b \pmod{23}$$

- （あなたの余りが$A = 8$だったなら，$C = 4$です）．

福岡とあなたで，同じ数字Cを共有できました．

何が起きたのか？

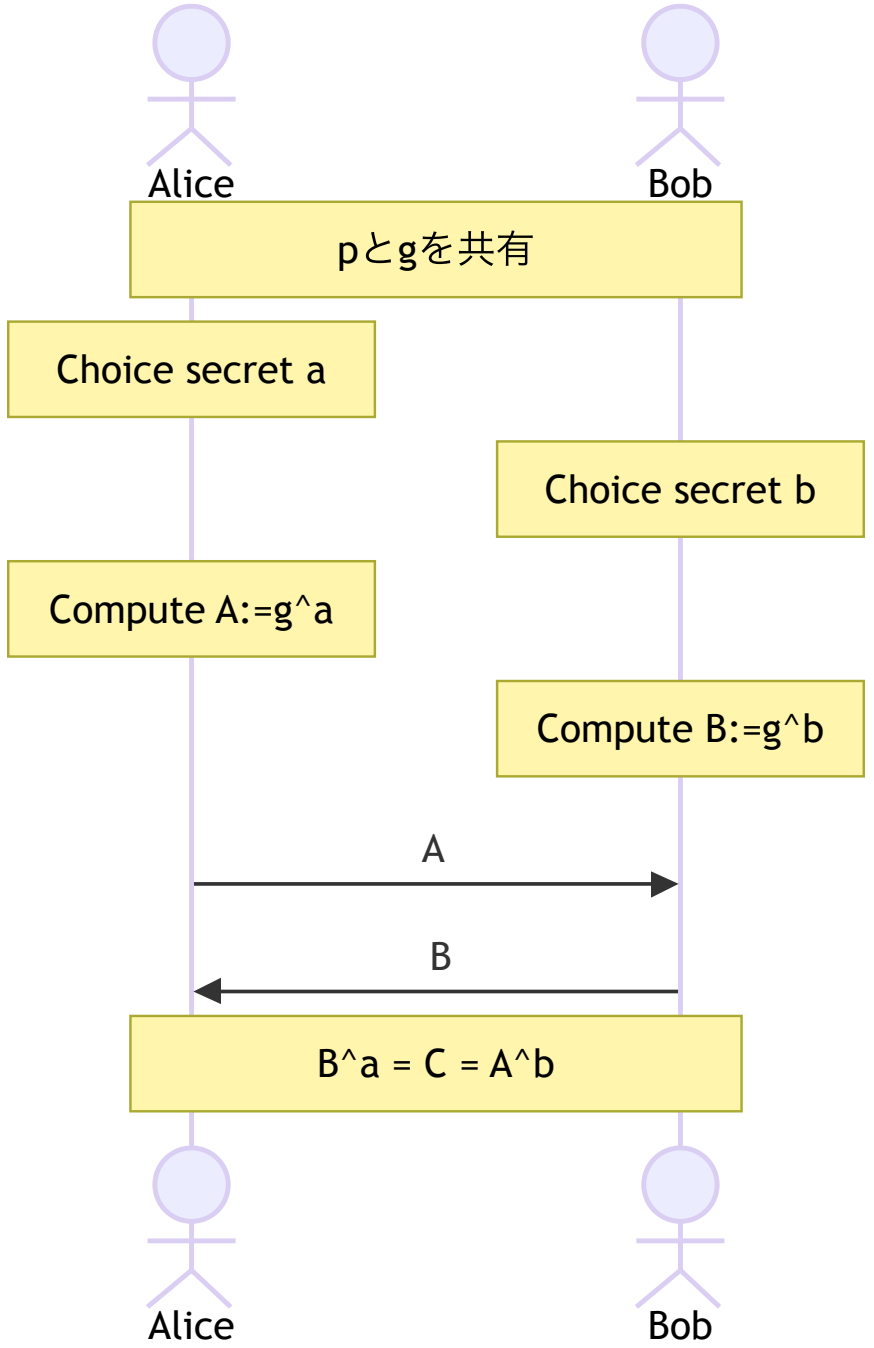
- 素数$p = 23$について，$G := \mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$は巡回群.
- $g = 2 \in G$を固定する
  - $5^2 \equiv 2 \pmod 2$なので，gは位数$q = 11$の元である.
- Alice（あなた）：$a \in G^\times$を秘密情報，$A := g^a$を公開情報とする.
- Bob（福岡）：$b \in G^\times$を秘密情報，$B := g^b$を公開情報とする.
- Alice：秘密情報aと，Bobの公開情報Bについて，$C := B^a$を計算.
- Bob：秘密情報bと，Aliceの公開情報Aについて，$C := A^b$を計算.

$$B^a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = A^a.$$

→計算結果は同じなので，数値を共有できる

Diffie-Hellman鍵共有（DH鍵共有）

- 前提：AliceさんとBobさんは数値Cを秘密裏に共有したい
- セットアップ：以下の情報(p, q, g)を固定する.
  - p, q：奇素数 s.t. $p = 2q + 1$（先程は $p = 23, q = 11$）.
  - $g \in \mathbb{F}_p^\times$：位数$q$の元. $G := \langle g \rangle \simeq \mathbb{Z}/q\mathbb{Z}$.
- 共有手順：右図



DH鍵共有の解読(1)：秘密鍵の解読とDLP

- 公開情報$A = g^a$から，秘密のaがわかるのでは？
  - 例えば$g = 2$，$A = 8$だったら，$a = 3$だと見抜けるのでは？

この秘密を解読するには，

$$\exp_g \colon \mathbb{Z}/q\mathbb{Z} \ni x \mapsto g^x \in G$$

の逆写像を計算できればよい：

$$\log_g \colon G \to \mathbb{Z}/q\mathbb{Z}.$$

離散対数問題（DLP）
位数nの巡回群Gと，生成元$g \in G$について，$\log_g \colon G \to \mathbb{Z}/n\mathbb{Z}$を計算せよ．

例：さっきの我々のケース

有限体離散対数問題（有限体DLP）
素数p, $g \in \mathbb{F}_p^\times$, $y \in \langle g \rangle$について, $\log_g y$を計算できるか？

- 計算例：$p = 23$, $g = 2$（先ほどの例）
  - $y = 8$については, $\log_2 8 = 3$である.
  - $y = 3$については, $\log_2 3 = \ldots$
    - $2^4 = 16, 2^5 = 32 \equiv 9, 2^6 = 18, 2^7 = 36 \equiv 13, 2^8 = 26 \equiv 3.$
    - →8である
- gの位数が11なので, 当たり前ではあるが, 10回計算すればわかる.

DLP予想

有限体離散対数問題予想（有限体DLP予想，もしくは単にDLP予想）
素数p, q，位数qの元$g \in \mathbb{F}_p^\times$，$y \in \langle g \rangle$について，$\log_g y$を計算するのは"困難"であろう

- ここでいう"困難"とは，「yのビット長$\log_2 y$について多項式時間のアルゴリズムがない」という意味
  - 「qのビット長$\log_2 q$についての多項式時間アルゴリズムがない」と同じ
- 先ほどの総当たりは$q - 1 = 2^{\log_2 q} - 1$回の計算が必要→多項式時間ではない

今のところDLPは解かれていないが，「絶対解けない」とも示されていない

注意：DLPの難しさは群の表現に依存する

DLPが簡単なケースも見ておく.

離散対数問題（DLP）
位数nの巡回群Gと，生成元$g \in G$について，$\log_g \colon G \to \mathbb{Z}/n\mathbb{Z}$を計算せよ.

Claim. $G = (\mathbb{Z}/n\mathbb{Z}, +)$（"$\simeq$"**ではなく"="**），$g \in G$を生成元としたとき，DLPは簡単に解ける.

Proof. この場合，全単射$\exp_g$は以下の様：$\exp_g \colon \mathbb{Z}/n\mathbb{Z} \ni x \mapsto x \cdot g \in G$.
よって$\log_g(y) = y/g = y \cdot g^{q-2}$→二分累乗法で$O(\log q)$オーダーで計算可. □

Remark. 有限体DLPで対象となる群は，$\mathbb{Z}/n\mathbb{Z}$と"同型"だが，"="ではない

群の同型類 *ではなく*，群の表現が大事

DH鍵共有の解読(2)：共有情報の漏洩

- 公開情報$A = g^a$と$B = g^b$から，AliceとBobの共有情報$C = g^{ab}$が見抜けるかも？
  - 例えば$p = 23$，$g = 2$，$A = 8$，$B = 3$だったら，$C = 4$と見抜けるかも？

Computational Diffie-Hellman問題（CDH問題）
素数位数巡回群G，$g, A, B \in G^\times$について，$g^{\log_g A \log_g B}$を計算できるか？

有限体CDH予想
$G \subset \mathbb{F}_p^\times$であるとき，CDH問題を解くのは"困難"であろう

DH鍵共有の解読(3)：共有情報のランダムネス

- ワンタイム暗号の特徴として，「*暗号文は乱数と見分けがつかない*」という性質があった.
- Diffie-Hellman共有においてはどうだろうか？

Decisional Diffie-Hellman問題（DDH問題）
素数位数巡回群G，$g \in G^\times$について，以下の二つの分布を見分けよ：

- $(g^a, g^b, g^{ab}) \in G^3$, where a, b are uniform on $\{1, \ldots, q-1\}$.
- $(g^a, g^b, g^c) \in G^3$, where a, b, c are uniform on $\{1, \ldots, q-1\}$.

有限体DDH予想（もしくは単にDDH予想）（Naive form）
$p = 2q + 1$，$G = \{x^2 \mid x \in \mathbb{F}_p^\times\}$であるとき，DDH問題は"困難"だろう

問題の関係性

- DLPが解けるならCDHは解ける
  - $\because \log_g A$と$\log_g B$を計算できるなら，$g^{\log_g A \log_g B}$も計算できる.
- CDHが解けるならDDHは解ける
  - $\because$ CDH問題が解けるなら，$(A, B, C) \in G^3$について，$g^{\log_g A \log_g B}$がCと一致するかをチェックすれば良い.
- また，DLPが解けないことが示せれば（つまりDL予想が示せれば），P≠NPが従う
  - $\{1, \ldots, q-1\} \ni x \mapsto g^x \in G^\times$の一方向性に他ならない.

よって,

DDH予想 $\Rightarrow$ CDH予想 $\Rightarrow$ DL予想 $\Rightarrow$ P≠NP予想

未解決問題たち

- P $\neq$ NP予想は有名な未解決予想（ミレニアム予想）.
- したがって，DDH，CDH，DLは全て未解決問題である.
- また，逆が言えるかもよくわかっていない：
  - P $\neq$ NP $\Rightarrow$ DL予想：不明
  - DL予想 $\Rightarrow$ CDH予想：不明
  - CDH予想 $\Rightarrow$ DDH予想：不明（CDHを満たしそうだが，DDHを満たさない例が知られており，おそらく真に強いと言われている）

現実社会でのDH鍵共有

それでも，Diffie-Hellman鍵共有はTLS/SSL通信でめちゃくちゃ使われている.

- TLS/SSLとは：インターネットでお互いに暗号通信を行うための仕様・フォーマットのこと．オンライン取引，SNSなどで日常的に使う
- 我々は日常的に，Diffie-Hellmanで共有鍵を導出し，AESで暗号文をやり取りしている：
- 実際に使われる素数pたち（参考：[RFC7919]）
  - 2048ビット：$p = 2^{2048} - 2^{1984} + \left(\lfloor 2^{1918} \cdot e \rfloor + 560316\right) \cdot 2^{64} - 1.$
  - 3072ビット：$p = 2^{3072} - 2^{3008} + \left(\lfloor 2^{2942} \cdot e \rfloor + 2625351\right) \cdot 2^{64} - 1.$
  - 4096ビット；$p = 2^{4096} - 2^{4032} + \left(\lfloor 2^{3966} \cdot e \rfloor + 5736041\right) \cdot 2^{64} - 1$

まとめ

- DL予想：「**秘密鍵が漏洩しないこと**」を保証する予想.
- CDH予想：「**共有物が漏洩しないこと**」を保証する予想.
- DDH予想：「**共有物が推定されないこと**」を保証する予想.
- 上の予想は全て未解決であり，全てP $\neq$ NPを系に持つめちゃくちゃに強い仮定.
- それでも世の中では「きっと大丈夫だろう」ということで使っている.

2. 鍵共有ってなに？

2-2. 楕円曲線Diffie-Hellman鍵共有

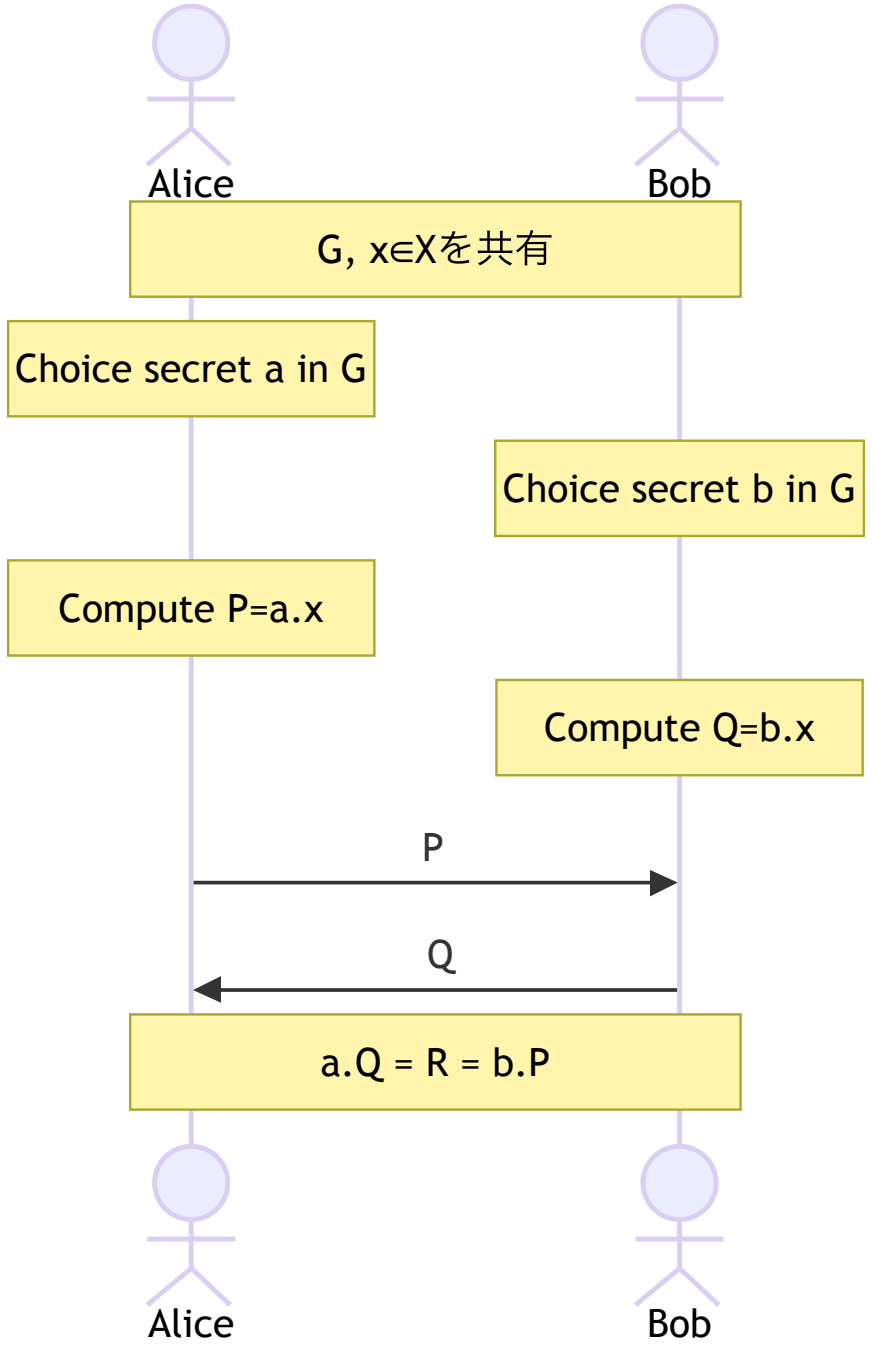
Diffie-Hellmanの一般化

- 素数qについて，群$G \simeq \mathbb{Z}/q\mathbb{Z}$のDLPの難しさは，$G$の表現に依存していた
  - $\mathbb{Z}/q\mathbb{Z} \curvearrowright (\mathbb{F}_q, +); a.\, x := a \cdot x$：簡単だった.
  - $\mathbb{Z}/q\mathbb{Z} \curvearrowright (\mathbb{F}_q^\times, \cdot); a.\, g := g^a$：難しそう.
- →Gの作用の言葉で問題を一般化できる

Group action Diffie-Hellman（GADH）

- G：アーベル群.
- $x \in X$：点付き対象.
- $G \curvearrowright X$：忠実な作用.

- Alice：秘密$a \in G$, $P = a.x$を公開, $R = a.Q$を共有
- Bob：秘密$b \in G$, $Q = b.x$を公開, $R = b.P$を共有
- $a.Q = (ab).P = (ba).P = b.P$



GADHの困難性

DLP/CDH/DDHの一般化 [Couveignes06], [Montgomery-Zhandry22]

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

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

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

- (GADLP) Compute $\mathrm{DL}_x(y)$ for given $y \in \mathrm{Orb}(x)$.
- (GACDH) For given $y_1, y_2 \in X$, compute $z = (\mathrm{DL}_x(y_1) \cdot \mathrm{DL}_x(y_2)).\,x$
- (GADDH) Distinguish the following two distributions on $\mathrm{Orb}(x)^3$:
  - $(a.\,x, b.\,x, (ab).\,x)$, where a, b are uniform on $\{1, \ldots, q-1\}$.
  - $(a.\,x, b.\,x, c.\,x)$, where a, b, c are uniform on $\{1, \ldots, q-1\}$.

Example: 有限体DDH/CDH/DDH

有限体DLP/CDH/DDH

$x \in X$, G, $G \curvearrowright X$を以下のように決める.

- $\mathbb{F}$: finite field.
- $x \in X := \mathbb{F}^\times$: order q.
- $G = \mathbb{Z}/q\mathbb{Z}$.
- $G \curvearrowright \mathbb{F}^\times$: $a.\, x := x^a$.

Remark. $\mathbb{F} = \mathbb{F}_p$, $p = 2q + 1$, p, qが素数なら, 今まで見てきたDiffie-Hellman.

他にもどんなのがあるだろうか？

Example: 簡単な例

$G,\ x \in E,\ G \curvearrowright E$を以下のように決める.

- $G = \mu_m = \{e^{2\pi i/k} \mid k = 1, \ldots, m\} \subset S^1, \zeta := e^{2\pi i/m}.$
- $E = \mathbb{C}^n \setminus \{0\}. x = (x_1, \ldots, x_n) \in E.$
- $w = (w_1, \ldots, w_n) \in \mathbb{Z}$: nと互いに素な整数列
- $G \curvearrowright E$: $g.(x_1, \ldots, x_n) = (g^{w_1}x_1, \ldots, g^{w_n}x_n)$

- これには以下の問題がある.
  - 誤差：コンピュータではEの元は浮動小数点で丸め処理→誤差が発生しうる
  - 数学的に簡単：$\mathrm{DE}_x(\zeta^a) = x \cdot \mathrm{Diag}(\zeta^{aw_1}, \ldots, \zeta^{aw_n}) \Rightarrow \mathrm{DL}_x(y)$は計算可

→離散空間に複雑に作用させる必要がありそうだ

例：高次元拡張[Menezes-Wu98].

DLP/CDH/DDH for $\mathrm{GL}_n(\mathbb{F})$

G, $x \in E$, $G \curvearrowright X$を以下のように決める：

- $G = \mathbb{Z}/q\mathbb{Z}$.
- $\mathbb{F}$：finite field
- $M \in X := \mathrm{GL}_n(\mathbb{F})$: order q.
- $G \curvearrowright \mathrm{GL}_n(\mathbb{F})$: $a.\, M := M^a$.

ただ，これは結局有限体DLPに帰着できることが知られている

→群を大きく変えないと行けない

Example: アーベル群

Xそれ自身をアーベル群としよう．整数aについて$[a]\colon X \to X$をa倍写像とする．

G，$x \in X$，$G \curvearrowright X$を以下のように決める．

- $n \in \mathbb{Z}_{>0}$.
- $X[n] := \mathrm{Ker}([n]\colon X \to X)\colon \mathbb{Z}/n\mathbb{Z}$-module.
- $x \in X[n] \setminus \{0_X\}$.
- $G \subset (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a \in G$，$y \in X[n]$について，$a.y = [a]y$.

$(X, +_X) = (\mathbb{F}_p^\times, \cdot)$の場合が有限体DLP.

離散空間で演算がある程度複雑→有限体上のアーベル多様体はどうだろうか？

Example: アーベル多様体

G, $x \in X$, $G \curvearrowright X$を以下のように決める.

- $\mathbb{F}$: finite field. $n \in \mathbb{Z}_{>0}$. A: abelian variety over $\mathbb{F}$.
- $X := A[n](\mathbb{F})$.
- $x \in X \setminus \{0_A\}$.
- $G \subset (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a \in G$, $y \in X$について, $a.y = [a]y$.

これの1次元版が**楕円曲線Diffie-Hellman鍵共有**

楕円曲線Diffie-Hellman

ECDLP/ECCDH/ECDDH G, $x \in X$, $G \curvearrowright X$を以下のように決める.

- $\mathbb{F}$: finite field. $n \in \mathbb{Z}_{>0}$. E: elliptic curve over $\mathbb{F}$.
- $X := E[n](\mathbb{F})$, $x \in X \setminus \{0_E\}$.
- $G \subset (\mathbb{Z}/n\mathbb{Z})^\times$.
- $a \in G$, $y \in X$について, $a.y = [a]y$.

この方式を使った鍵共有を, **楕円曲線Diffie-Hellman鍵共有（ECDH）**と呼ぶ.

現代社会での鍵共有方式は, 有限体DHとECDHの二大巨頭

楕円曲線とはなにか？

Definition.
体k上の*楕円曲線*Eとは，滑らかな射影的代数曲線であって，種数1かつk-値点$O_E \in E(k)$を持つものである.

Fact. (E, O_E)をk上の楕円曲線とする.

- 線形系$|3O_E|$は$\mathbb{P}^2_k$へのk上の閉埋め込みを定める.
- kの標数が2でも3でもないなら，Eは以下で定義できる（Weierstrass form）：

$$E = (Y^2Z - (X^3 + aXZ^2 + bZ^3)) \subset \mathbb{P}^2_k = \operatorname{Proj} k[X, Y, Z].$$
$$O_E = [0 : 1 : 0]$$
$$E \setminus \{O_E\} = (y^2 = x^3 + ax + b) \subset \mathbb{A}^2_k$$

- Eはk上のアーベル群スキームになる．特にk-値点$E(k)$はアーベル群である.

なぜ楕円曲線なのか？

群作用のDiffie-Hellmanで必要な要件を考えると...

- 要件1：計算誤差が発生しない→Xは離散的であるほうが望ましい
  - $\mathbb{C}$上の楕円曲線などでは計算誤差が発生する
  - 有限体上の楕円曲線なら，計算誤差が発生しない
- 要件2：作用の計算がexplicitにわかっていて，効率的に計算できる
  - 2次元以上のアーベル多様体は，具体的な和演算の書き下しが困難
  - 有限体上の楕円曲線の和演算は座標で効率的に書き下せる

これらの条件をECDHは満たす．しかし依然として，DL予想，CDH予想，DDH予想は未解決であり，全てP $\neq$ NPを系に持つめちゃくちゃに強い仮定である．

実際のECDH

- Eを$\mathbb{F}_p$上の楕円曲線，$x \in X = E(\mathbb{F}_p)$を$n$-torsion pointとする.
- 安全性のためにnは奇素数かつ，効率性のためにcofactor $h := \#E(\mathbb{F}_p)/\operatorname{Orb}(x)$はなるべく小さいことが要求される.
  - Hasse bound
    $|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}$

name	$\lceil \log_2 p \rceil$	cofactor
secp256r1	256	1
secp384r1	384	1
secp521r1	521	1
x25519	255	8
x448	448	4

- 参考：[RFC8422], [SECG-SEC2], [RFC7748]

有限体DHとECDHの比較

- 現状の解読手法で解読にかかる計算量を，"ビットセキュリティ"と言う．

鍵共有方式	ビットセキュリティ	公開情報の長さ
ffdhe2048	103	2048
ffdhe3072	125	3072
ffdhe4096	150	4096
secp256r1	128	512
secp384r1	192	768
secp521r1	260	1042
x25519	127	510
x448	224	896

有限体DHはポピュラーだが，公開情報の長さを見るとECDHのほうが効率的

初日のまとめ

- 共通鍵暗号：古くから使われている暗号
  - 現代ではAESが日常的に使われている
- 共通鍵暗号を使うには，あらかじめ二者間で**秘密を共有する必要**がある.
- 秘密を共有する方法として，有限体Diffie-Hellman，楕円曲線Diffie-Hellmanを見た.
  - アーベル群の作用の言葉でDiffie-Hellmanは整理できる.
  - ただし，「計算誤差が出ず」，「計算が効率的にでき」，「離散対数問題（DL），Diffie-Hellman問題（CDH，DDH）が解けない」ことが要求される.
- これらの安全性は離散対数予想，Diffie-Hellman予想の仮定の下で成立するが，これらの予想は未解決であり，非常に強い仮定である.

→現代社会の土台は純粋数学が支えているし，これからもそうだろう

明日やること

- 群作用とはいいつつも，有限群DHも楕円曲線DHも，以下の範疇に収まる：

Gをアーベル群，$0 \neq g \in G$を位数nの元とする．

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

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．

- しかし上は量子計算機で解くことができてしまう！
- 明日は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だろうDiffie-Hellmanを紹介します．

References

- [Shannon49]: C.E.Shannon, "Communication theory of secrecy systems", *The Bell system technical journal* 28.4 (1949): 656-715.
- [Menezes-Wu98]: A.Menezes and Y-H.Wu, "The discrete logarithm problem in $GL(n, q)$", *Ars Combinatorica* 47 (1997), 23–32.
- [Montgomery-Zhandry22]: H.Montgomery and M.Zhandry, "Full quantum equivalence of group action DLog and CDH, and more", *Journal of Cryptology* 37.4 (2024): 39.
- [Couveignes06]: J-M.Couveignes. "Hard Homogeneous Spaces" *IACR Cryptology ePrint Archive* 2006/291, (2006). https://ia.cr/2006/291.
- [Fukuoka20]: T. Fukuoka, "Relative linear extensions of sextic del Pezzo fibrations over curves", *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) Vol. XXI (2020), 1371–1409.

おわり

お問い合わせはこちら：fukuoka.takeru@fujitsu.com