耐量子計算機暗号：量子コンピュータ時代の安全な情報通信に向けて

縫田　光司（ぬいだ　こうじ）
九州大学 マス・フォア・インダストリ研究所

研究集会「量子暗号理論と耐量子暗号」
2022/3/18　@早稲田大学（オンライン）

https://www.morikita.co.jp/books/book/3503

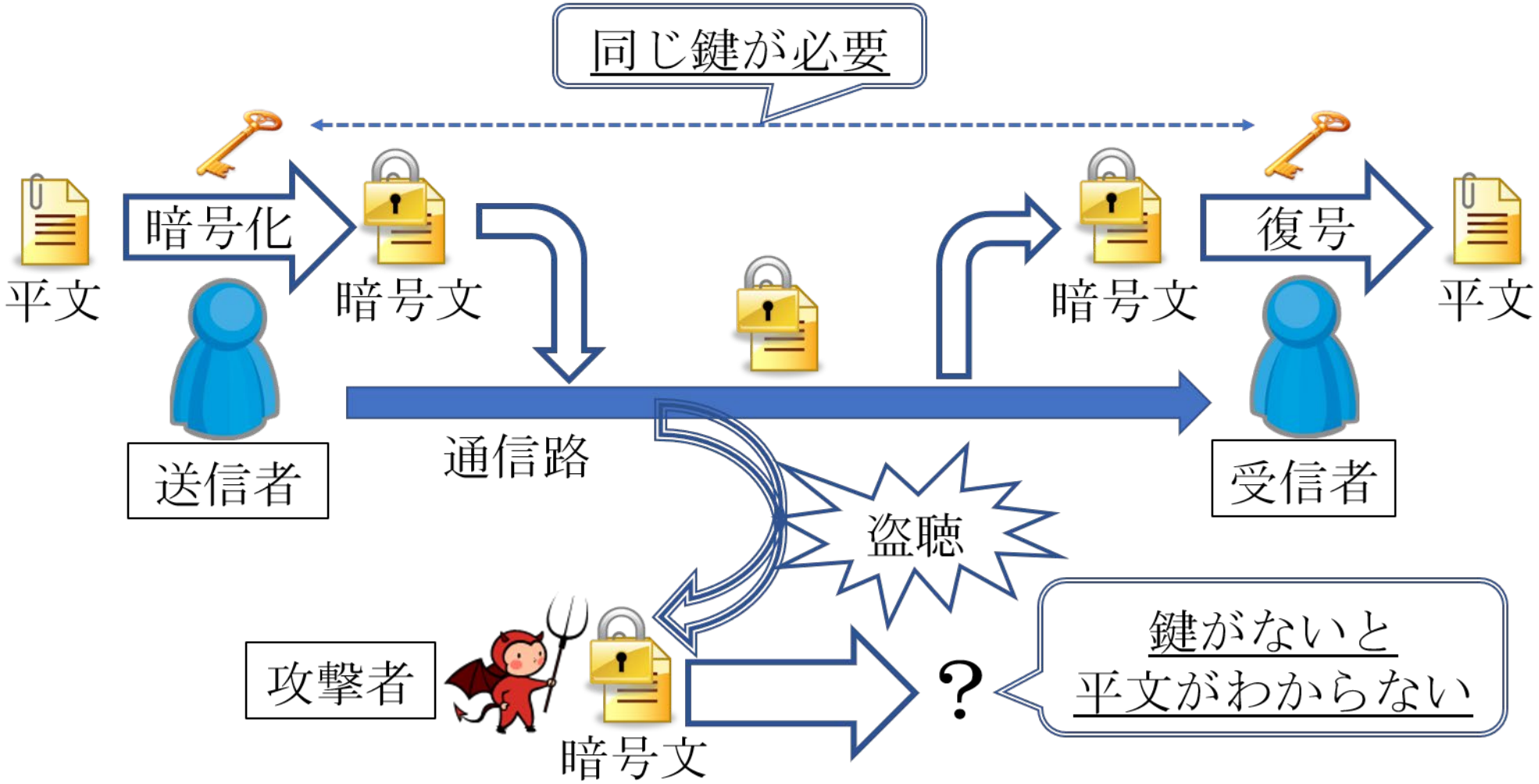
本日の目次

- （公開鍵）暗号技術とその安全性評価の概要
- 耐量子計算機暗号の歴史と研究動向
- 耐量子計算機暗号の安全性評価の方法論と現状

本日の目次

- **（公開鍵）暗号技術とその安全性評価の概要**
- 耐量子計算機暗号の歴史と研究動向
- 耐量子計算機暗号の安全性評価の方法論と現状

（共通鍵）暗号化通信


同じ鍵が必要
暗号化
平文
暗号文
送信者
通信路
盗聴
攻撃者
暗号文
?
鍵がないと
平文がわからない
暗号文
復号
平文
受信者

バーナム暗号（ワンタイムパッド）

- G. S. Vernam, 1919（米国特許）
- 大まかな説明：各ビットを「反転する／しない」が秘密の鍵

0110 → 1011 → 0110

暗号化 (1,1,0,1)　　復号 (1,1,0,1)

- （適切に使えば）メッセージの「完璧な秘匿」が可能

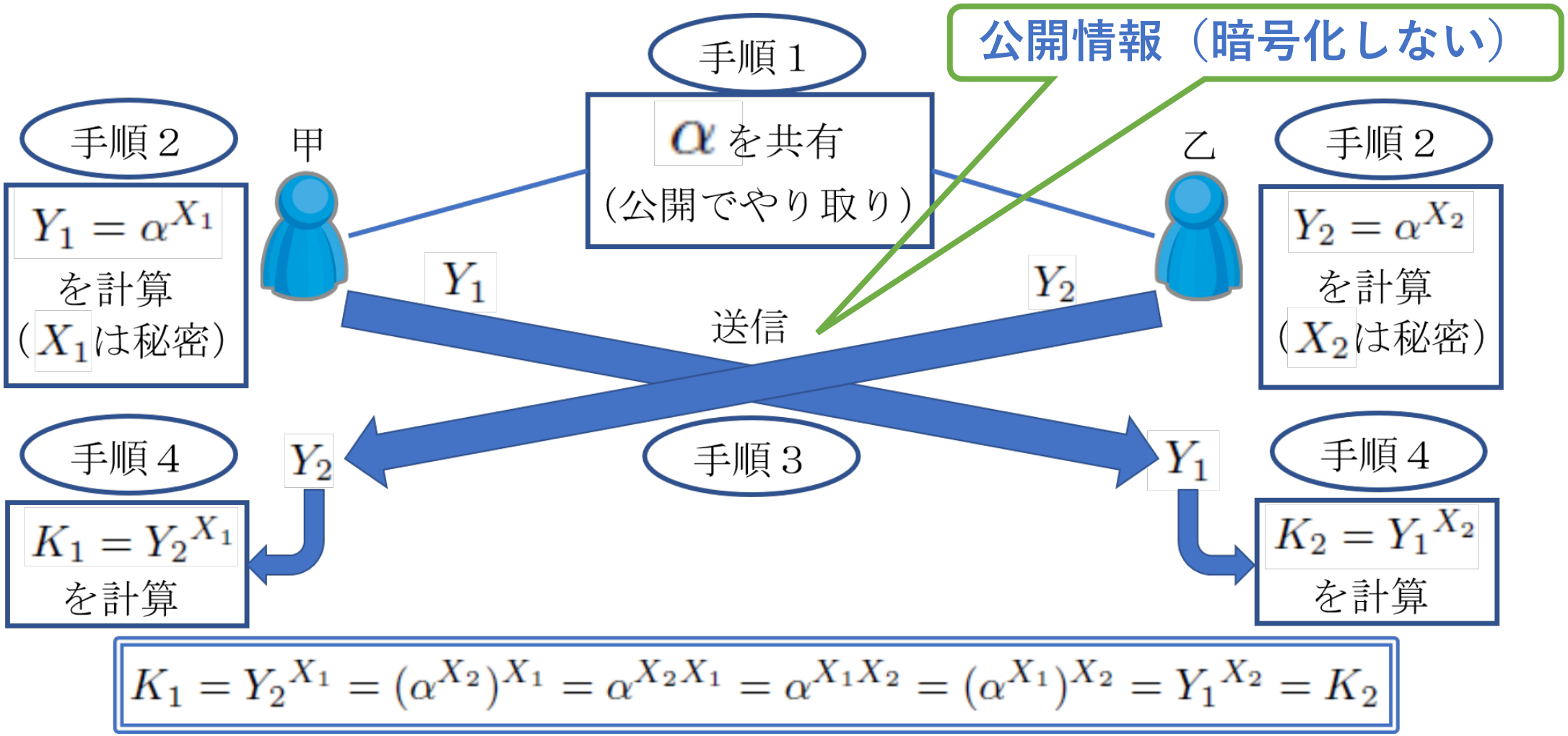
ワンタイムパッドの利点と欠点

- 利点
  - 安全性を数学的に（**無仮定で**）証明可能
- 欠点
  - **鍵サイズが大きい**
    （ワンタイムパッドと同等の安全性を実現するためには、
    メッセージと同じかそれ以上の鍵サイズが必要と証明されている）
  - （上記の帰結として、）**鍵を１回しか使えない**：
    複数のメッセージを同じ鍵で暗号化すると安全でなくなる

欠点の克服：「計算量的安全性」

- 安全性を「少し」弱めて、鍵サイズの制約を解消
- 様々な方法論：
  - 専用の共通鍵暗号化方式（AESなど）
  - 擬似乱数による鍵生成＋ワンタイムパッド（ストリーム暗号）
  - **「公開鍵型」鍵共有プロトコル**＋ワンタイムパッド
  - **公開鍵暗号化方式**（鍵共有と暗号化の一括化）
    ＊「鍵共有と暗号化の一括化」に見えない方式もある

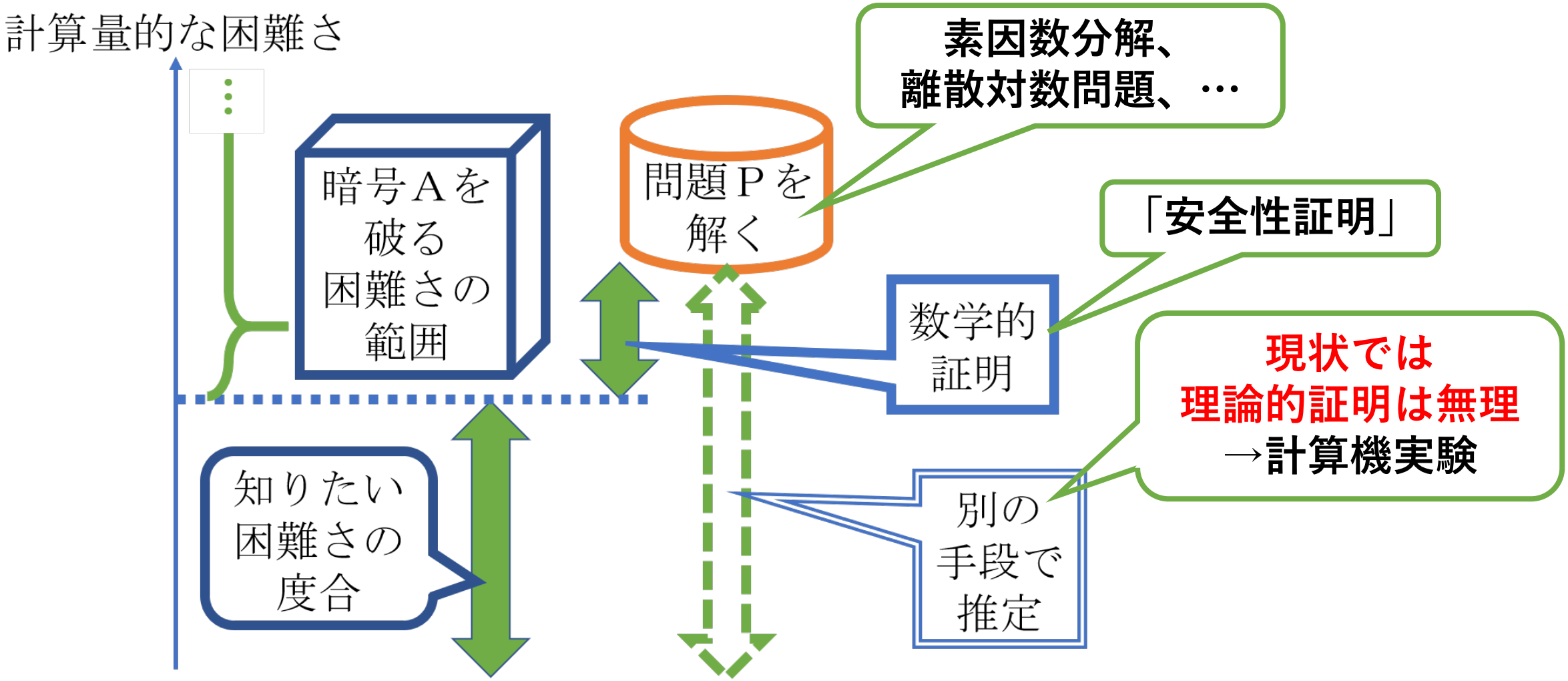
ディフィー・ヘルマン（DH）鍵共有



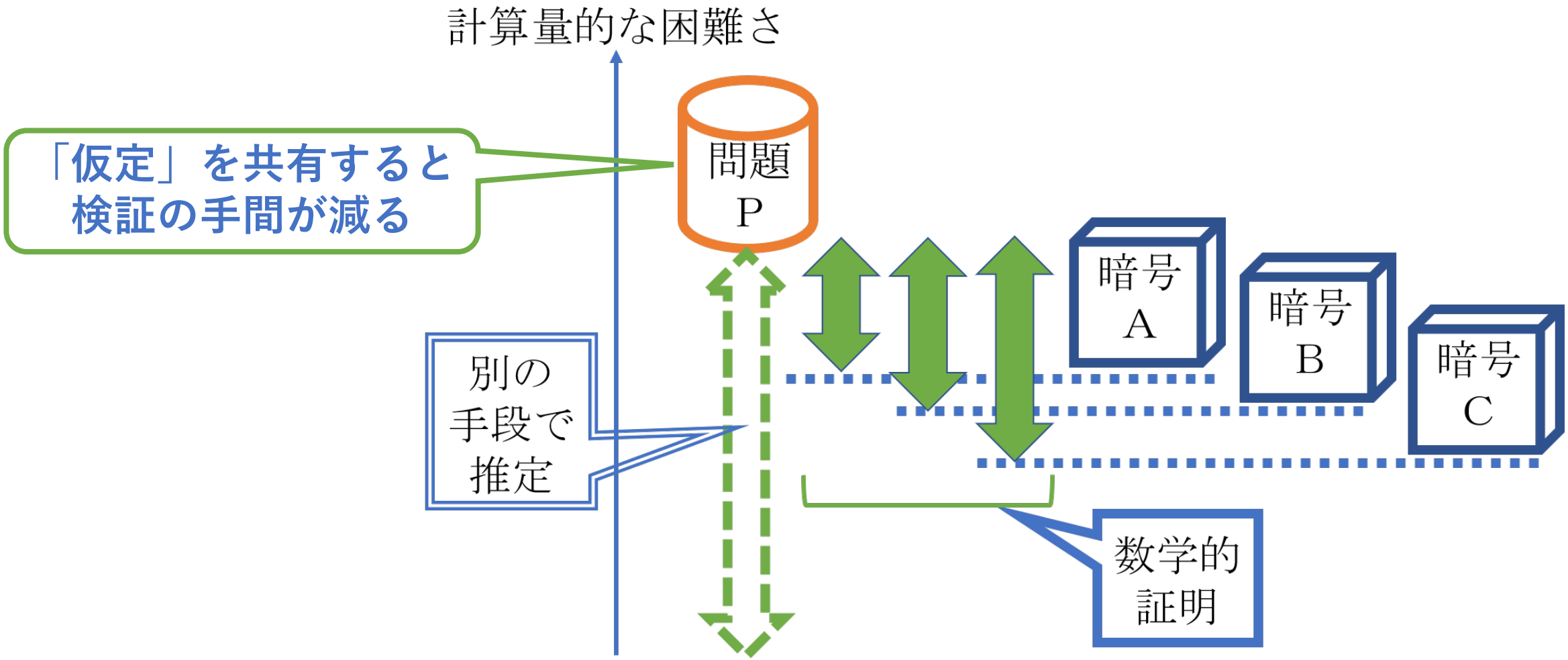
DH鍵共有と計算量的安全性

- αとα^Xは公開情報（Xは秘密）
- 数学的には、αとα^XからXがただ一つに決まる
  （「離散対数問題」）
- もし攻撃者の計算時間が無尽蔵であれば、秘密Xを特定可能
  （→安全性が崩壊）
- しかし、（うまく設定すれば）**現実的な範囲の計算時間では秘密Xを特定できないと期待される**
  - 注：αとα^Xが数直線上の値であれば解析的な手段で簡単だが、
    ここでは群などの「周期的な」構造を用いているため自明でない

計算量的安全性の評価の方法論



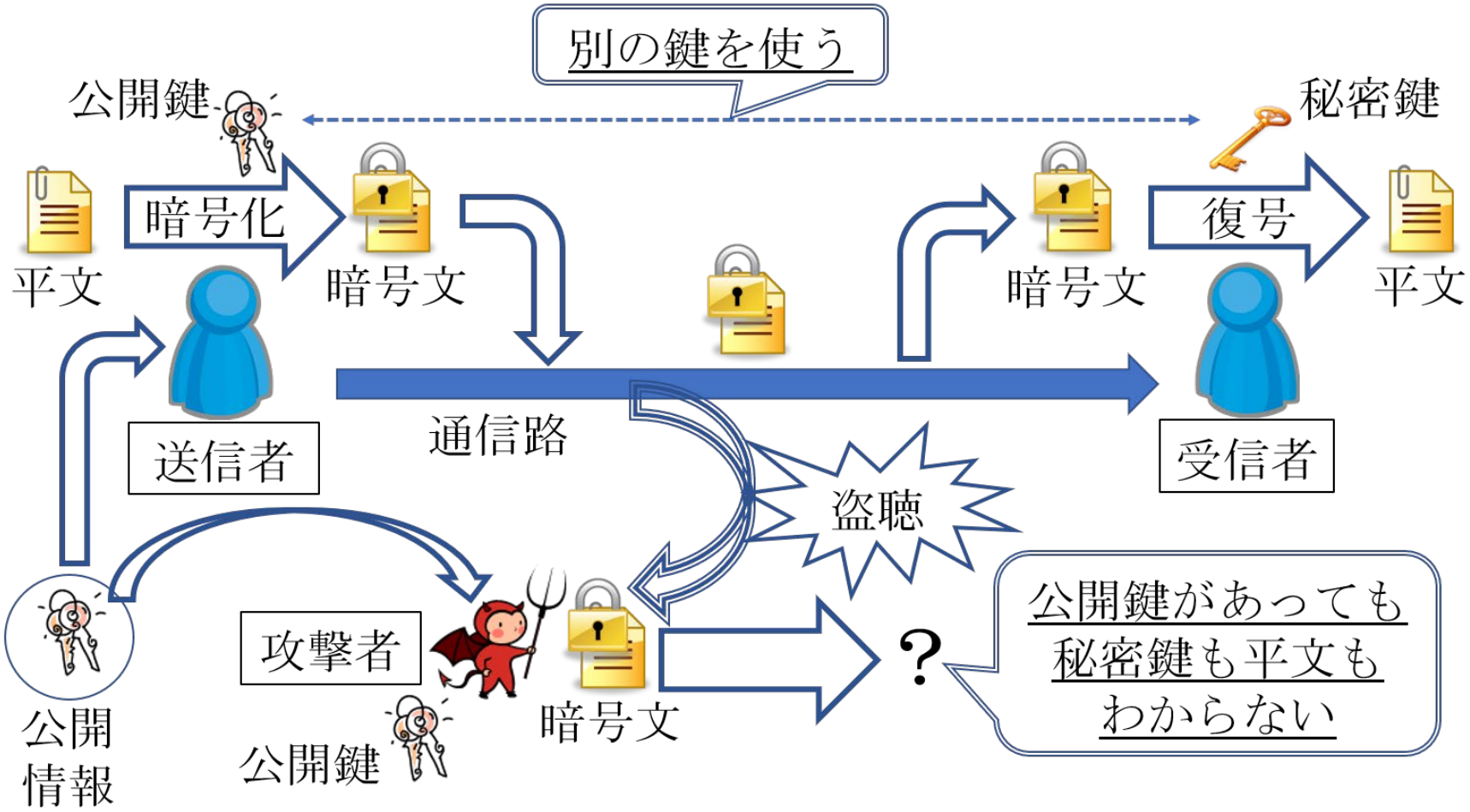
「標準的な安全性仮定」の重要性



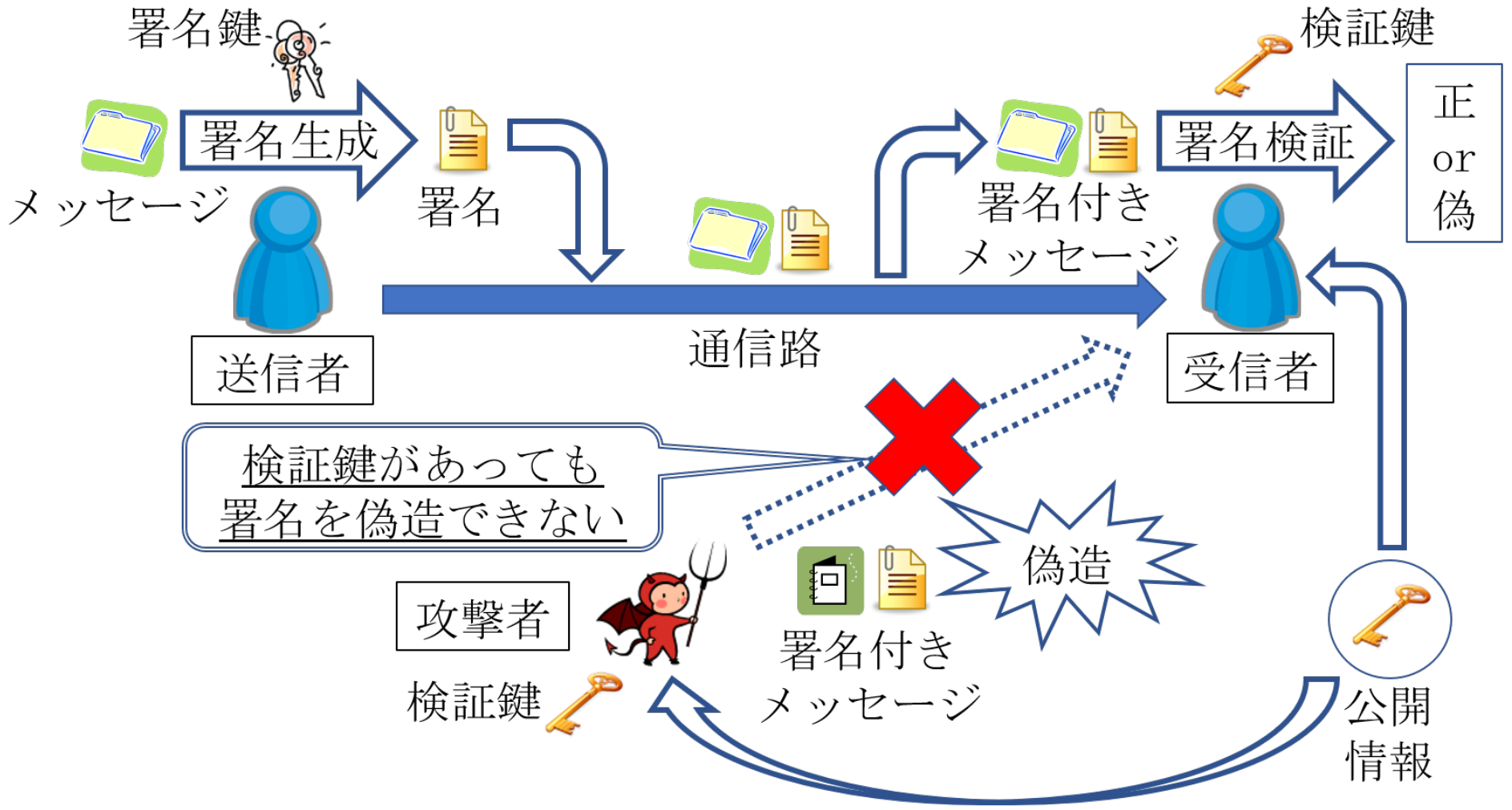
暗号解読コンテスト

- 実験による安全性評価の方法論：「精一杯解読を試みる」
  - 「それでも全然無理」なパラメータ設定にすれば当面は安全
- 研究者を「精一杯頑張らせる」仕組み：解読コンテスト
  - 素因数分解（RSA Factoring Challenge）　＊終了済
  - 格子暗号（Lattice Challenge）　＊2008年から
  - 多変数多項式暗号（Fukuoka MQ Challenge）　＊2015年から
  - 符号ベース暗号 https://decodingchallenge.org/ ＊2019年から
  - 同種写像暗号 https://www.microsoft.com/en-us/msrc/sike-cryptographic-challenge ＊2021年から

公開鍵暗号化通信


別の鍵を使う
公開鍵
秘密鍵
暗号化
復号
平文
暗号文
暗号文
平文
送信者
通信路
受信者
盗聴
攻撃者
公開
情報
公開鍵
暗号文
?
公開鍵があっても
秘密鍵も平文も
わからない

電子署名


署名鍵
検証鍵
署名生成
署名検証
正
or
偽
メッセージ
署名
署名付き
メッセージ
送信者
通信路
受信者
検証鍵があっても
署名を偽造できない
偽造
攻撃者
署名付き
メッセージ
検証鍵
公開
情報

本日の目次

- （公開鍵）暗号技術とその安全性評価の概要
- **耐量子計算機暗号の歴史と研究動向**
- 耐量子計算機暗号の安全性評価の方法論と現状

量子計算機（量子コンピュータ）

- 量子計算（量子力学的原理が組み込まれた数学モデルに基づく計算）を実行できるコンピュータ
- （「量子計算機がなぜ強力か」の説明は難しいが、例えば）通常の（「古典計算」の）nビットはn個の成分からなるが、n量子ビットは2^n個もの成分を内包する
  - が、それらの成分を自在に取り出せるわけではないので、量子アルゴリズムの設計は一筋縄ではいかない
- ある種の問題について、**古典計算機を大幅に超える性能を発揮**
  →（計算量的安全な）**暗号技術への脅威にもなり得る**

ショアの量子アルゴリズム

- P. W. Shor: Algorithms for quantum computation: discrete logarithms and factoring. In: IEEE FOCS 1994
- ショアの量子アルゴリズムを用いると、（よりによって）
  素因数分解（←RSA暗号の安全性の根拠）
  離散対数問題（←「楕円曲線暗号」の安全性の根拠）
  が効率的に計算可能となる
- つまり、**これらの問題に基づく方式（←現時点での標準的な公開鍵暗号技術のほぼ全て）が安全でなくなる**
  - ただし、現在の量子計算機（数十～百数十量子ビット程度）では実用的な暗号方式を破るには規模が全然足りないので、まだ安心

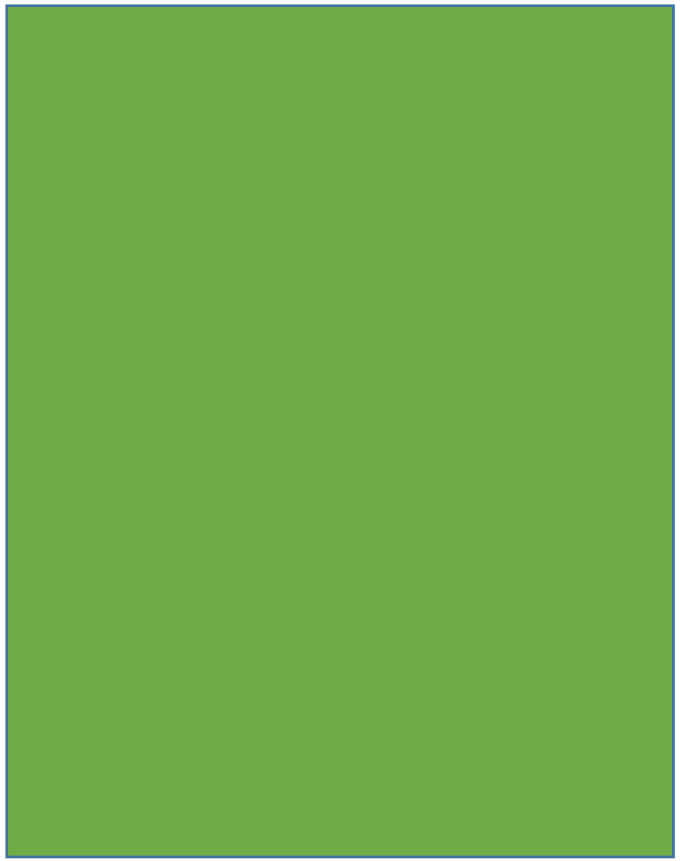
耐量子計算機暗号

- 既存の量子アルゴリズムで破れない公開鍵暗号技術
  - もちろん、従来型の古典計算機でも破れてはいけない
- 注：暗号技術が「破れる／破れない」の意味
  - 理論的には、「多項式時間アルゴリズム」で「無視できない解読確率（優位度）」を実現可能かどうか
  - 実用的には、「多項式時間」→「現実的時間」（例：2^{128}ステップ）（参考：安永さんのご講演）
- 量子計算機の将来的な大規模化を見据えて、米国NISTにより標準化公募が行われ、応募された方式を現在厳選中

大規模量子計算機の実現時期？

- ショアのアルゴリズムが動くほど大規模な量子計算機がいつ頃実現するかの推測は難しい（情報技術の進歩は急激）
  - 「2030年頃に実現」との意見がある（NIST PQC 標準化は「2030年」を見据えたスケジュール）
  - 一方で、「永遠に実現されない」との意見もある
- 「まだ実現されてもいない（大規模な）量子計算機に対する安全性対策」に、どれぐらいリソースを割いてもらえるか？
  - これ自体は暗号技術全般の宿命かもしれない
  - 既存サービスの暗号部分の置き換えではなく、新規サービスにはじめから耐量子計算機暗号を組み込む方が普及しやすい？

NIST PQC 標準化公募

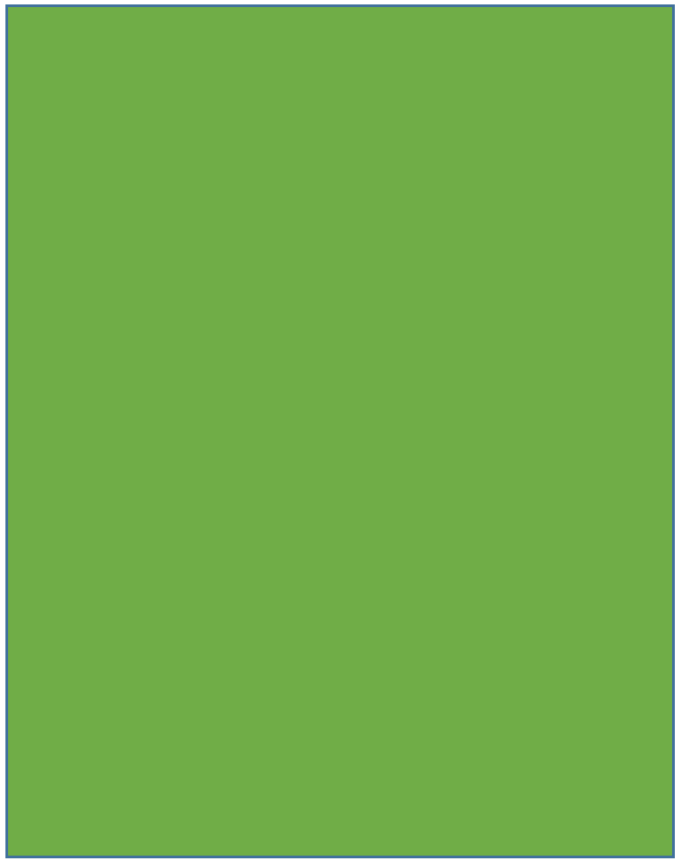


応募総数：69件
（2017年12月）

	暗号化／鍵共有	電子署名
Finalists	Classic McEliece CRYSTALS-KYBER NTRU SABER	CRYSTALS-DILITHIUM FALCON Rainbow
Alternate Candidates	BIKE FrodoKEM HQC NTRU Prime SIKE	GeMSS Picnic SPHINCS+

第3ラウンド：7+8件（2020年7月）

NIST PQC 標準化公募



応募総数：69件
（2017年12月）

符号ベース暗号
多変数多項式暗号
格子暗号
同種写像暗号

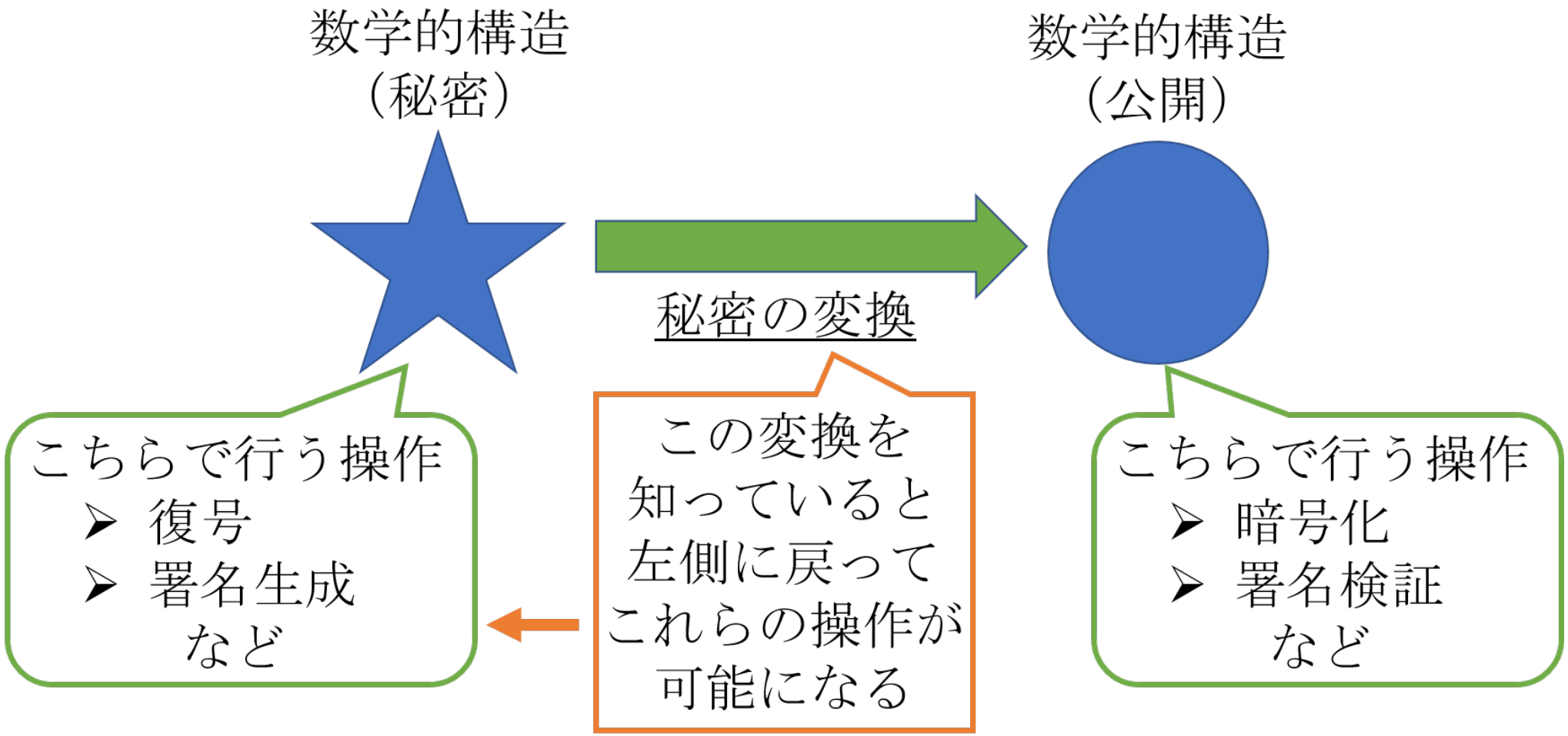
	暗号化／鍵共有	電子署名
Finalists	Classic McEliece CRYSTALS-KYBER NTRU SABER	CRYSTALS-DILITHIUM FALCON Rainbow
Alternate Candidates	BIKE FrodoKEM HQC NTRU Prime SIKE	GeMSS Picnic SPHINCS+

第3ラウンド：7+8件（2020年7月）

耐量子計算機暗号（時系列順）

- 1978年：符号ベース暗号（McEliece）
- 1988年：多変数多項式暗号（松本・今井）
- （1994年：ショアの量子アルゴリズム）
- 1997年：格子暗号（Ajtai-Dwork）
- 2006年：同種写像暗号（Couveignes, Rostovtsev-Stolbunov）

公開鍵暗号技術の設計指針（の一つ）



符号ベース暗号：誤り訂正符号

- **誤り訂正符号**（ノイズのある通信路での情報通信技術）を暗号技術に応用したもの
- 誤り訂正符号：メッセージをうまく「符号化」すると、ノイズの影響で符号語が少し変化しても、もとの符号語へ正しく「復号」できる
  - 符号語の集合：（有限体上の）連立一次方程式の解集合
- 誤り訂正符号の例：（3重）繰り返し符号
  - 同じメッセージを3回繰り返す
  - 多数決をとって復号すると、誤りが1個までなら正しく復元できる
  - （効率が悪いので、実際にはもっと巧みで効率的な構成を用いる）

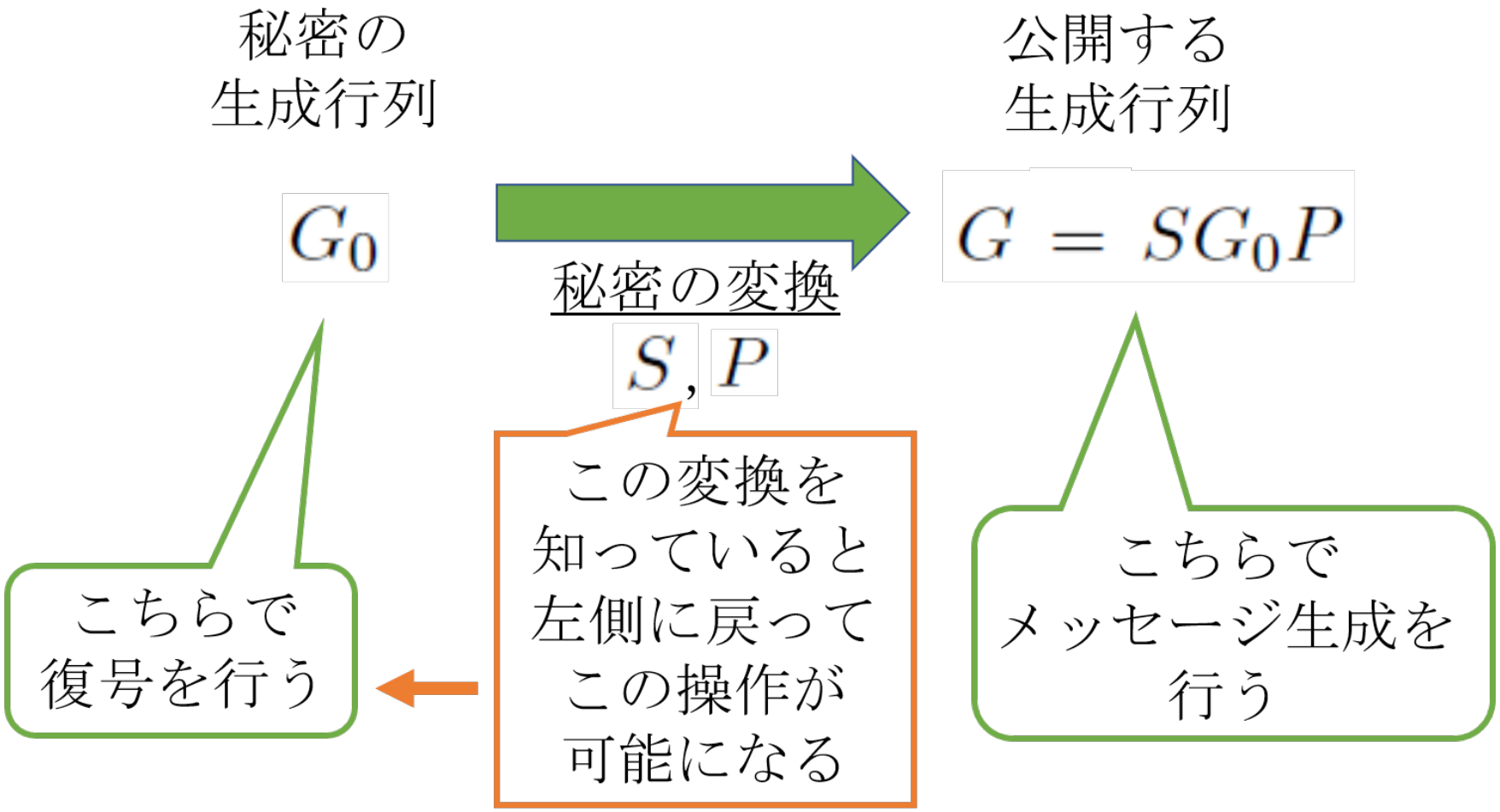
（線型）誤り訂正符号の概要

- 符号化：ある（横長の）行列G（生成行列）を用意して、メッセージのベクトルを（左から）掛ける
  - 符号語はもとのメッセージより高次元のベクトル
- パリティ検査行列：符号語を（転置して、右から）掛けると零ベクトルになるような行列H
  - 符号語空間は（転置を除き）Hが定める線型写像の核と一致
- 複号：符号のサイズが小さければ、
  - Hの逆像の（ハミング重みの小さい）代表元を予め列挙しておく
  - 受信語にHを掛けて、上記の代表元と比較すると誤りベクトルが判明
  - サイズが大きい場合には（計算量的な理由で）別の工夫が必要

符号ベース暗号（概要）

- 暗号化：メッセージにランダムな（小さい）ノイズを加える
- 復号：誤り訂正符号の機能でノイズを除去する
- 一般の（ランダムな）誤り訂正符号の場合、
  暗号化は簡単にできるが復号（ノイズ除去）は難しい
- 巧く構成した誤り訂正符号であれば復号も簡単
- **「一般の形から巧い形への変換法」（これが秘密鍵）を知っていれば**、後者に変換して復号を行える

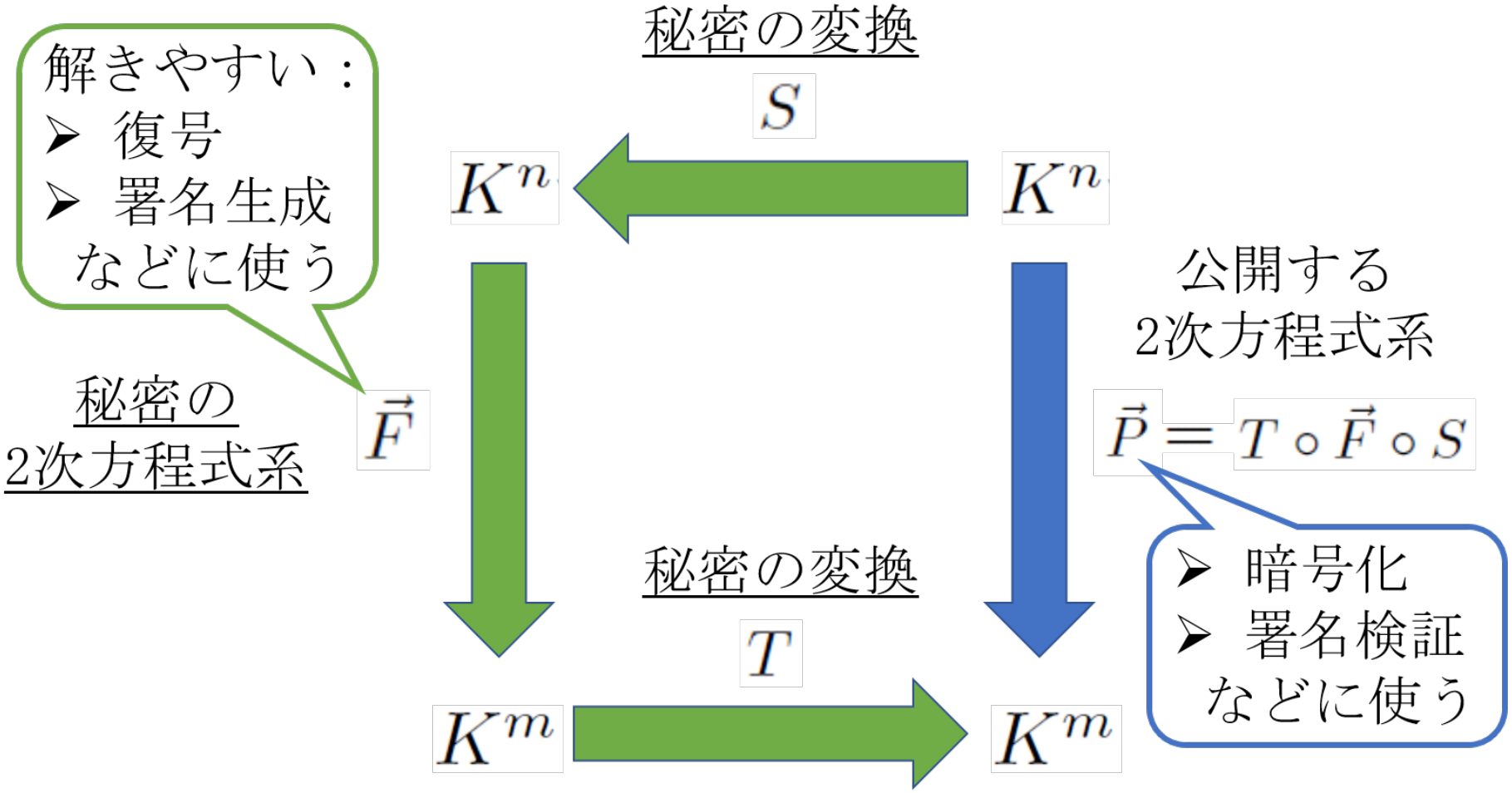
符号ベース暗号（概念図）


秘密の
生成行列
G_0
公開する
生成行列
$G = SG_0P$
秘密の変換
S, P
こちらで
復号を行う
この変換を
知っていると
左側に戻って
この操作が
可能になる
こちらで
メッセージ生成を
行う

多変数多項式暗号（概要）

- **有限体上の**連立2次方程式系を用いる
- 暗号化／署名検証：多項式への値の代入（簡単）
- 復号／署名生成：連立方程式の解の計算
  - 一般の場合には難しい
    （最適化問題のような解析的手法が使えない）
  - 巧い形の場合には簡単
    （例：$f_1(x_1)=0,\ f_2(x_1,x_2)=0,\ f_3(x_1,x_2,x_3)=0,\ldots$の形の場合、$x_1,x_2,x_3,\ldots$の順番に解の値を決定できる）
- **「一般の形から巧い形への変換法」（これが秘密鍵）を知っていれば**、後者に変換して復号／署名生成を行える

多変数多項式暗号（概念図）



耐量子計算機暗号の多様性

- ショア以前の公開鍵暗号技術は、「定番の方式」が明快だった（まずはRSA暗号、その後は楕円曲線暗号）
- 耐量子計算機暗号では、異なる構成原理ごとに利点・欠点や得意・不得意がさまざまで、「これが定番」と決めにくい
  →どの原理についても、近年も盛んに研究され続けている

本日の目次

- （公開鍵）暗号技術とその安全性評価の概要
- 耐量子計算機暗号の歴史と研究動向
- **耐量子計算機暗号の安全性評価の方法論と現状**

耐量子計算機暗号の安全性評価

- 安全性証明も（可能なら）行うが、最終的には計算機実験で「精一杯解読を試みる」過程が不可欠
  - Lattice Challenge, Fukuoka MQ Challenge, 他
  - この点は従来の公開鍵暗号と同様
- 耐量子計算機暗号ならではの難しさ：
  - 「解読を試みる」のに使える量子計算機がまだ存在しない
  - 問題の難しさを決めるパラメータの個数が多く順序付けしにくい（例：素因数分解は「整数の桁数」だけだが、多変数多項式暗号は「有限体のサイズ」「変数の個数」「方程式の個数」の3次元量）
  - 種類によってはかなり高度な数学的知識が要求される

安全性評価に頻出する量子アルゴリズム

- いずれもショアのアルゴリズムほど劇的な効率化ではないが、汎用性が高いため広く応用される
- グローバーのアルゴリズム（L. K. Grover, 1996）：（無構造の）データ集合に対する検索を行う
  - N個のデータ集合のとき、およそ$N^{1/2}$回の試行で（高確率で）成功
- 量子ウォーク（A. Ambainis, 2007、など）：グラフの頂点集合上でのデータ探索を行う
  - 例：N個の頂点のうち、「同じ種類」の頂点を探す問題についておよそ$N^{2/3}$回の試行で（高確率で）成功

注意：耐量子計算機共通鍵暗号

- 共通鍵暗号についての暗号業界の当初見解：
  グローバーの量子検索アルゴリズムへの対策として、
  鍵サイズを倍程度に伸ばしておけば安全であろう
- 2010年頃より、ある種の共通鍵暗号に対しては、
  （ショアのアルゴリズムとは別系統の）量子アルゴリズムで
  効率的な解読が可能であることが解明され始めた
- 現時点でAESのような実用的方式への大きな影響は見られないものの、「耐量子計算機共通鍵暗号」の歴史はまだ浅いので
  今後の研究動向にも注視が必要と考える
- 参考：細山田さんのご講演

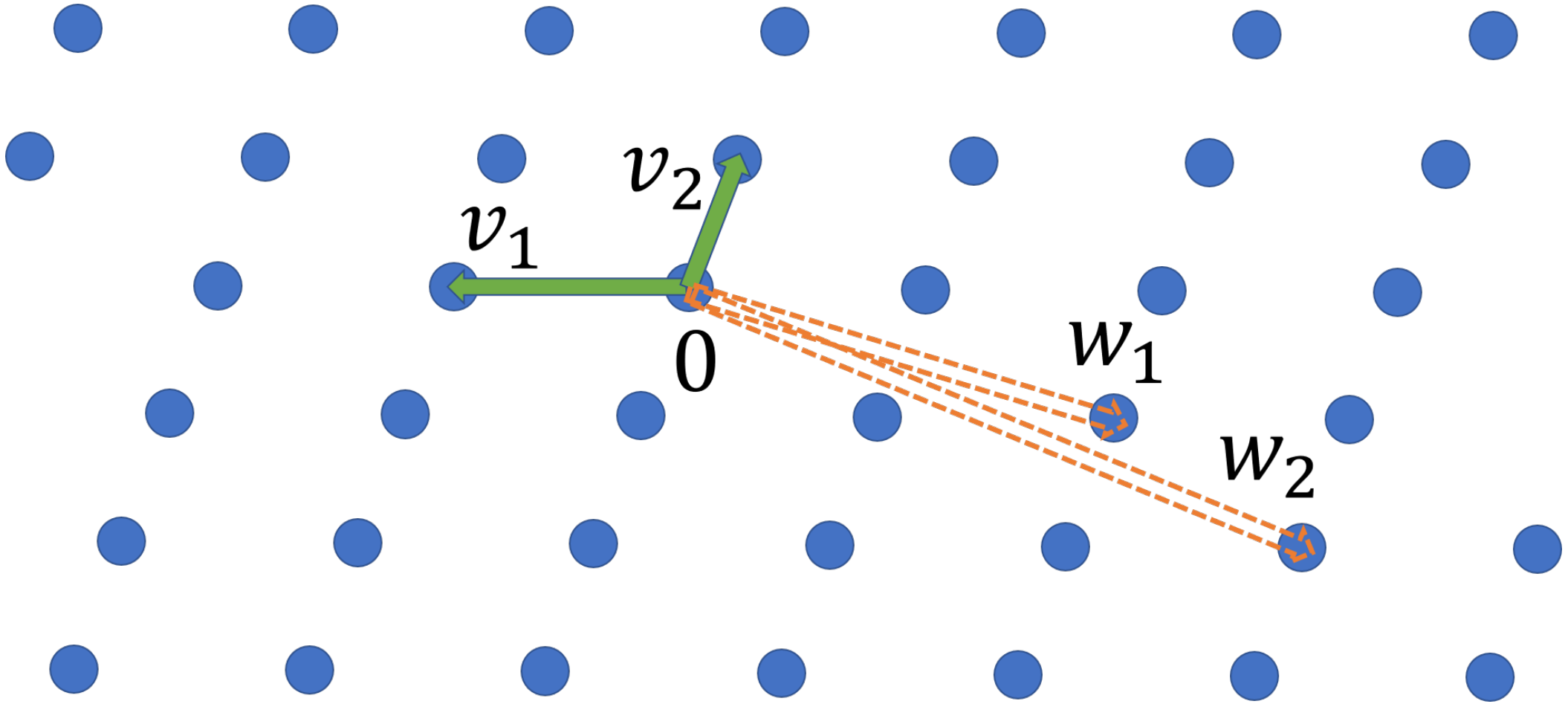
符号ベース暗号の安全性解析

- もし「あらゆる誤り訂正符号について、ハミング重みが小さい（非零）符号語を効率的に発見できる」ならば、
  あらゆる誤り訂正符号の復号を効率的に行える（Stern, 1989）
- **重みが小さい符号語の探索問題**の困難性が、符号ベース暗号の安全性と密接に関連する
- 古典計算でのアルゴリズム（Becker et al., EUROCRYPT 2012、など）や、量子ウォークと組み合わせた量子アルゴリズム（Kirshanova, PQCrypto 2018）などが近年も研究されている
- 話者の印象：だいぶ「枯れた技術」になってきている
  （符号ベース暗号の40年以上の歴史の重み）

格子暗号

- 符号ベース暗号と同様に、ある点集合の中から「小さい」点を探す問題の困難性に基づく
  - 「小さい」の定義は符号の場合と異なる
  - 格子暗号の場合は「最短ベクトル問題」（SVP）と呼ばれる
- 符号ベース暗号における点集合は「高次元の立方体の頂点（の一部）」だったが、格子暗号では立方体だけでなく全空間に広がる格子点の集合（次ページ参照）を考える
- **「格子がどのように指定されているか」で問題の難度が変わる**
  - 「基底ベクトル」が入力として与えられて、格子の点集合は基底ベクトルの組み合わせで作れる点たちの集合として定まる

2次元格子と基底ベクトルの例



最短ベクトル問題の主な手法（概要）

- Enumeration（列挙法）（Pohst, 1981、～）：
  基底ベクトルの組み合わせを（なるべく効率的に）全探索する
- Sieving（篩法）（Ajtai, 2001、～）：
  材料となる格子点を大量に準備して、それらの相互作用で
  格子点の集合を原点へ向けて凝縮させていく
- Random Sampling Reduction（Schnorr, 2003、～）：
  なるべく原点側へ向かいやすくなるように遷移確率を上手く
  定めて格子点たちのランダムな探索を行う
- 参考：安田さんのご講演

SVP Challenge の世界記録の変遷

https://www.latticechallenge.org/svp-challenge/index.php

- 最短ベクトル問題に特化したLattice Challengeの一部門
  - 基本的には格子の次元が高いほど好成績とされる
- 初期の記録：Enumeration
- 128次元（2013年9月）～150次元（2017年1月）：Random Sampling Reduction
  - 深瀬・柏原、および柏原・照屋の研究グループによる記録
- 151次元（2018年8月）～180次元（2021年2月、現記録）：SubSieve（Sievingの改良手法、Ducas et al.）
- 話者の印象：近年も伸びが著しく、まだ底が見えない

格子暗号と量子アルゴリズム

- かなり極端な形の格子（詳細は割愛）については、ショアの量子アルゴリズムの拡張版を用いて、最短ベクトル問題をそこそこ効率的に解ける（Regev, 2004）
  - 「かなり極端な形」：ギャップの大きな一意最短ベクトル問題
  - 「そこそこ効率的」：準指数時間アルゴリズム
- ただし、ごく初期の方式を除いて、格子暗号においてこうした「極端な形の格子」は現れないため、安全性への影響は薄い

多変数多項式暗号の安全性解析

- 基本的には、暗号方式から得られる連立2次方程式系の解をどれだけ効率的に計算できるかが問題
  - 暗号方式によっては、その構造を利用した固有の攻撃も存在する
- 「グレブナー基底」を効率的に計算することで方程式を解ける
- グレブナー基底の計算量は主に、方程式系の「正則次数」（degree of regularity）という量と、linear algebra constant と呼ばれる値ω（後述）を用いて見積もられる
  - 前者の量を見積もるのは理論的にだいぶ難しい
- Fukuoka MQ Challengeの記録も定期的に更新されている

  https://www.mqchallenge.org/

多変数多項式暗号の安全性解析

- linear algebra constant：「n次正方行列どうしの積をおよそn^{ω}の計算量で計算できる」を満たす値$\omega \geq 2$
  - 素朴な（定義通りの）計算法：$\omega = 3$
  - （Strassen, 1969）$\omega < 2.81$
  - （Le Gall, 2014）$\omega < 2.37287$
  - （Alman-Williams, 2020年10月）$\omega < 2.37286$
- 話者の印象：だいぶ「枯れてきている」ようにも思えるが、グレブナー基底（や行列積）の計算は暗号分野以外でも注目度が高いため、思わぬ技術革新が起きるかもしれない
  - ただし油断は禁物：Rainbowの提案パラメータの一つへの最近の攻撃

同種写像暗号

- これまでの構成原理（符号ベース、多変数多項式、格子）には「公開鍵サイズが大きくなりやすい」難点がある
  - 行列や連立方程式系のような「2次元」のデータの指定が必要
- **同種写像暗号**：$y^2 = x^3 + Ax^2 + x$という形の式で定義される図形（楕円曲線）を用いる暗号技術（主に鍵共有）
  - SIDH（Jao-De Feo, 2011）、CSIDH（Castryck et al., 2018）など：これらはDH鍵共有方式の発展版
  - Aの値だけで曲線を表せるので、公開鍵サイズが小さくて済む
  - 従来の楕円曲線暗号は、曲線を一つ決めてその上の点たちの関連性を使ったが、同種写像暗号は複数の曲線たちの関連性を使っている

楕円曲線と同種写像（概要）

- （Montgomery型の）楕円曲線：$y^2 = x^3 + Ax^2 + x$
- 楕円曲線の有理点（と「無限遠点」）の集合には
  ある方法で可換群の構造が定まる
- 楕円曲線の間の**同種写像**：各成分が座標値の有理式で表せて、
  かつ有理点群の間の群準同型写像を与えるもの
- 同種写像の性質：もとの曲線と、同種写像（が定める群準同型写像）の核となる有限部分群が与えられると、同種写像の
  行き先の曲線と同種写像の組が（同型を除き）ただ一つ定まる
  - 具体的な計算も可能（Véluの公式）

同種写像暗号の安全性解析

- 基本的には、「二つの楕円曲線が与えられたとき、その間の同種写像の計算が難しい」ことに基づいた安全性
- 直接的な計算にしても何らかの迂回手段にしても、根本的に楕円曲線や同種写像自体が数学的にかなり高度な対象なので安全性解析にも相応の予備知識が要求される
- CSIDHの状況では、ショアの量子アルゴリズムの拡張版でそこそこ効率的（準指数時間）に計算可（Childs et al., 2014）
- 話者の印象：歴史が浅く、また技術的にも高度な方式なので安全性の推移について現時点では推測が難しい

本日のまとめ

- 現在の標準的公開鍵暗号（RSA暗号、楕円曲線暗号）を破れる規模の量子計算機が実現するまで（2030年頃？）に、耐量子計算機暗号の開発と充分な安全性評価が必要
  - NISTの標準化公募を中心とする研究コミュニティの形成
- 主要な種類（符号ベース、多変数多項式、格子、同種写像）のそれぞれについて、安全性評価の現状を手短に紹介
- 種類によって特徴（計算量、データ量、安全性評価の安定具合、量子攻撃の影響度合い、サイドチャネル攻撃耐性、…）が異なるため、適用する現場と相性の良い種類の選択が重要