（耐量子）公開鍵暗号入門

第三回量子情報ワークショップ（2020.7.2）

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
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号
- 高機能暗号

目次

- イントロダクション
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号
- 高機能暗号

暗号とは？

- 「**暗号**（あんごう）とは、セキュア通信の手法の種類で、第三者が通信文を見ても特別な知識なしでは読めないように変換する、というような手法をおおまかには指す。」（Wikipediaより引用）

暗号とは？

鍵

- 「**暗号**（あんごう）とは、セキュア通信の手法の種類で、第三者が通信文を見ても特別な知識なしでは読めないように変換する、というような手法をおおまかには指す。」（Wikipediaより引用）

暗号とは？

鍵

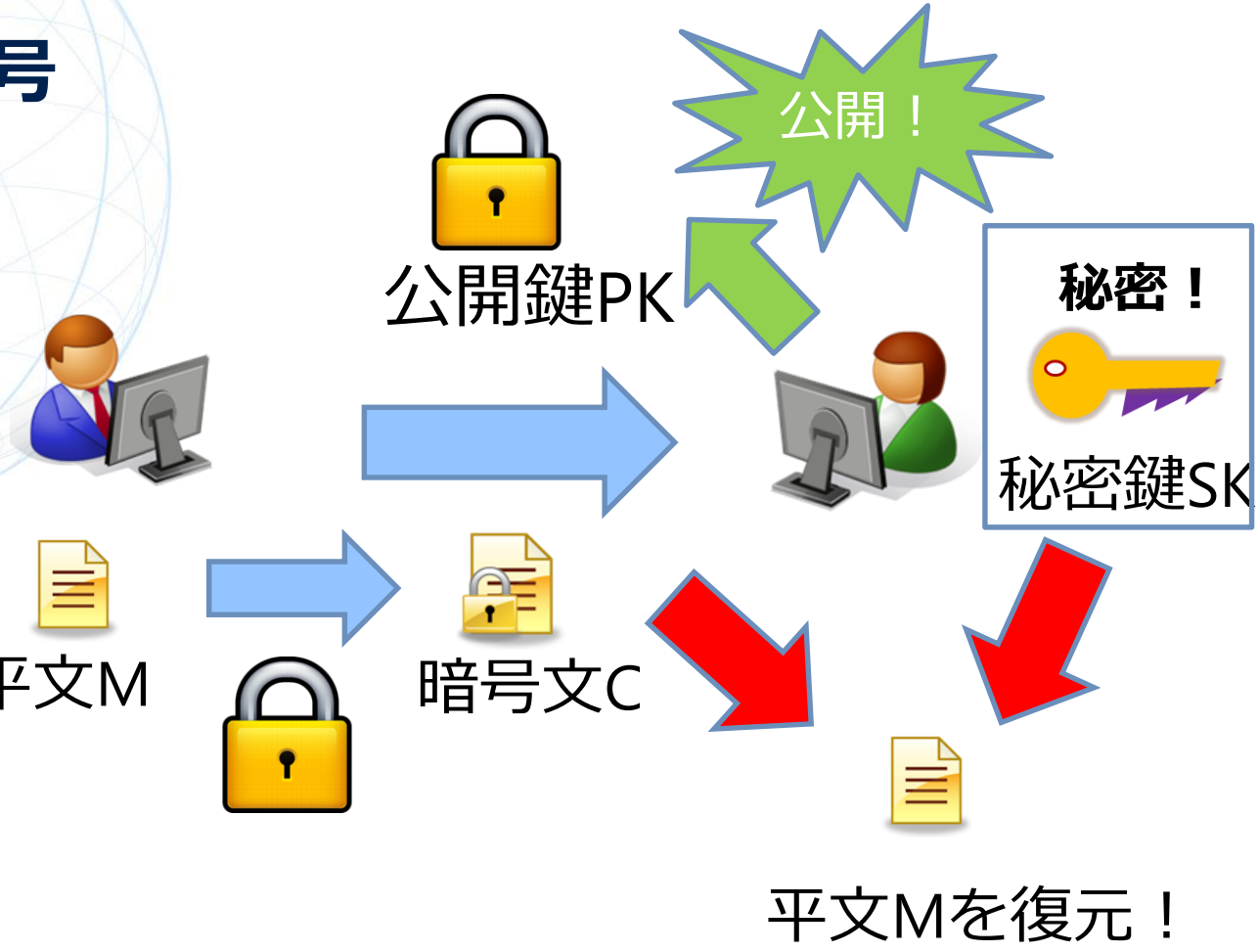
- 「**暗号**（あんごう）とは、セキュア通信の手法の種類で、第三者が通信文を見ても特別な知識なしでは読めないように変換する、というような手法をおおまかには指す。」（Wikipediaより引用）
- 共通鍵暗号：送信者と受信者で事前に鍵の共有が必要
  - シーザー暗号、ヴィジュネル暗号、エニグマ 、DES、AES 等…

暗号とは？

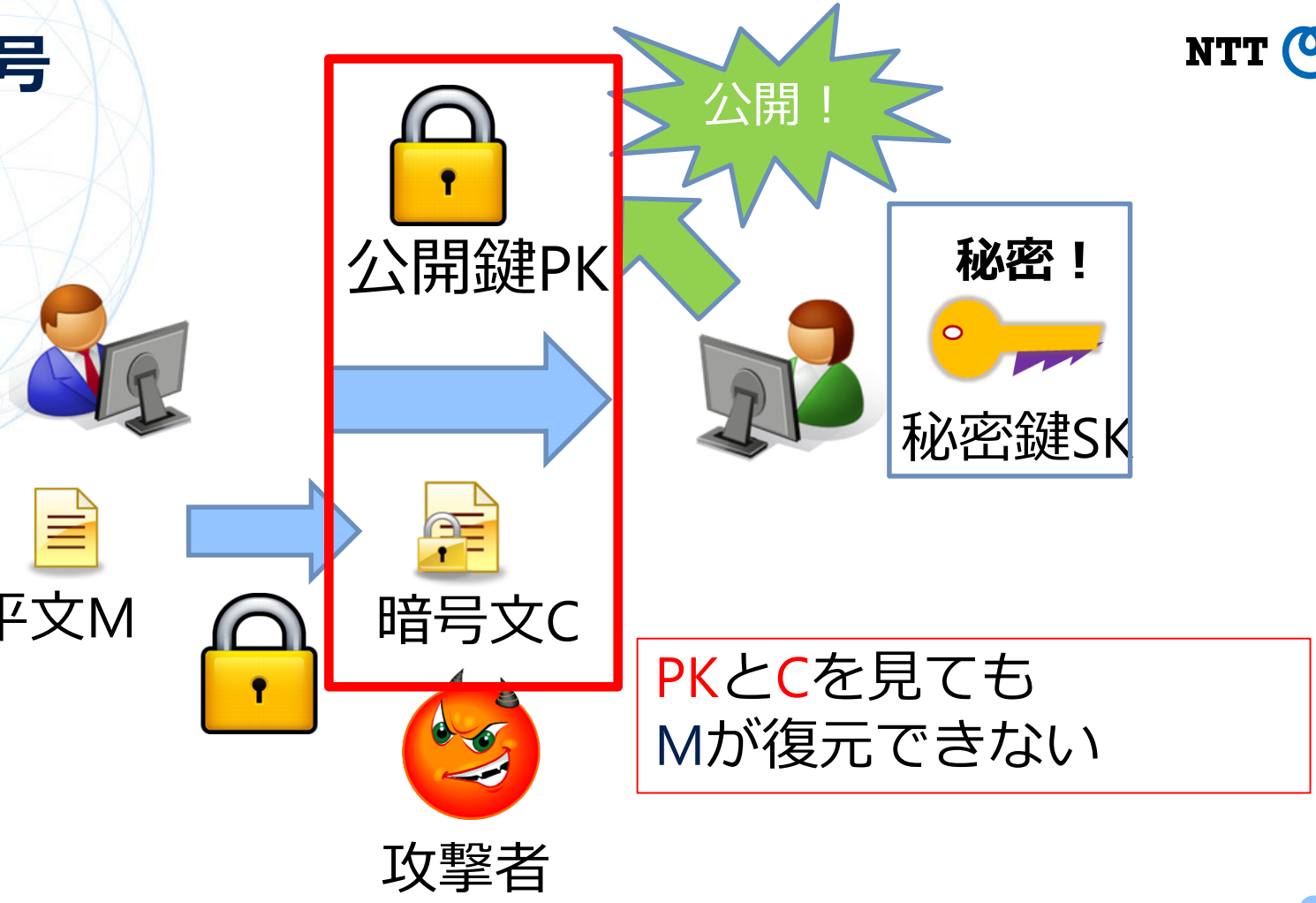
鍵

- 「**暗号**（あんごう）とは、セキュア通信の手法の種類で、第三者が通信文を見ても特別な知識なしでは読めないように変換する、というような手法をおおまかには指す。」（Wikipediaより引用）
- 共通鍵暗号：送信者と受信者で事前に鍵の共有が必要
  - シーザー暗号、ヴィジュネル暗号、エニグマ 、DES、AES 等…
- 公開鍵暗号：送信者と受信者で事前に鍵の共有が**不要**
  - 1976年頃：Merkle, Diffie, Hellmanらにより公開鍵暗号の概念の提案
  - 1977年：Rivest, Shamir, Adlemanによる初の公開鍵暗号（RSA暗号）の提案
  - (1973年：イギリスの諜報機関GCHQ所属の数学者Cocksも独立にRSA暗号を発見していたことが後に判明)
  - 近年ではインターネットやICカードのセキュリティのために不可欠な技術

公開鍵暗号



公開鍵暗号



PKとCを見ても
Mが復元できない

公開鍵暗号の作り方

- そんなことが可能なのか？
- 攻撃者が計算能力無制限の場合は不可能！
  - 攻撃者は全てのメッセージを暗号化してみて得られた暗号文に一致するか確かめれば良い。（暗号化アルゴリズムが乱択的の場合、乱数も全て試す）
- 攻撃者の計算能力を制限すれば可能（と信じられている）
  - 本当に攻撃方法が存在しないことを証明するのは少なくともP≠NP予想の解決を意味するため、現時点ではあくまで「予想」or「仮定」
- アイディア：計算するのは簡単だがもとに戻すのは難しい関数（一方向性関数）を使う。
- 例：素因数分解
  - 23×41=943を計算するのは簡単だが1247を素因数分解するのは"難しい"

目次

- イントロダクション
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号

素因数分解の困難性を利用した公開鍵暗号

- 素因数分解の困難性を利用した暗号と言えばRSA暗号が有名
- が、実はRSA暗号の安全性と素因数分解の困難性は等価ではない
  - 素因数分解が解ける→RSA暗号が解読できる、は言えるがその逆は言えない
- そこで、本日は安全性（一方向性）が素因数分解との困難性と等価であることが証明可能な暗号であるRabin暗号を紹介

Rabin暗号

- PとQをともに4で割って3余る素数とし、$N = PQ$とする。
- 公開鍵：N, 秘密鍵(P, Q)
- Fact：P or Qを法とする平方根の計算は容易
  - mod Pでのyの平方根は$\pm y^{\frac{P+1}{4}}\ mod\ P$
- 暗号化：メッセージ$M \in \{0,1, \dots, N-1\}$の暗号文を
  $C \coloneqq M^2\ mod\ N$とする
- 復号：まずCの$mod P, mod\ Q$での平方根M_p, M_qを求める。
  次に、中国人剰余定理で$M = M_\mathrm{p}, mod\ p\ \ M = M_\mathrm{q}$ mod q
  なるM を求める
  - 注：実際にはこのようなMは4通りあるため、そのどれであるかを特定するための補助情報を暗号文に含めておく。（Mがmod PおよびMod Qでそれぞれ平方剰余であるかを補助情報とすればよい）

Rabin暗号の安全性証明

- Rabin暗号を破るのが素因数分解と同じくらい難しいことを示したい
- →Rabin暗号を破る攻撃者が存在したと仮定して、素因数分解を行う**帰着アルゴリズム**を構成する
- アイディア：$M^2 = M'^2 \ mod\ N$なる$M \neq M' mod\ N$が見つかったらNは素因数分解できる（フェルマーの平方差法）
  - $(\mathrm{M}-\mathrm{M}')(\mathrm{M}+\mathrm{M}') \equiv 0\ mod\ N$であり、$|\mathrm{M}-\mathrm{M}'| < N$から、$(\mathrm{M}-\mathrm{M}')$とNの最大公約数を計算すればNの非自明な約数が得られる。

帰着アルゴリズム
入力：合成数N=PQ
出力：素因数分解結果(P, Q)

1. $M \in \{0,1,\dots,N-1\}$をランダムに取って$C := M^2\ mod\ N$を計算
2. Rabin暗号の攻撃者にCを解読してもらい、その出力M'を得る
3. $M = M'$だったら失敗なので諦める
4. そうでなければ上記方法で素因数分解を出力する

目次

- イントロダクション
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号
- 高機能暗号

公開鍵暗号と量子コンピュータ

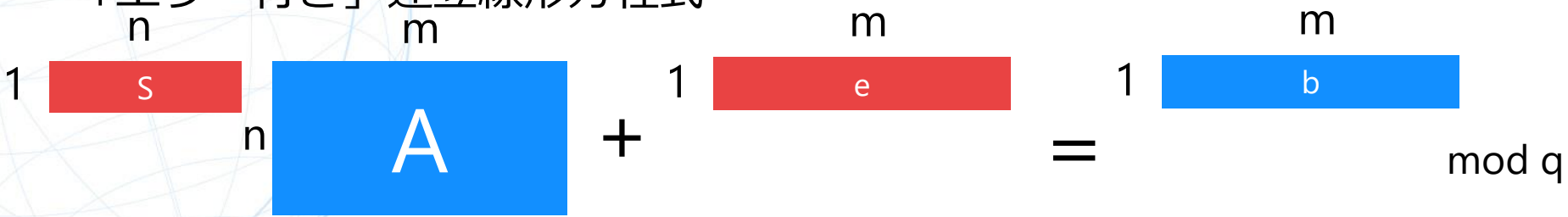
- 現在、世の中で使用されている公開鍵暗号方式の大半はRSA暗号か楕円曲線暗号（楕円曲線群上の離散対数問題の困難性に基づいた暗号）
- 1994年、Shorが量子コンピュータを用いれば素因数分解や離散対数問題が効率的に（多項式時間で）解けることを証明（Shorのアルゴリズム）
  - つまり、**汎用量子コンピュータが完成すれば現在広く使われている公開鍵暗号方式は解読されてしまう！**

耐量子公開鍵暗号

- 近年、量子コンピュータを用いても破られない**耐量子公開鍵暗号**の研究が活発になってきている
  - 量子暗号との違いに注意！
- 2016年、米国標準技術局（NIST）が耐量子公開鍵暗号の選定をスタート、2022-2024年頃までを目途に完了予定
  - 電子署名の標準化も同時進行
- 耐量子公開鍵暗号の候補
  - **格子ベース**、符号ベース、多次多変数多項式ベース、同種写像ベース etc.
  - 今回は格子ベースのうちで**Learning with Errors (LWE)**問題と呼ばれる問題の耐量子困難性に基づく暗号方式を紹介

Learning with Error (LWE)問題

- 「エラー付き」連立線形方程式



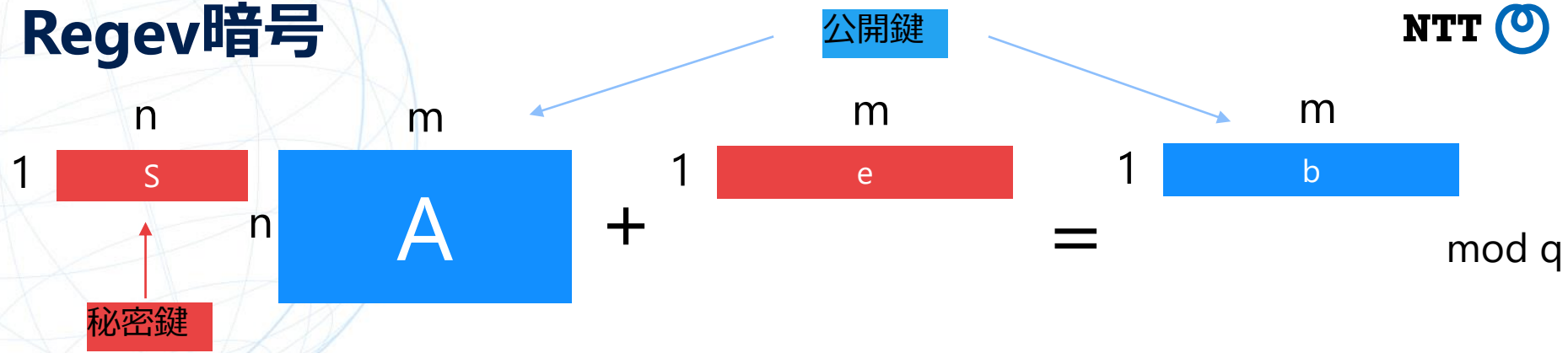
q:素数、s, Aはmod qで一様ランダム、eの各成分はqに比べて"小さい"
（典型的にはeは標準偏差の小さい離散ガウス分布から取る）

- （探索版）LWE問題：Aとbが与えられた時、sを求めよ
  - もしeがなければただの連立方程式なのでガウスの消去法等で簡単に解けるが、小さな「エラー」が追加されるだけで劇的に難しくなる
- （識別版）LWE問題：Aとbが与えられた時、上記の形になっているか、単なるランダム行列とランダムベクトルの組なのか識別せよ。
  - 実は探索版と等価[Regev 09] (qがpolynomial sizeの時)

LWE問題の耐量子困難性

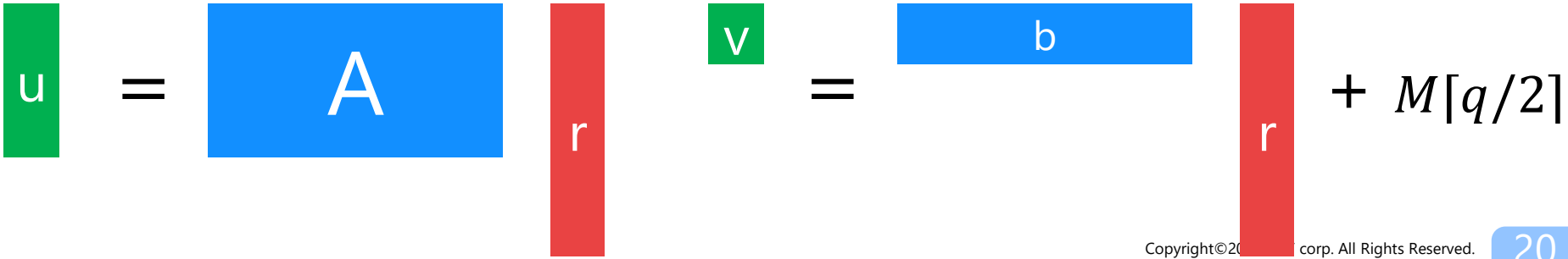
- LWE問題は量子コンピュータでも（多項式時間で）解くのが困難だと信じられている
  - 根拠：RegevはLWE問題が解けるならば格子最短ベクトル（SVP）問題の緩和版が解けることを示した。
  - SVP問題はNP困難なので、量子コンピュータを用いても解けないと信じられている。
  - その緩和版も量子コンピュータを用いても解けないと信じられている。
  - したがって、 LWE問題も量子コンピュータを用いても解けないと信じられている

Regev暗号



暗号化：メッセージ$M \in \{0,1\}$に対して、

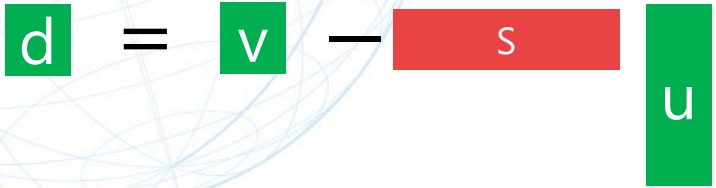
1. $r \in \{0,1\}^m$をランダムに取る
2. 暗号文u, vを以下のように生成



Regev暗号

復号

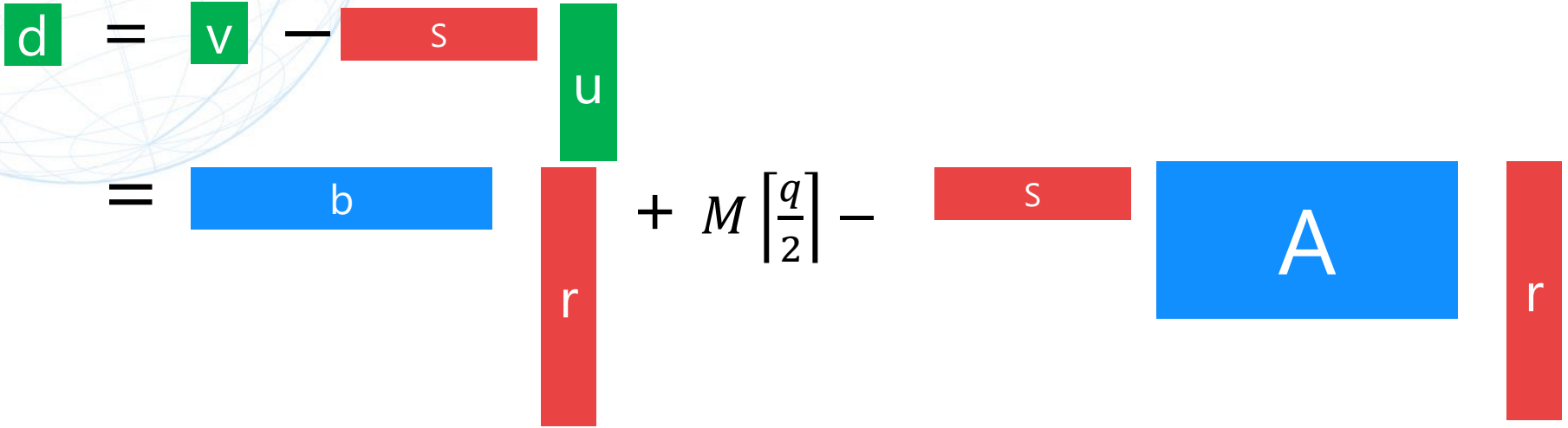
1. dを以下のように計算



Regev暗号

復号

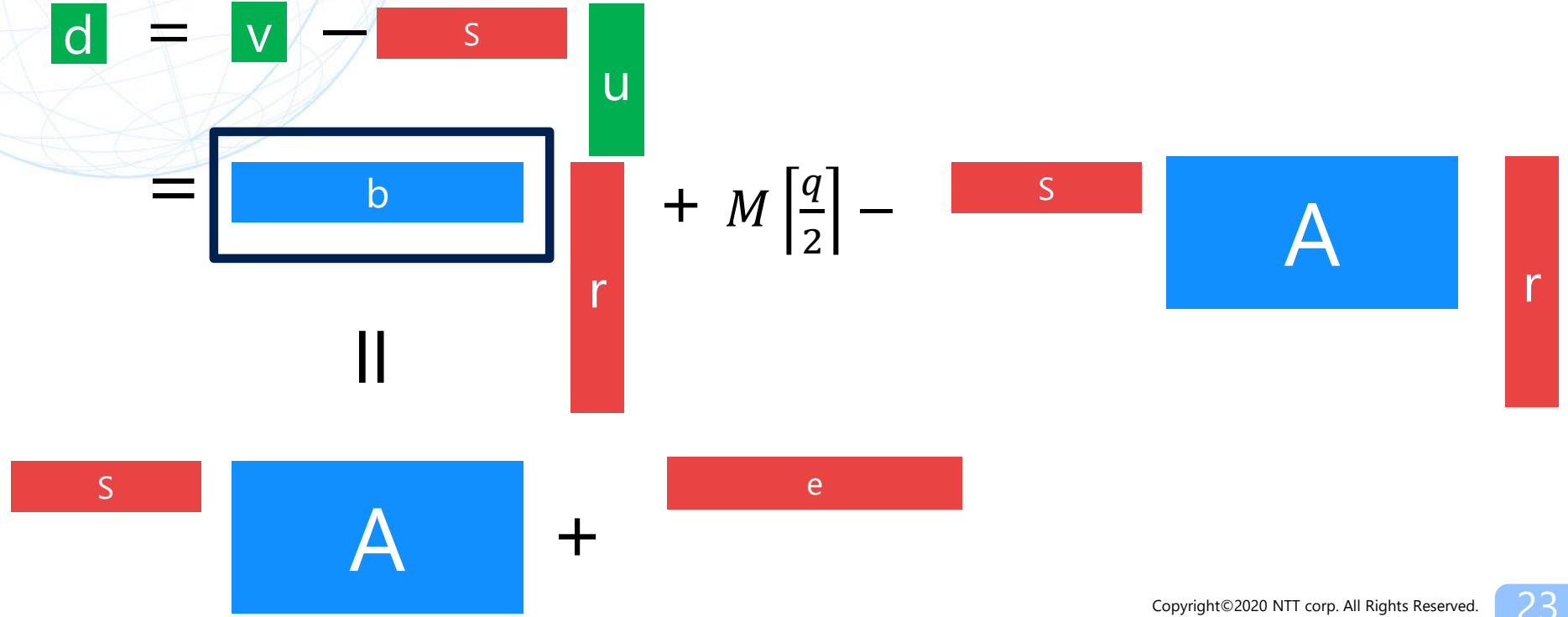
1. dを以下のように計算



Regev暗号

復号

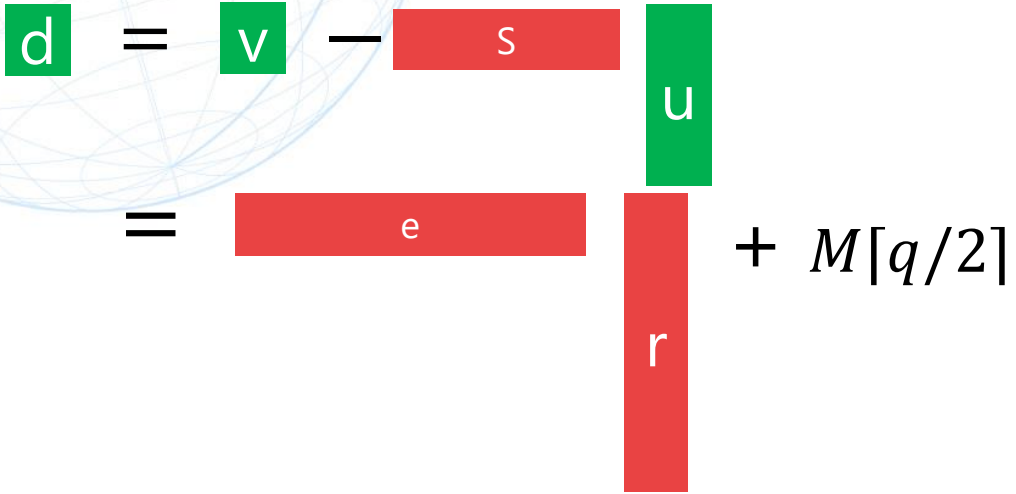
1. dを以下のように計算



Regev暗号

復号

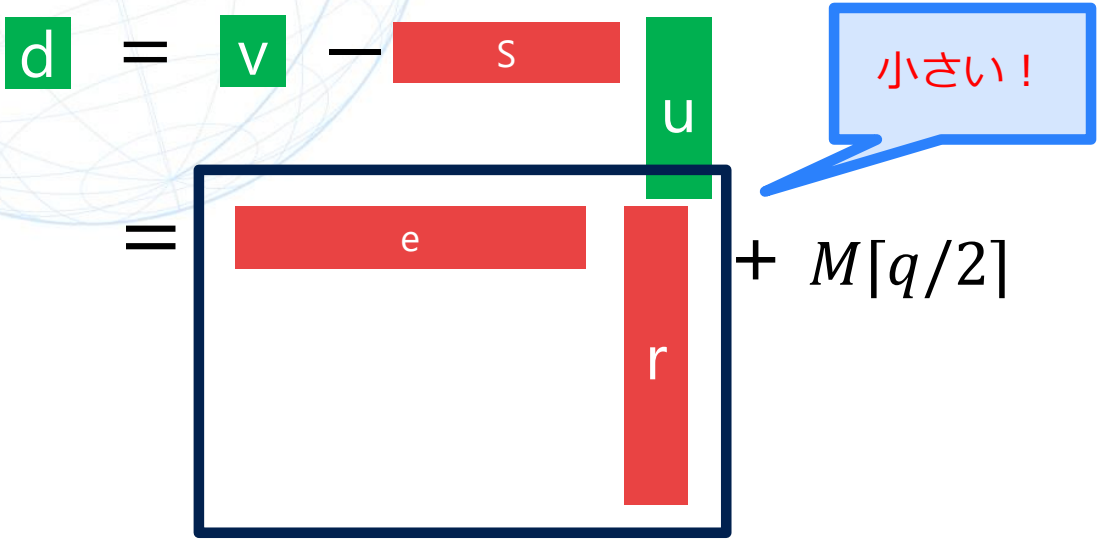
1. dを以下のように計算



Regev暗号

復号

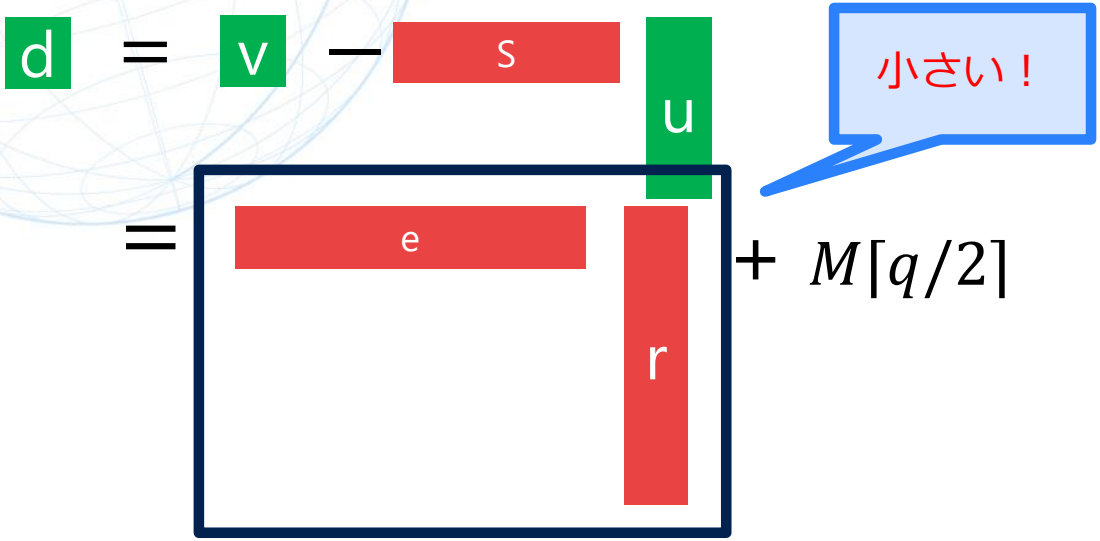
1. dを以下のように計算



Regev暗号

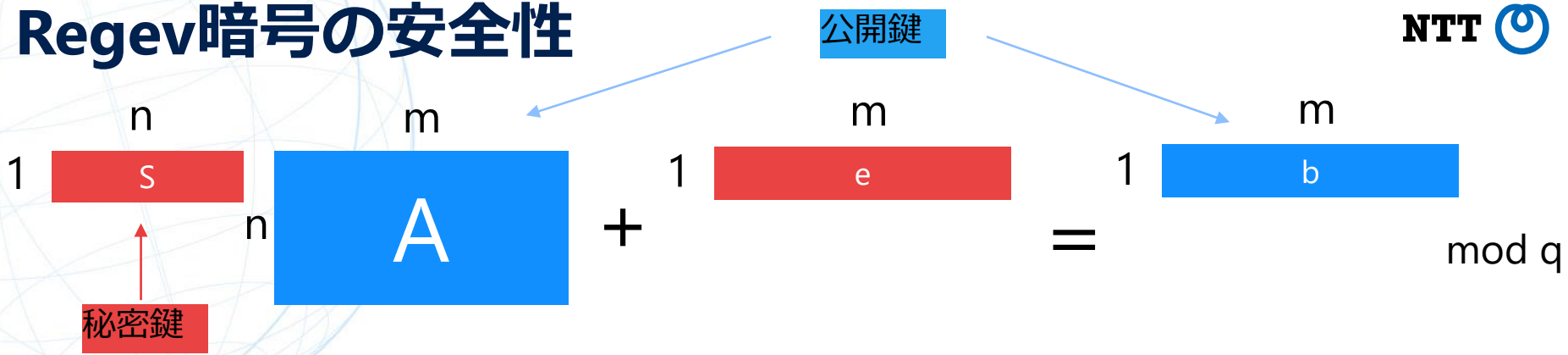
復号

1. dを以下のように計算



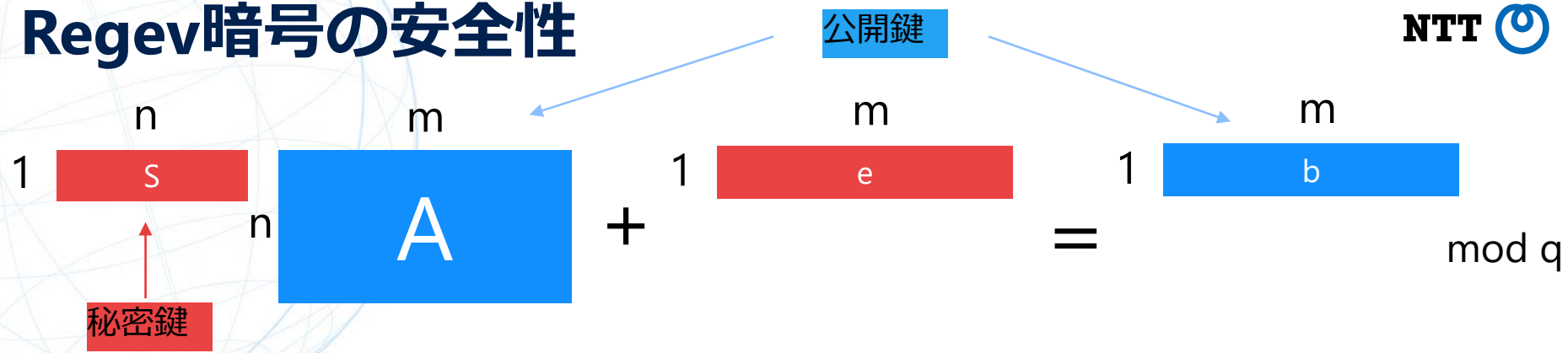
2. dが"0に近ければ"復号結果として0を出力、さもなくば1を出力

Regev暗号の安全性



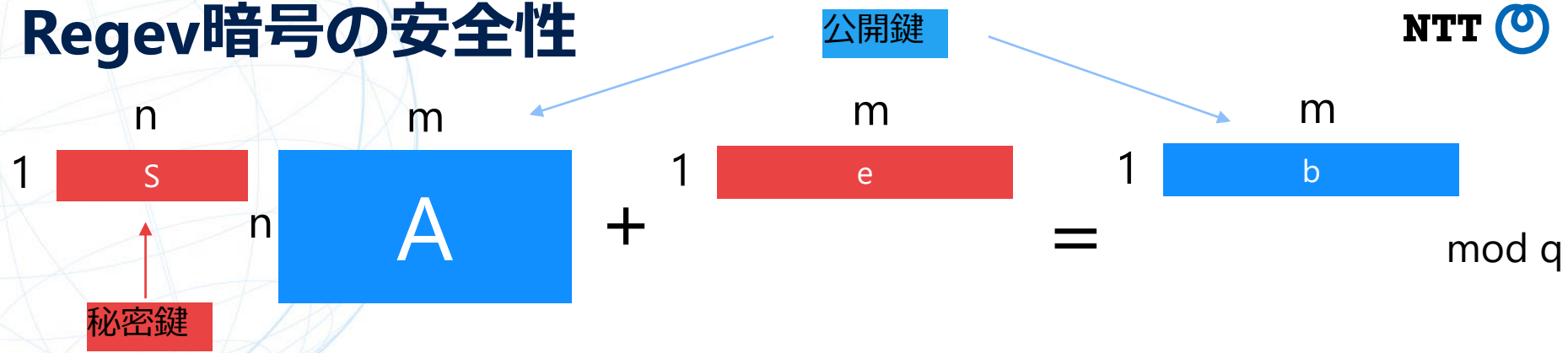
- LWE問題が（耐量子）困難→Regev暗号は（耐量子）安全と言いたい
- 直感：公開鍵から秘密鍵を求めるのはLWE問題そのものである。
  秘密鍵がないと復号できないのでLWE問題が解けなければ復号できない

Regev暗号の安全性



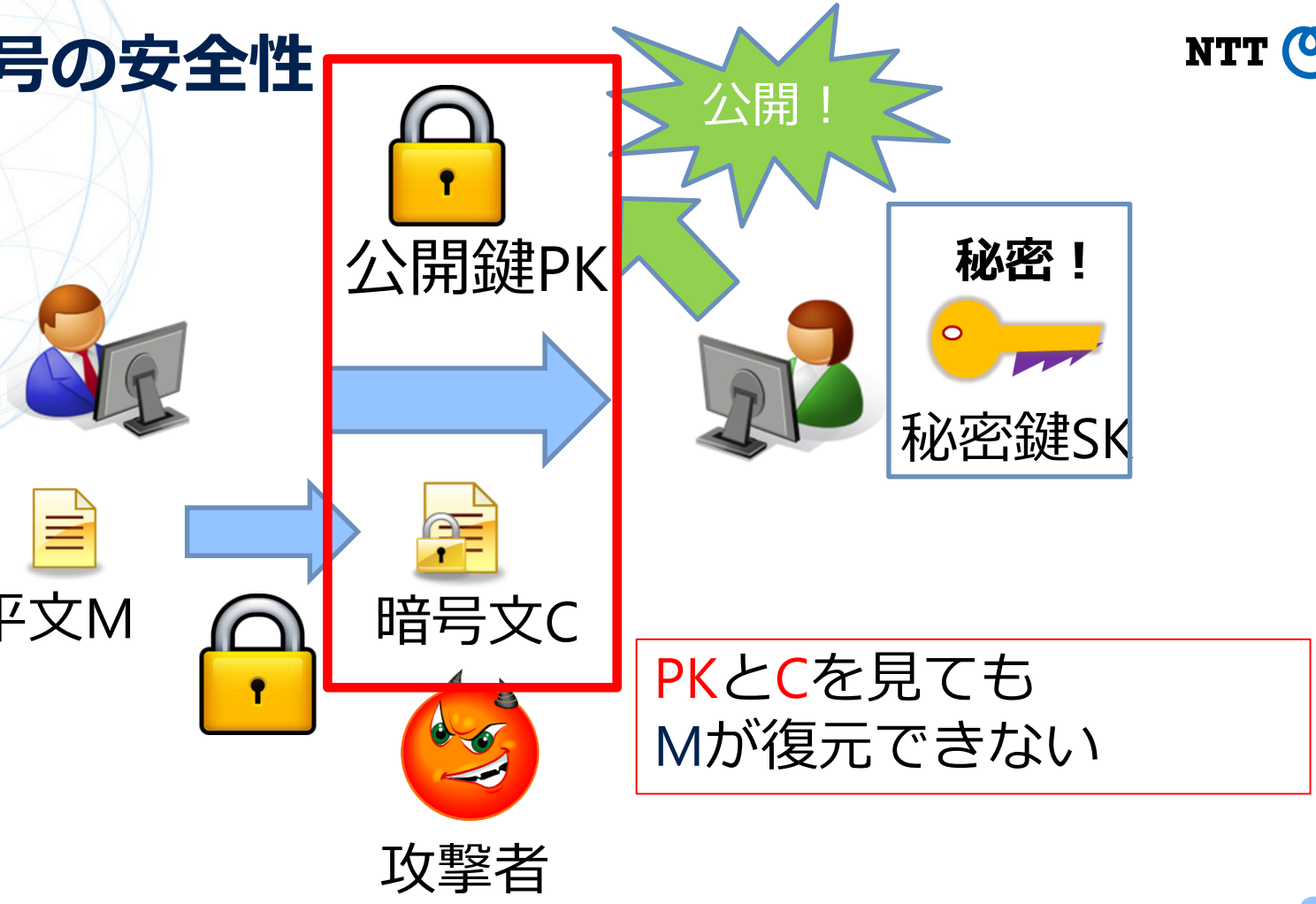
- LWE問題が（耐量子）困難→Regev暗号は（耐量子）安全と言いたい
- 直感：公開鍵から秘密鍵を求めるのはLWE問題そのものである。
  秘密鍵がないと復号できないのでLWE問題が解けなければ復号できない

Regev暗号の安全性



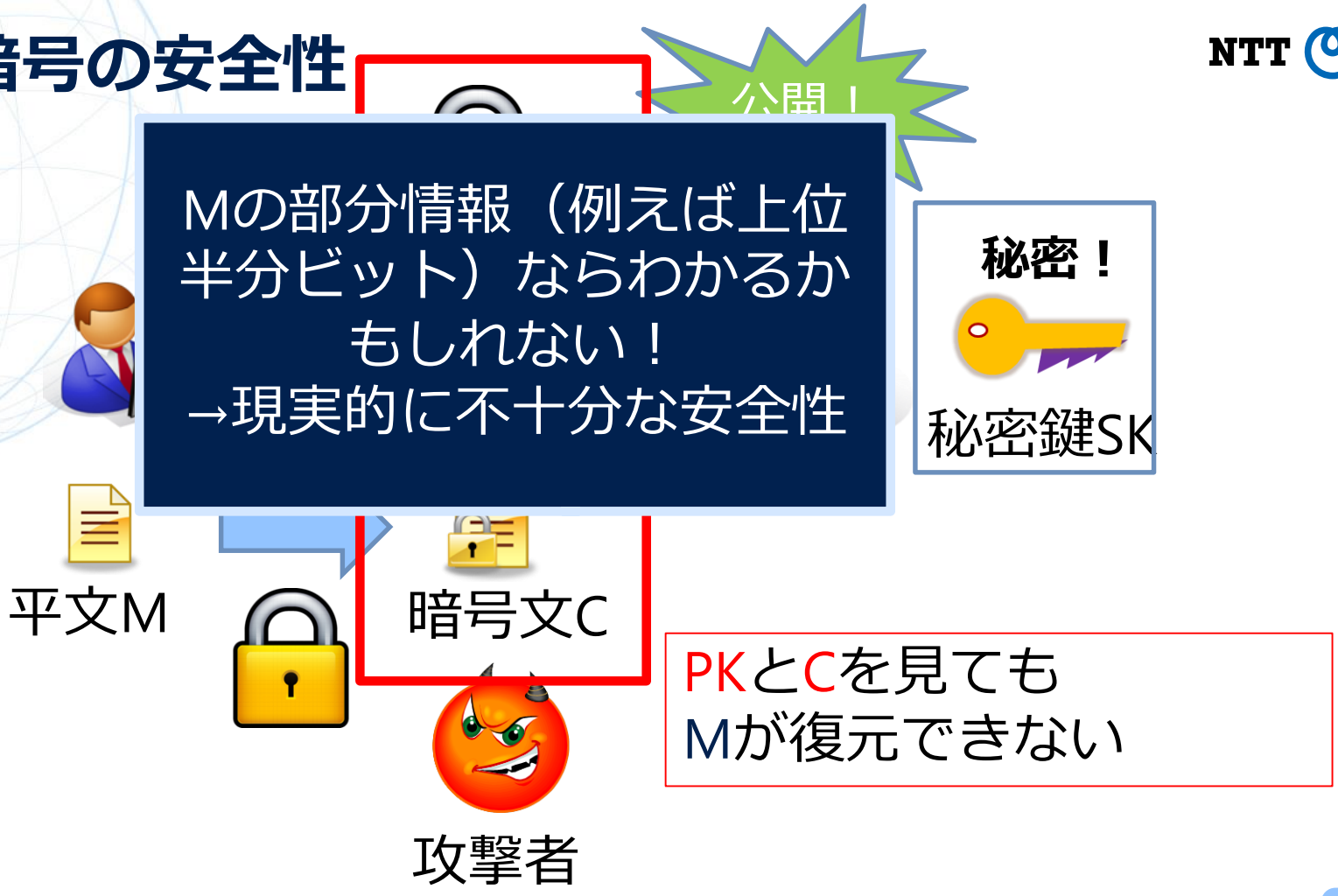
- LWE問題が（耐量子）困難→Regev暗号は（耐量子）安全と言いたい
- 直感：公開鍵から秘密鍵を求めるのはLWE問題そのものである。
  秘密鍵がないと復号できないのでLWE問題が解けなければ復号できない
- 厳密に示すためには、Regev暗号の安全性を破る任意の攻撃者を利用して
  LWE問題を解く**帰着アルゴリズム**を構成することが必要！
  - そのためにはまず暗号の安全性を厳密に定義することが必要

公開鍵暗号の安全性



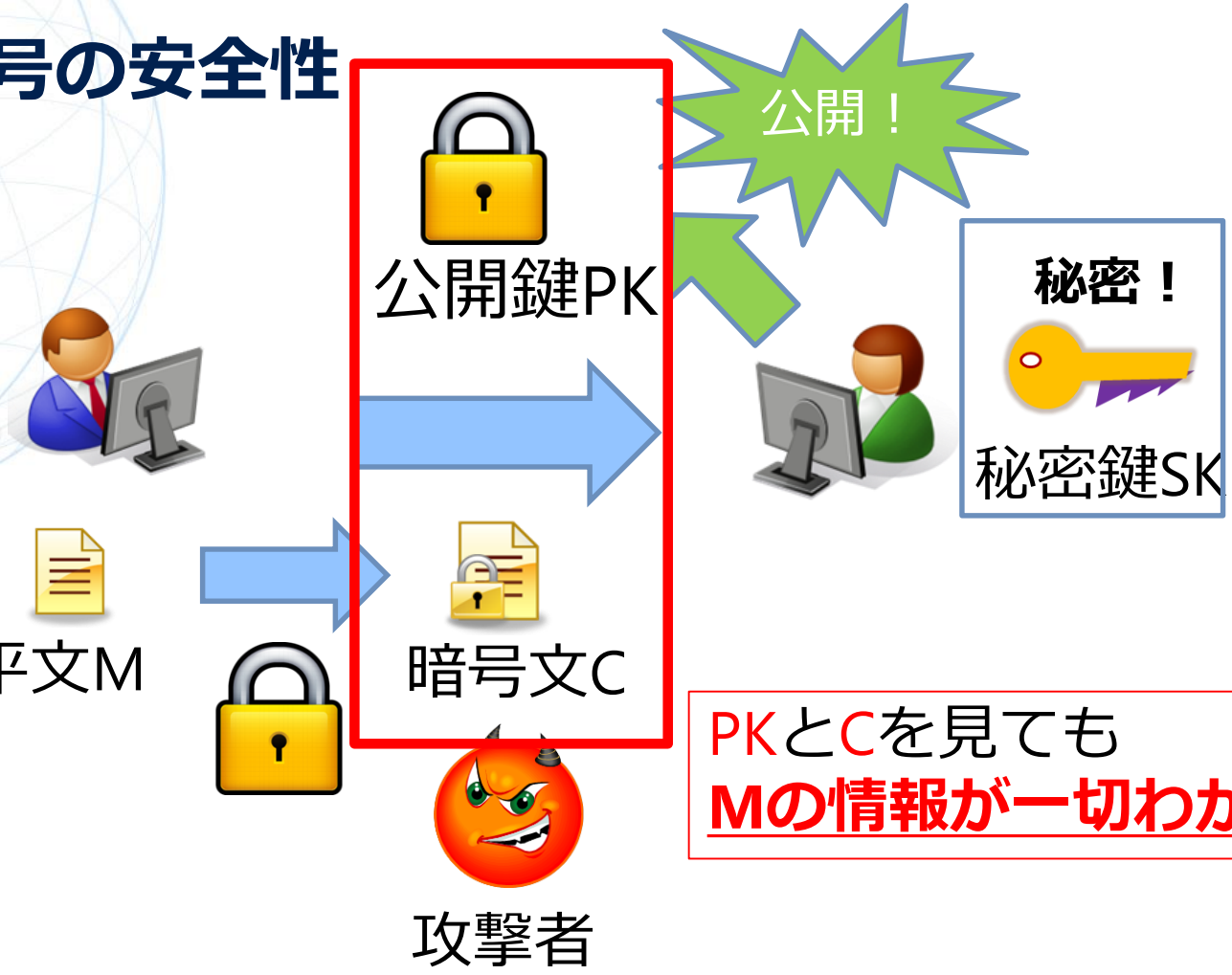
PKとCを見ても
Mが復元できない

公開鍵暗号の安全性



PKとCを見ても
Mが復元できない

公開鍵暗号の安全性



PKとCを見ても
Mの情報が一切わからない

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(1^λ)→(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

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

チャレンジャー

$b \in \{0,1\}$をランダムに選ぶ

PK

M_0, M_1

$C^* = Enc(PK, M_b)$

b'

- 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。

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

チャレンジャー

$b \in \{0,1\}$をランダムに選ぶ

PK

M_0, M_1

$C^* = Enc(PK, M_b)$

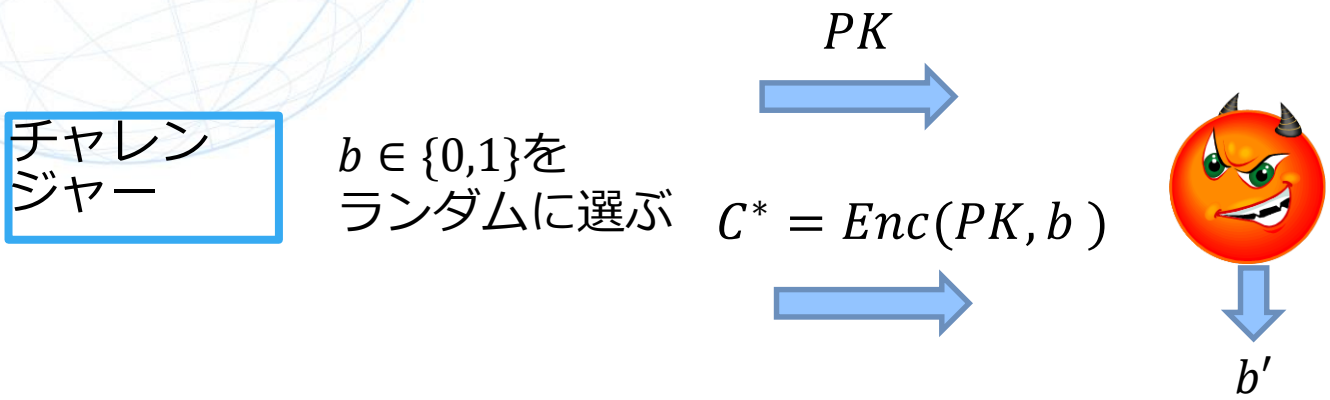
b'

- 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。

セキュリティパラメータ（≒方式の効率）に対して超多項式的に減衰

IND-CPA安全性（１ビット暗号の場合）

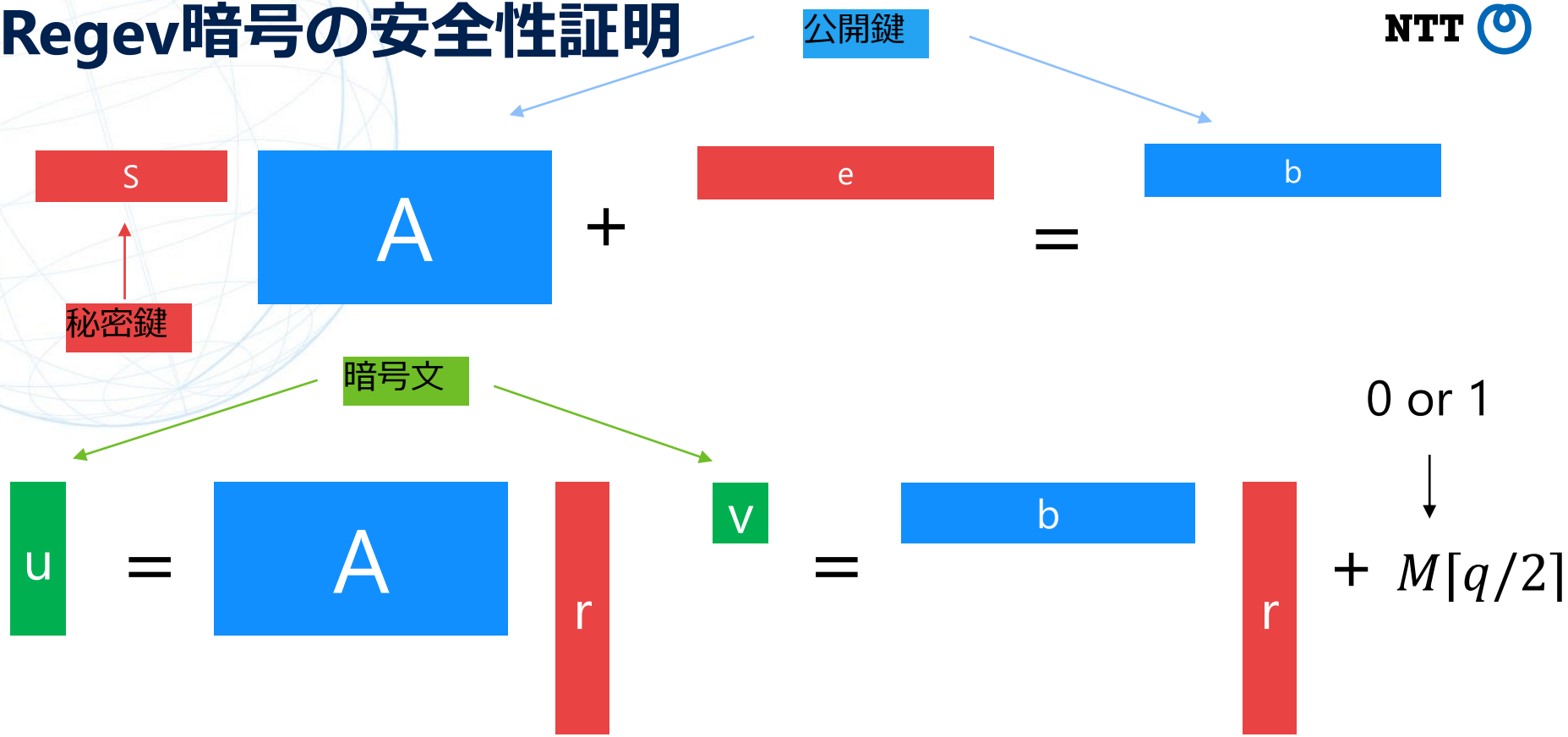
- 「攻撃者がMの情報を一切得られない」ことの数学的定義がIND-CPA安全性（選択平文攻撃に対する識別不可能性）
- 攻撃者と"チャレンジャー"の間の以下のゲームを考える



- 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。

セキュリティパラメータ（≒方式の効率）に対して超多項式的に減衰

Regev暗号の安全性証明



Regev暗号の安全性証明

公開鍵

A

b

Aとbを独立ランダムに選ぶとする。
→(識別)LWE問題の困難性より、
攻撃者の勝利確率は無視可能な程度しか変わらない

暗号文

u = A r

v = b r + $M[q/2]$

0 or 1

Regev暗号の安全性証明

公開鍵

A

b

Aとbを独立ランダムに選ぶとする。
→(識別)LWE問題の困難性より、
攻撃者の勝利確率は無視可能な程度しか変わらない

暗号文

u = A r

v = b r + $M\lfloor q/2 \rfloor$

0 or 1

Aとbが独立ランダムの時、Arとbrの分布もほぼ独立ランダム（Leftover Hash Lemma）
直感的説明：rのエントロピーはm, に対し, u, vの取り得る最大エントロピーは$n\log q$
→m ≫ $n\log q$ ならu, vを一様ランダムにするための"十分なエントロピー"がある

Regev暗号の安全性証明

公開鍵

A

b

Aとbを独立ランダムに選ぶとする。
→(識別)LWE問題の困難性より、
攻撃者の勝利確率は無視可能な程度しか変わらない

暗号文

u

v

uとは無関係の乱数

0 or 1

$= R + M\lfloor q/2 \rfloor$

Aとbが独立ランダムの時、Arとbrの分布もほぼ独立ランダム（Leftover Hash Lemma）
直感的説明：rのエントロピーは$m,$に対し$,u,v$の取り得る最大エントロピーは$n\log q$
→$\mathrm{m} \gg n\log q$ ならu,vを一様ランダムにするための"十分なエントロピー"がある

Regev暗号の安全性証明

公開鍵

A

b

Aとbを独立ランダムに選ぶとする。
→(識別)LWE問題の困難性より、
攻撃者の勝利確率は無視可能な程度しか変わらない

暗号文

u

v

uとは無関係の乱数

0 or 1

$= R + M\lfloor q/2 \rfloor$

Mの情報はRで完全にマスクされているので、このゲームでは攻撃者の勝利確率は1/2
→元々のゲームでの勝利確率は1/2+negl (LWE仮定のもとで)

耐量子暗号＝耐量子仮定を使った暗号？

- Regev暗号のLWE仮定に基づく安全性証明を紹介した
  - LWE仮定が耐量子困難→Regev暗号が耐量子IND-CPA安全
- 安全性証明自体には"量子な議論"は一切出てこない
  - 攻撃者をブラックボックスと考えれば帰着アルゴリズム自体は古典
- 古典の安全性証明＋耐量子仮定→耐量子安全性証明？
- 多くのケースではYes
- しかし例外もあり
  - **ランダムオラクルを用いた安全性証明**
  - 対話プロトコルの安全性証明→明日

目次

- イントロダクション
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号
- 高機能暗号

（古典）ランダムオラクルモデル (ROM) [BR93]

（古典）ランダム関数 $H: X \rightarrow Y$

- ランダム関数を計算する（古典）オラクルを仮定したモデル
  - 現実世界ではハッシュ関数をランダムオラクルとして使う
- 安全性証明のヒューリスティックなモデルとして広く使われる
  - **トラップドア関数→IND-CPA公開鍵暗号**
  - **より強い安全性（IND-CCA安全性）を持った公開鍵暗号**
  - **対話プロトコルの非対話化（Fiat-Shamir Transform）→明日 etc.…**

量子ランダムオラクルモデル (QROM) [BDF+11]

（古典）ランダム関数 $H: X \to Y$

- ランダムオラクルに量子アクセスを許すのが量子ランダムオラクル
  - 耐量子安全性を考える際には攻撃者がハッシュ関数を量子重ね合わせで計算するかもしれないのでこのようにモデルを変形することが必要
- 古典ランダムオラクルモデルでの安全性証明は攻撃者のオラクルクエリが古典であることを本質的に使用していることが多いため、単純には量子ランダムオラクルモデルでの安全性証明に**拡張出来ない**ことが多い

→安全性証明内で"量子"な議論が必要

ROM vs QROM

- ROMとQROMの"パワー"に差はあるのか？
- ある"タスク"（= **Fourier Sampling** ）が存在してQROMではクエリ1回で出来るが、ROMでは指数回のクエリが必要[Aaronson10]
  - Fourier Sampling: 関数$H:\{0,1\}^n \to \{\pm 1\}$がオラクルとして与えられた時、確率$\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot z}H(x)\right)^2$で$z \in \{0,1\}^n$をSampleせよ
- ROMでは安全だがQROMでは安全でない暗号は存在するか？
  - 「Fourier Samplingが解けるならば解読出来る」ような暗号を設計する方法は知られていないので、上記例は暗号の文脈では使えない
- YES (LWE仮定のもとで) [YZ20] (based on [BKVV20])
- ROMで安全でもQROMで安全とは限らないので、ROMで安全と証明されていてもQROMでの安全性証明が別途必要

トラップドア関数 (TDF)

- 単射関数$F: X \to Y$が（耐量子）TDFとは次を満たすこと
  - **（耐量子）一方向性**：ランダムな$x \in X$について$y = F(x)$が与えられた時、（量子）多項式時間アルゴリズムがxを出力できる確率は無視可能
  - **トラップドアが存在**：あるトラップドアtdが存在して、tdが与えられた場合$F(x)$からxを古典多項式時間で復元可能
- LWE等の標準的仮定からTDFの構成が知られている
  - 耐量子でなくてよければ素因数分解の困難性からも構成可能（RSA暗号 etc）
- Fを暗号化アルゴリズムと見ることで一方向性を満たす公開鍵暗号の特別ケース（暗号化が決定的）とも見れる
  - 暗号化が決定的なのでIND-CPA安全性は満たすことが出来ない

TDF+ランダムオラクル→IND-CPA安全な公開鍵暗号[BR93]

- トラップドア関数$F: X \to Y$とランダムオラクル$H: X \to \{0,1\}^{\ell}$を仮定
- 公開鍵：F, 秘密鍵: td
- 暗号化：平文$M \in \{0,1\}^{\ell}$に対して、乱数$x \in X$をランダムに取り、暗号文$(y := F(x), c := M \oplus H(x))$を出力
- 復号：トラップドアtdを使って$x = F^{-1}(y)$を計算し、$M = C \oplus H(x)$を出力
- 定理[BR93]: Fが一方向性を満たすならば上記方式は（古典）ランダムオラクルモデルでIND-CPA安全

古典ランダムオラクルモデルでの安全性証明

NTT

- トラップドア関数$F: X \to Y$と暗号文$\left(y := F(x), c := M \oplus H(x)\right)$を受け取った時、Mの情報が隠れていることを示せばよい
  - 多項式時間攻撃者はFと$y := F(x)$が与えられた時、$H(x)$をランダムビット列と識別出来ない（$=H$はFのハードコア関数である）ことを示せばよい。
- 古典ランダムオラクルモデルにおいて、$H(x)$の情報を得る唯一の方法はxをランダムオラクルにクエリすること
- $H(x)$をランダムと識別できる→xをクエリする確率が無視不可能→Fの一方向性を破っている
- Fが一方向性を満たす→上記方式はIND-CPA安全 QED.

古典ランダムオラクルモデルでの安全性証明

NTT

- トラップドア関数$F: X \to Y$と暗号文$\left(y := F(x), c := M \oplus H(x)\right)$を受け取った時、Mの情報が隠れていることを示せばよい
  - 多項式時間攻撃者はFと$y := F(x)$が与えられた時、$H(x)$をランダムビット列と識別出来ない（$=H$はFのハードコア関数である）ことを示せばよい。
- **古典ランダムオラクルモデルにおいて、$H(x)$の情報を得る唯一の方法はxをランダムオラクルにクエリすること**
- $H(x)$をランダムと識別[illegible]$\to x$をクエリする確率が無視不可能$\to F$の
- Fが一

量子の場合そうとは言えない

e.g., $\frac{1}{\sqrt{|X|}}\sum_{x\in X}|x\rangle$をクエリ→$\frac{1}{\sqrt{|X|}}\sum_{x\in X}|x\rangle\,|H(x)\rangle$

→ある意味全ての$x \in X$に対する$H(x)$の"情報"を一回のクエリで得ている

量子ランダムオラクルモデルでの安全性証明

NTT

- 示したい事：攻撃者は$H(x)$とランダムが識別できる
  →攻撃者を使ってxを計算できる

One-Way to Hiding Lemma [Unruh 15]
$A: H$にq回量子クエリするアルゴリズム、$x \in X, z := H(x), z' \leftarrow \{0,1\}^{\ell}$とすると

$$|\Pr[1 \leftarrow A^H(z)] - \Pr[1 \leftarrow A^H(z')]| \leq 2q\sqrt{\epsilon}$$

$\epsilon := \Pr[$Aのクエリをランダムに一つ選んで観測した結果$= x]$

- 上記Lemmaより、
  もし攻撃者は$H(x)$とランダムと識別出来る確率が無視不能
  →Aのクエリをランダムに一つ選んで観測するとxになる確率が無視不能
  →これを使って量子ランダムオラクルモデルでもFの一方向性に帰着可

One-Way to Hiding Lemmaの証明（概略）

NTT

- 示したい事：$|\Pr[1 \leftarrow A^H(H(x))] - \Pr[1 \leftarrow A^H(z')]| \leq 2q\sqrt{\epsilon}$

  $\epsilon := \Pr[\text{Aのクエリをランダムに一つ選んで観測した結果} = x]$

今、H'を$H'(x') := \begin{cases} H(x') & \text{if } x' \neq x \\ z' & \text{if } x' = x \end{cases}$ とすると、

$$\Pr[1 \leftarrow A^H(z')] = \Pr[1 \leftarrow A^{H'}(H(x))]$$

なので、$|\Pr[1 \leftarrow A^H(H(x))] - \Pr[1 \leftarrow A^{H'}(H(x))]| \leq 2q\sqrt{\epsilon}$
を示せば良い

任意の固定されたx, Hに対してこれが成り立つことを示す

One-Way to Hiding Lemmaの証明（概略）

NTT

- 示したい事：$|\Pr[1 \leftarrow A^{H}(H(x))] - \Pr[1 \leftarrow A^{H'}(H(x))]| \leq 2q\sqrt{\epsilon}$

$\epsilon := \Pr[\text{Aのクエリをランダムに一つ選んで観測した結果} = x]$

$|\psi_i\rangle$:オラクルがHの時のi回目のクエリ直前の状態

$|\psi'_i\rangle$:オラクルがH'の時のi回目のクエリ直前の状態

明らかに、$|\psi_1\rangle = |\psi'_1\rangle$

一方、$\mathrm{TD}(|\psi_{i+1}\rangle, |\psi'_{i+1}\rangle) \leq \mathrm{TD}(|\psi_i\rangle, |\psi'_i\rangle) + 2|\Pi_x|\psi_i\rangle|$

(Π_x：クエリレジスタがxである状態への射影)

直感的説明：HとH'は入力xの時しか相違しないので差は

"xをクエリした成分"からしか生じない（証明は[Unruh15]参照）

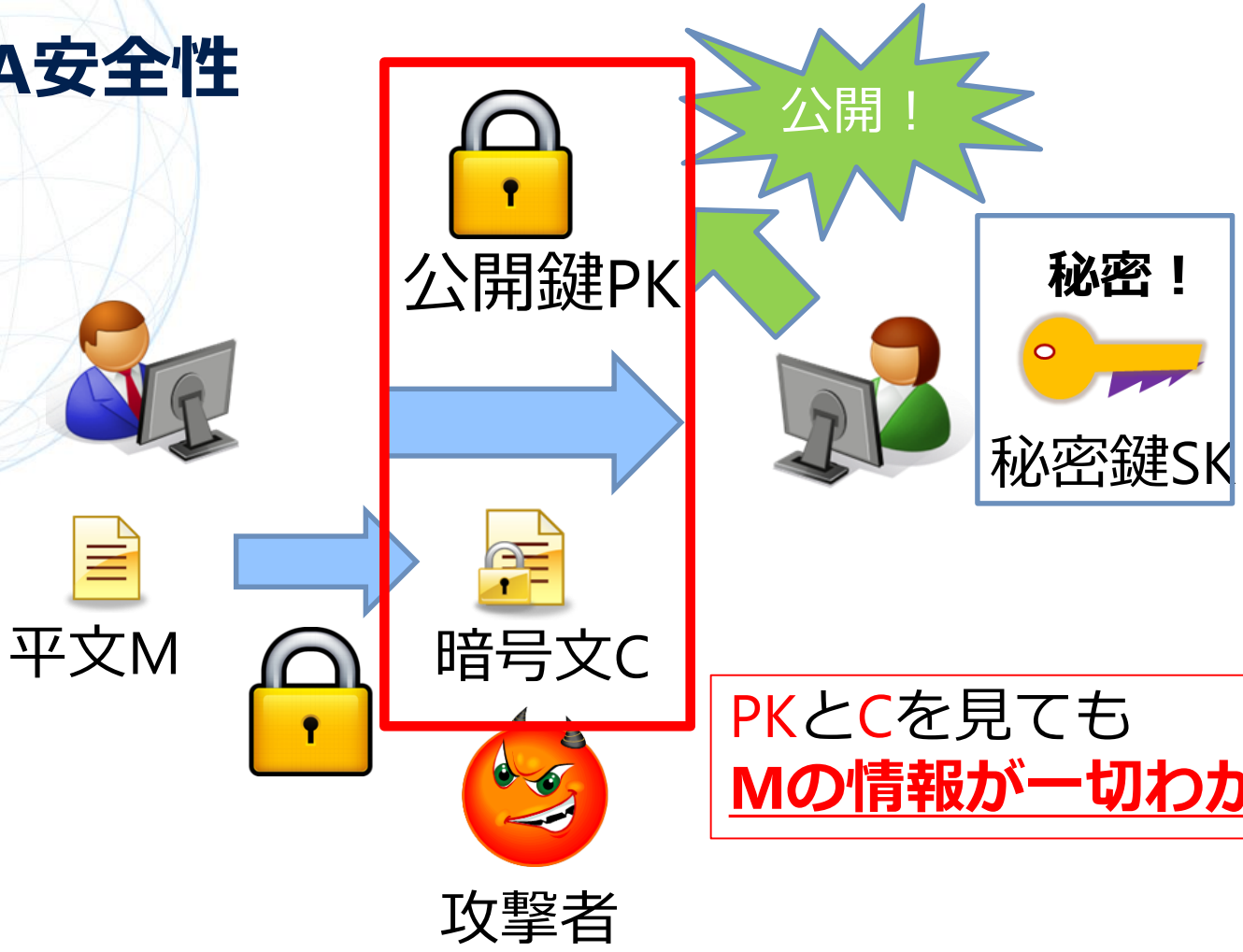
示したい式の左辺$\leq \mathrm{TD}(|\psi_{q+1}\rangle, |\psi'_{q+1}\rangle) \leq \sum_{i\in\{1,..,q\}} 2|\Pi_x|\psi_i\rangle|$

$$\leq 2\sqrt{q\sum_{i\in\{1,..,q\}}|\Pi_x|\psi_i\rangle|^2} = 2q\sqrt{\epsilon}$$

目次

- イントロダクション
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号
- 高機能暗号

IND-CPA安全性



PKとCを見ても
Mの情報が一切わからない

IND-CCA安全性

公開鍵PK

公開！

秘密！

秘密鍵SK

平文M

暗号文C

$C'(\neq C)$

復号オラクル

M'

攻撃者

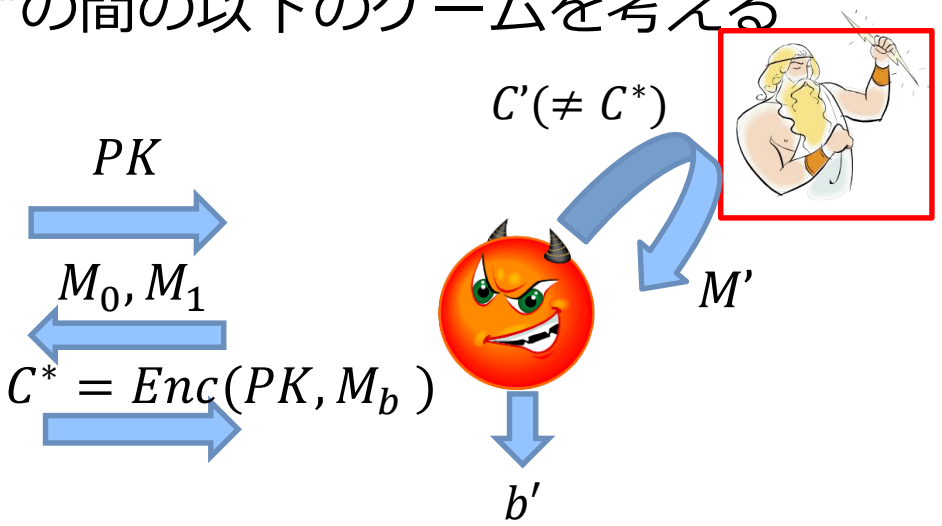
PKとCを見て更に**復号オラクル**が与えられても
Mの情報が一切わからない

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

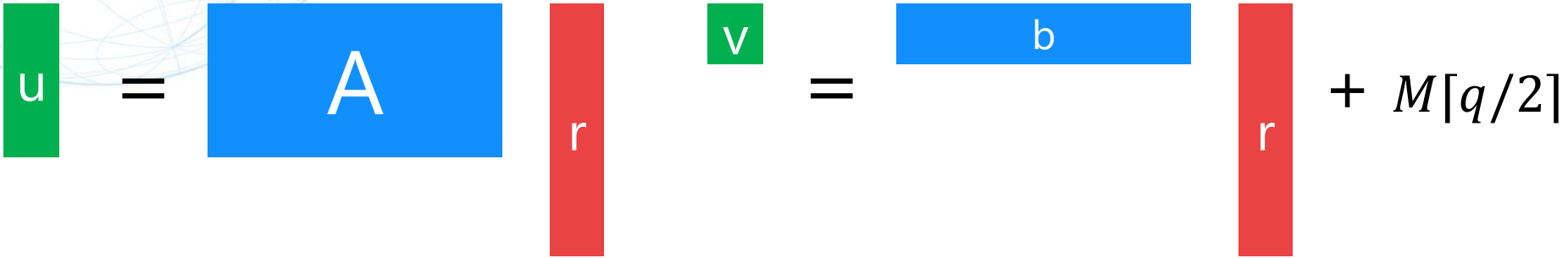
チャレンジャー

$b \in \{0,1\}$を
ランダムに選ぶ



- 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。

Regev暗号はIND-CCA安全でない



$v' = v + 1$として、(u, v')を復号オラクルにクエリ
→高い確率でMが得られる

何故IND-CCA安全性を考えるのか？

- 現実世界には通常復号オラクルは存在しない
  →IND-CCA安全性は強すぎる安全性を要求しているのでは？
- 実際90年代後半頃までINC-CPA安全性で十分と考えられていた
- 98年、BleichenbacherはPKCS#1 v1.5と呼ばれる当時のRSA暗号の標準仕様の一つに攻撃が可能であることを示した
  - 仕様上"部分的な"復号オラクルを攻撃者が得られたことに起因
- それ以降、実用上の要求としてIND-CCA安全性が必須とされるようになった
  - NISTの耐量子標準化でもほとんどの提案方式はIND-CCA安全

ハイブリッド暗号

- 実際に公開鍵暗号を実用する際には**ハイブリッド暗号**という手法を使うのが標準的
  - 公開鍵暗号で共通鍵暗号の鍵を暗号化、その鍵を用いて平文を共通鍵暗号で暗号化
- 公開鍵暗号部分で暗号化すべきは共通鍵暗号の鍵のみ
  - 公開鍵暗号部分の平文を自由に選べる必要なし
    →**KEM(Key Encapsulation Mechanism)**で十分

暗号化の際に平文を入力に取らず、
暗号文とその中に暗号化された"鍵"を出力する

Key Encapsulation Mechanism

- KEMは以下のアルゴリズムからなる

KeyGen(1^{λ})→(PK,SK)

Enc(PK)→(C,K)

Dec(SK,C)→K

- 正当性：　Dec(SK, Enc(PK))=K
- IND-CPA安全性：Cが与えられた時Kはランダムと識別不能
- IND-CCA安全性：Cと復号オラクルが与えられた時
  Kはランダムと識別不能

ハイブリッド暗号

PKE. Enc (pk, m)

1. $(c_{KEM}, K) \leftarrow \mathrm{KEM.Enc}(pk)$
2. $c_{SKE} \leftarrow \mathrm{SKE.Enc}\ (K, m)$
3. 暗号文(c_{KEM}, c_{SKE})を出力

PKE. Dec $(sk, (c_{KEM}, c_{SKE}))$

1. $K \leftarrow \mathrm{KEM.Dec}(sk, c_{KEM})$
2. $m \leftarrow \mathrm{SKE}.Dec\ (K, c_{SKE})$
3. mを出力

（※ PKE:公開鍵暗号 SKE:共通鍵暗号）

簡単に作れる

IND-CCA安全KEM+IND-CCA安全SKE→IND-CCA PKE

→IND-CCA安全PKEを作るにはIND-CCA安全KEMを作れば十分

TDF+ランダムオラクル→IND-CCA安全なKEM

NTT

- トラップドア関数$F: X \to Y$とランダムオラクル$H: X \to \{0,1\}^{\ell}$を仮定
- 公開鍵：F, 秘密鍵: td
- 暗号化：乱数$x \in X$をランダムに取り、
  暗号文$y := F(x)$および鍵$K = H(x)$を出力
- 復号：トラップドアtdを使って$x = F^{-1}(y)$を計算し、
  $K = H(x)$を出力
- 定理[BDF+11]: Fが一方向性を満たすならば上記方式は
  量子ランダムオラクルモデルでIND-CCA安全

IND-CCA安全性の証明

公開鍵：F, 秘密鍵: td
暗号化：乱数$x \in X$をランダムに取り、
　　暗号文$y := F(x)$および鍵$K = H(x)$を出力
復号：$x = F^{-1}(y)$を計算し、 $K = H(x)$を出力

量子多項式攻撃者Aに対して、以下のゲームを考える
ゲーム*1:*

$x^* \leftarrow$ random, $y^* \leftarrow F(x^*)$, $K_1 := H(x^*)$, $K_0 \leftarrow$ random, $b \leftarrow \{0,1\}$
Aは(y^*, K_b)と復号オラクルと量子ランダムオラクルを与えられる

この時Aがbを当てられる確率≈1/2
→IND-CCA安全

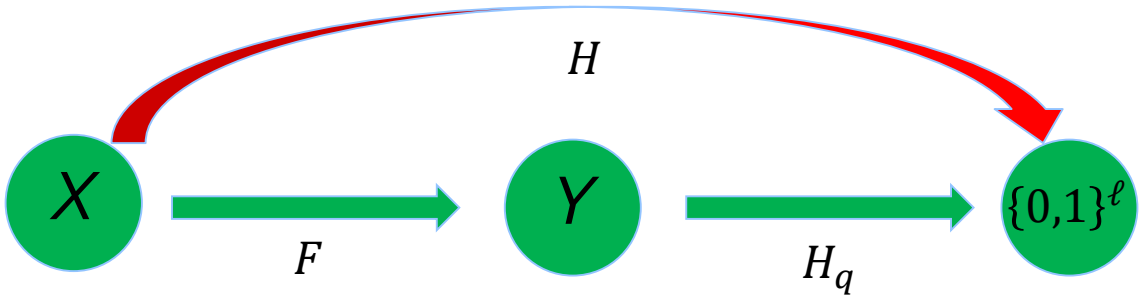
IND-CCA安全性の証明

公開鍵：F, 秘密鍵: td
暗号化：乱数$x \in X$をランダムに取り、
　　暗号文$y := F(x)$および鍵$K = H(x)$を出力
復号：$x = F^{-1}(y)$を計算し、 $K = H(x)$を出力

ゲーム2:
Hを単なるランダム関数とする代わりに、別のランダム関数H_qを使って

$$H(x) := H_q \circ F\ (x)$$

と定める

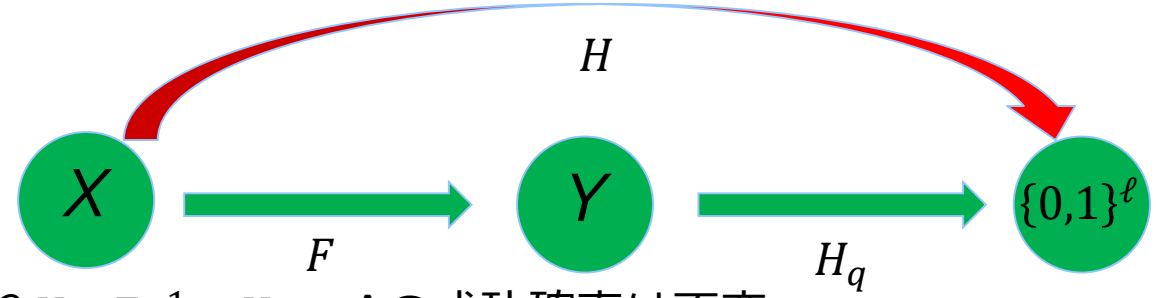


Fは単射なので、このようにしてもHはランダム関数→Aの成功確率は不変

IND-CCA安全性の証明

公開鍵：F, 秘密鍵: td
暗号化：乱数$x \in X$をランダムに取り、
　　暗号文$y := F(x)$および鍵$K = H(x)$を出力
復号：$x = F^{-1}(y)$を計算し、 $K = H(x)$を出力

ゲーム3:
復号オラクルは$H(F^{-1}(y))$を計算する代わりに$H_q(y)$を計算



図より$H \circ F^{-1} = H_q$ →Aの成功確率は不変
この時点でゲームを実行するのに**トラップドアが不要**に！

IND-CCA安全性の証明

公開鍵：F, 秘密鍵: td
暗号化：乱数$x \in X$をランダムに取り、
　　暗号文$y := F(x)$および鍵$K = H(x)$を出力
復号：$x = F^{-1}(y)$を計算し、 $K = H(x)$を出力

ゲーム*3:*

$x^* \leftarrow$ random, $y^* \leftarrow F(x^*)$, $K_1 := H(x^*) = H_q(y^*)$, $K_0 \leftarrow$ random, $b \leftarrow \{0,1\}$
Aは(y^*, K_b)と以下の二つのオラクルを与えられる
変形復号オラクル：$y \neq y^*$を入力として$H_q(y)$を出力
変形量子ランダムオラクル：xを入力として$H_q(F(x))$を出力

One-Way-to-Hiding Lemmaより、K_0とK_1が識別出来る
→ x^*が見つけられる→Fの一方向性が破れる
よってFの一方向性のもとで上記方式はIND-CCA安全

帰着ロスについて

- IND-CCA攻撃者の識別確率ϵ→TDFが確率$\epsilon' \approx \frac{\epsilon^2}{q^2}$で破れる
  - One-Way To Hiding Lemmaを適用： $\epsilon = O(q\sqrt{\epsilon'})$
- $\epsilon = 2^{-128}, q = 2^{80}$とすると、TDFは確率$2^{-416}$でも破れないようにする必要がある
  - 非常に大きなパラメータ増大→効率悪化
- 理想：IND-CCA攻撃者の識別確率ϵ→TDFが確率ϵで破れる（**タイト帰着**）
- TDFにより強い安全性を仮定すればタイト帰着可能[SXY18]
- TDFの安全性そのままでもよりタイトな帰着も研究されてきている
  - $\epsilon' \approx \epsilon^2$ [BHH+19]
  - $\epsilon' \approx \frac{\epsilon}{q}$ [KSSS20]

TDFの作り方

- TDFとランダムオラクルを用いてIND-CCA暗号を作る方法を紹介した
- TDFを作る方法は？
  - 具体的構成（e.g., [GPV08]）
  - **PKE+derandomization**
- $F(x) := Enc(x; H(x))$
- 元々のPKE方式が一方向⇒Fの一方向性が示せる
  - One-Way-to-Hiding Lemmaを使う

IND-CPA安全→IND-CCA安全への変換

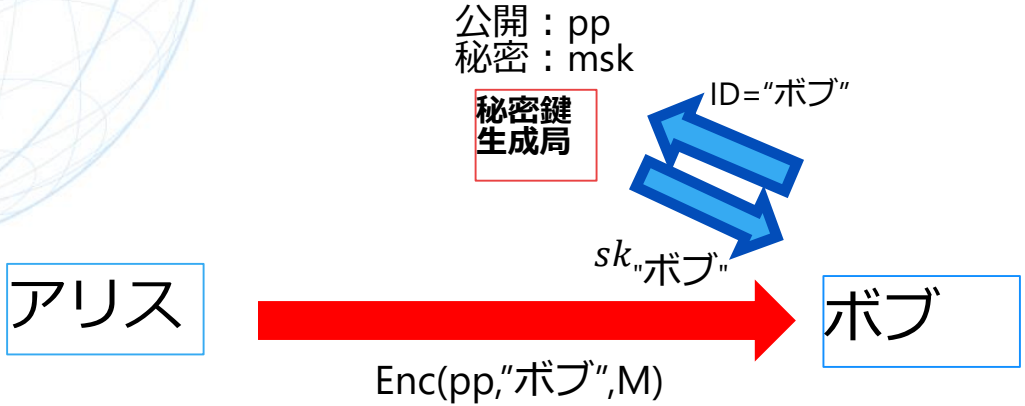
- 藤崎岡本変換と呼ばれる変換（の1バージョン）[FO13]
  - 量子ランダムオラクルモデルでの安全性証明[TU16, HHK17 etc.]
  - NISTの標準化候補でも多くの候補がこの変換（かその変形）を使用
- （量子）ランダムオラクルモデルを使わずにIND-CPA安全からIND-CCA安全へ変換できるかは数十年来の未解決問題
  - 最近のブレークスルーでTDF→IND-CCA安全な公開鍵暗号は示された[HKW20]

目次

- イントロダクション
- 素因数分解に基づく公開鍵暗号(Rabin暗号)
- 耐量子公開鍵暗号（Regev暗号）
- 量子ランダムオラクルモデル
- 選択暗号文攻撃（CCA）安全な公開鍵暗号
- 高機能暗号

IDベース暗号

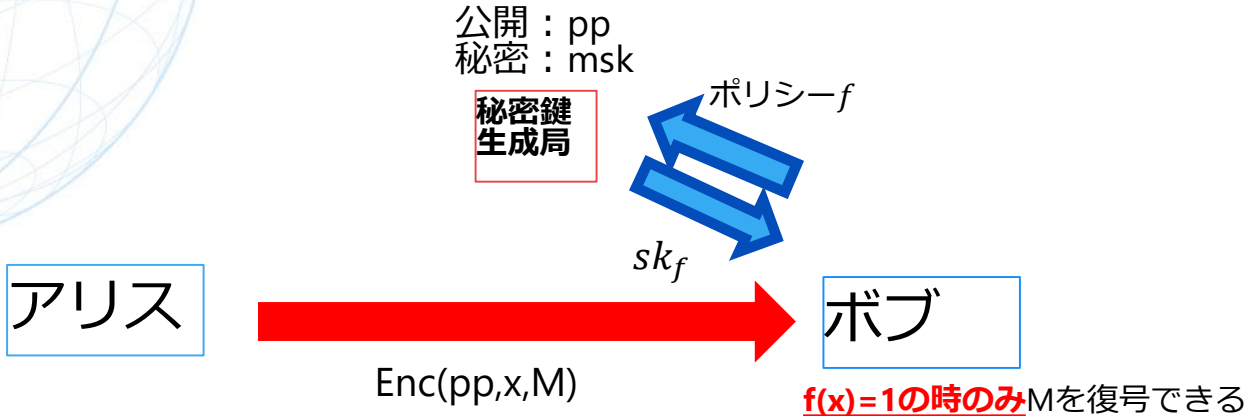
- 任意の文字列を公開鍵に出来る暗号
  - 公開鍵とIDの紐づけが不要



- LWEに基づく構成：[GPV08,ABB10,CHKP10…]

属性ベース暗号

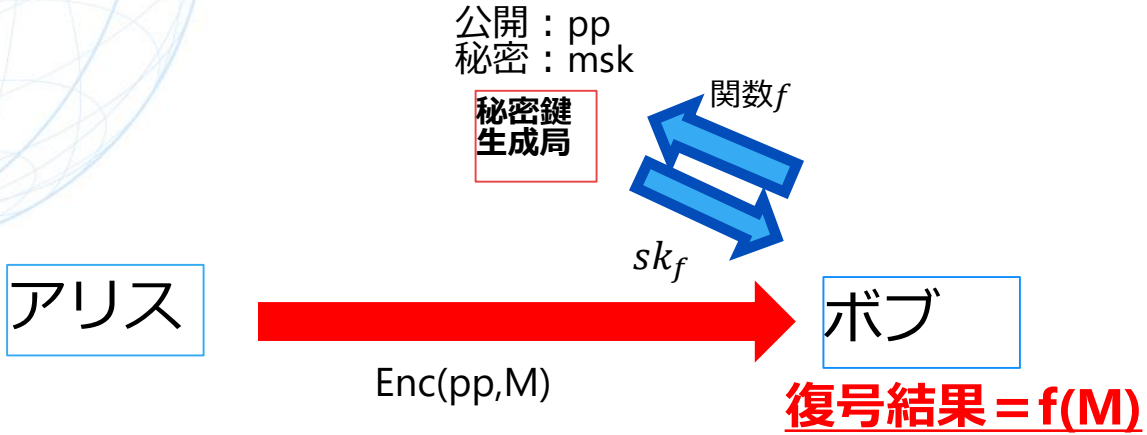
- ポリシーを用いたアクセスコントロール



- LWEに基づく構成：[GVW15,BGG+14…]

関数型暗号

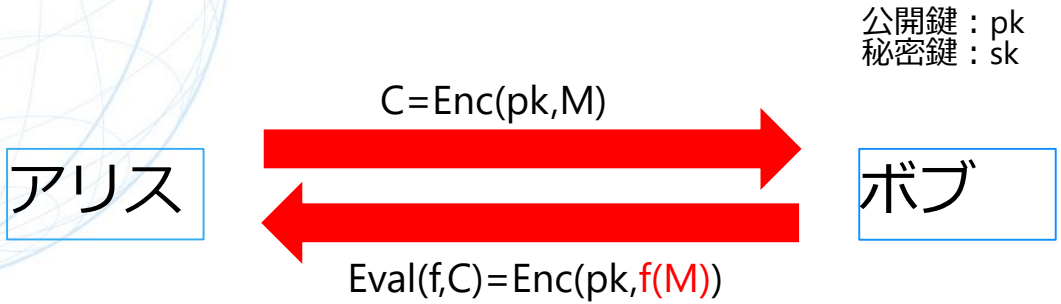
- 平文の任意の関数を計算



- PKEに基づく構成：[GVW12], LWEに基づく構成：[GKP+13],
  - 結託耐性に上限がある
- 難読化に基づく構成[GGH+16…]
  - 結託耐性に上限がないが、効率悪+仮定への安全性解析が不十分

完全準同型暗号

- 暗号化したまま任意の関数を計算



- LWEに基づく構成[BV11,GSW13…]
  - 厳密にいうと、LWE+Circular安全性を仮定
- 量子回路も扱える版[Mahadev18,Brakerski18]
  - ブラインド計算への応用

まとめ

- 量子コンピュータでも破れないと期待される耐量子公開鍵暗号が研究されている
  - 今日はその中でもLWE問題に基づくものを紹介
- 実用上IND-CCA安全性と呼ばれる安全性を持つことが望ましい
- IND-CCA安全な耐量子公開鍵暗号の構成には量子ランダムオラクルモデルを使う事で効率の良い方式が構成できる
  - 安全性証明のメインツール：One-Way-to-Hiding Lemma
- LWEは様々な高機能暗号の構成にも使える

明日：（耐量子）ゼロ知識証明

参考文献

- [Regev09]:Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM.
- [Aaronson10]: S. Aaronson. BQP and the polynomial hierarchy. STOC 2010
- [BKVV20]: Zvika Brakerski, Venkata Koppula, Umesh Vazirani, and Thomas Vidick. Simpler proofs of quantumness. TQC20
- [YZ20]: Takashi Yamakawa and Mark Zhandry, A Note on Separating Classical and Quantum Random Oracles https://eprint.iacr.org/2020/787
- [BR93]:Mihir Bellare and Phillip Rogaway. Random oracle are practical: A paradigm for designing ecient protocols. CCS93
- [BDF+11]:Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaner, and Mark Zhandry. Random oracles in a quantum world. Asiacrypt11
- [Unruh15]:Dominique Unruh. Revocable quantum timed-release encryption. Journal of the ACM.
- [GPV08]: Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC2008
- [SXY18]: Tsunekazu Saito, Keita Xagawa, Takashi Yamakawa, Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model Eurocrypt 20
- [BHH+19]: *Nina Bindel and Mike Hamburg and Kathrin Hövelmanns and Andreas Hülsing and Edoardo Persichetti Tighter proofs of CCA security in the quantum random oracle model TCC19*
- [KSSS20]: Veronika Kuchta, Amin Sakzad, Ron Steinfeld and Shifeng Sun, Measure-rewind-measure: tighter quantum random oracle model proofs for one-way to hiding lemma and CCA security, Eurocrypt20
- [FO13]: Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. J. Cryptology.
- [TU16]: Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms, TCC2016B
- [HHK17]:Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the Fujisaki-Okamoto transformation, TCC 2017.
- [HKW20] Susan Hohenberger and Venkata Koppula and Brent Waters, Chosen Ciphertext Security from Injective Trapdoor Functions, CRYPTO 2020

参考文献

- [ABB10]:Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (h) ibe in the standard model. Eurocrypt2010
- [CHKP10]:David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. Eurocrypt2010
- [GVW15]:Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. *Journal of the ACM*,
- [BGG+14]: Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits Eurocrypt 14
- [GVW12] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption with bounded collusions via multi-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*,
- [GGH+16]: Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters: Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits. SIAM J. Comput
- [GKP+13]: Shafi Goldwasser, Yael Tauman Kalai, Raluca A. Popa, Vinod Vaikuntanathan, Nickolai Zeldovich: Reusable garbled circuits and succinct functional encryption. STOC 2013
- [BV11]:Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011
- [GSW13]:Craig Gentry and Amit Sahai and Brent Waters, Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, CRYPTO 13
- [Mahadev18]:Urmila Mahadev: Classical Homomorphic Encryption for Quantum Circuits. FOCS 2018
- [Brakerski18]: Zvika Brakerski: Quantum FHE (Almost) As Secure As Classical. CRYPTO 2018