
暗号・認証分科会

目次

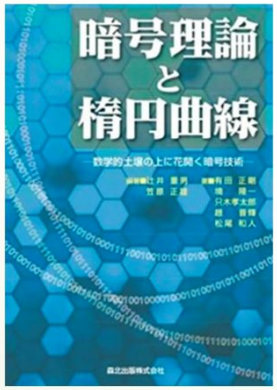
活動方針

・最先端にまでわたる暗号・認証技術を整理・体系化すること

・一般の人々が暗号・認証技術の安全性の本質を理解できるような説明手法を構築すること

活動メンバー

研究リーダー：趙 晋輝 先生



指導教授　：花岡 悟一郎 先生

活動メンバー

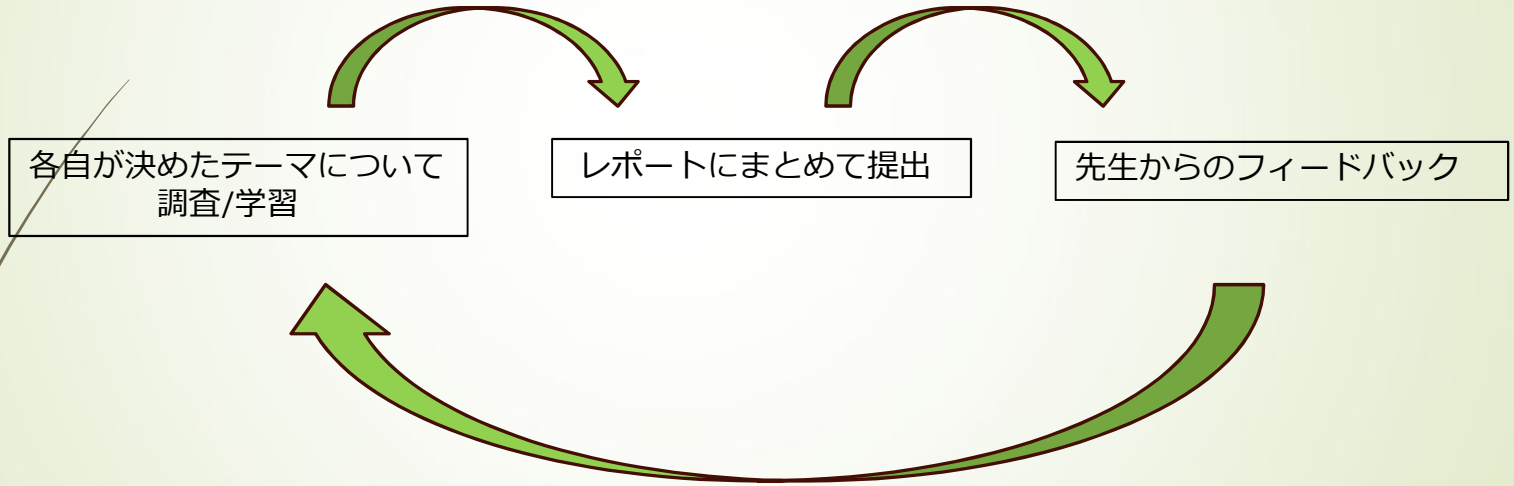
M2

・上里 優介　・奥村 祐太　・藤田 真緒

M1

・福井 恵悟　・四方 隆之介　・佐藤 佑哉　・村上 誠樹

活動内容


各自が決めたテーマについて
調査/学習
レポートにまとめて提出
先生からのフィードバック
修正点/改善点を理解した上で

活動テーマ

- 福井 恵悟 … 準同型暗号
- 四方 隆之介 … プロキシ再暗号化
- 村上 誠樹 … 耐量子計算機暗号への安全性
- 佐藤 佑哉 … 量子鍵配送

1. 従来の暗号技術 ~機能性と安全性~

暗号とは

○ 簡単なプロトコル

○ 単純な秘匿のみではなく，より高度な機能も求められる時代

・クラウドストレージの浸透

・電子投票

など

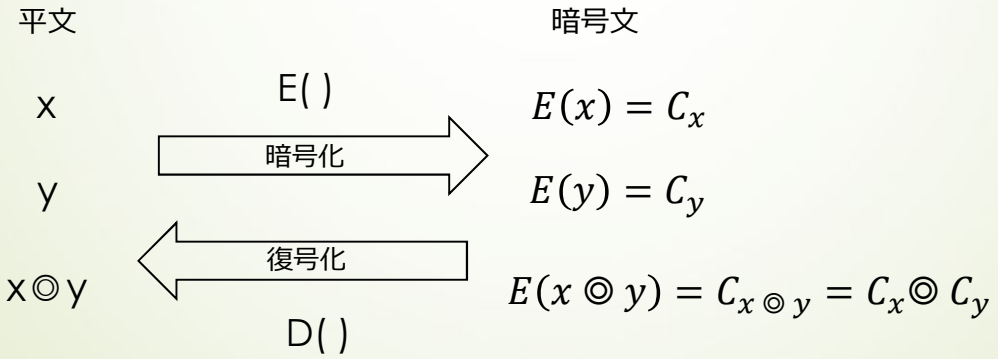
準同型暗号

○ 準同型暗号とは … データを暗号化したまま計算や操作ができる暗号技術

復号化せずに計算・分析可能

サーバーに暗号文のみ格納可能

・暗号文の加算・乗算が, 平文の加算・乗算となることを意味する



◎が+の場合, 加法準同型暗号
◎が×の場合, 乗法準同型暗号
両方満たす場合, 完全準同型暗号

身近なシナリオで考える

○ シナリオ

A君は数学の宿題を先生Bに採点してもらう必要がある. しかし, 間違いを見られるのが恥ずかしく, 解答を見せずに採点してもらいたい…

採点方法

・ある問題をx=42と回答

・$C_x = E(x) = E(42)$

提出

・模範回答yから$C_y = E(y)$を計算

・C_xとC_yを用いて$C_{x-y} = E(x-y)$を計算

返却

・復号化 $\mathrm{D}(C_{x-y})$を行う

$\mathrm{D}(C_{x-y}) = 0$ なら正解
$\mathrm{D}(C_{x-y}) \neq 0$ なら不正解

正解漏洩対策

○ 同じ問題の追試が行われるとする

・先程の場合

返却

$D(C_{x-y}) = z$なら
$y = x + z$だね

・対策を行なった場合

返却

$r(x-y) = z$からじゃ
yはわからないなあ

・乱数rを設定

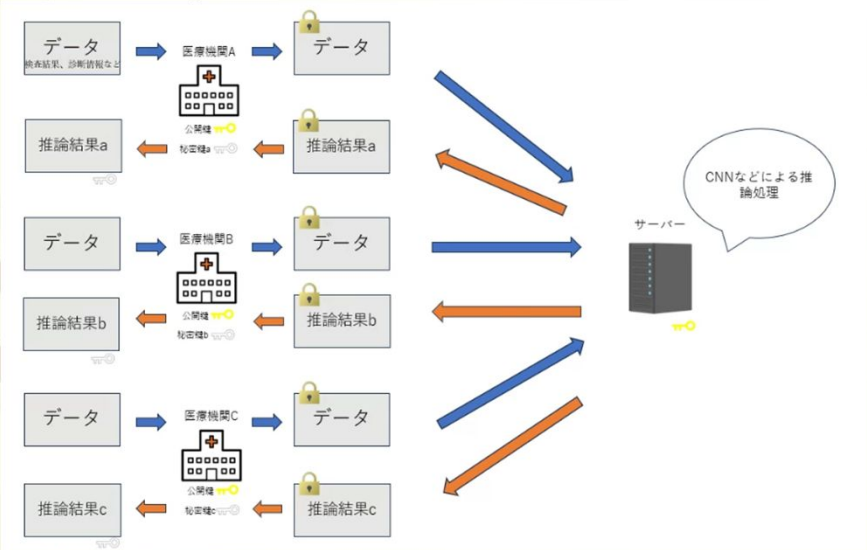
・$C_{r(x-y)} = E(r(x-y))$を計算

$D(C_{r(x-y)}) = 0$ なら正解
$D(Cr_{(x-y)}) \neq 0$ なら不正解

具体的なユースケース

○ 医療データの活用

- 医療データを予測し,患者の疾患予測に役立てたい
- 医療データには個人情報も含まれる…



1. 診察データの暗号化
   各医療機関が公開鍵を使って診断データを暗号化、サーバーに送信

2. 暗号化されたまま計算
   サーバーに構築されたAIモデルを使って暗号化されたまま疾患を推論

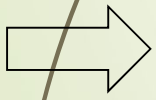
3. 結果をもとの病院に送り返す
   戻ってきた推論結果を秘密鍵を使って復号化しデータを見る

プロキシ再暗号化

○ プロキシ再暗号化とは … データを安全に複数の第三者に共有できる方法.
復号することなく，暗号文を他の暗号文に変換する.

・一般的なプロキシは, サーバーとの接続時にリクエストとレスポンスを中継する役割を持つ.

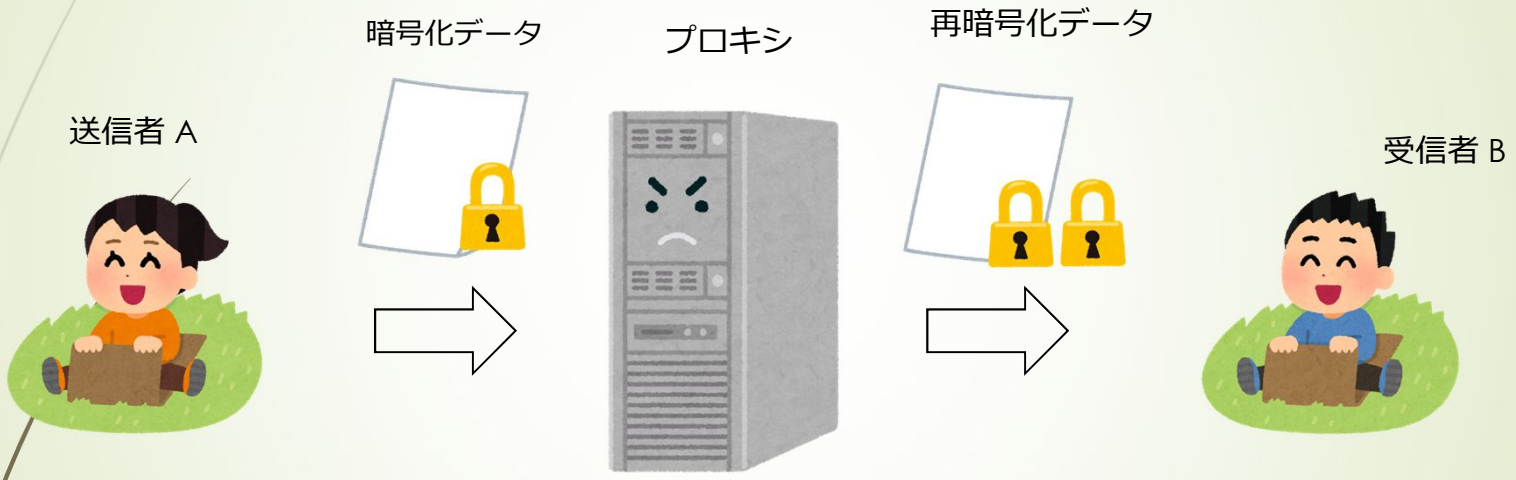
・プロキシ再暗号化におけるプロキシ機能は, 再暗号化鍵を用いて“暗号文の再暗号化”を行う.



△Aによって暗号化された文をBが復号できるような暗号文に,復号することなく変換.
△プロキシ自身等の許可されていない第三者がデータの内容をアクセスすることはできない！

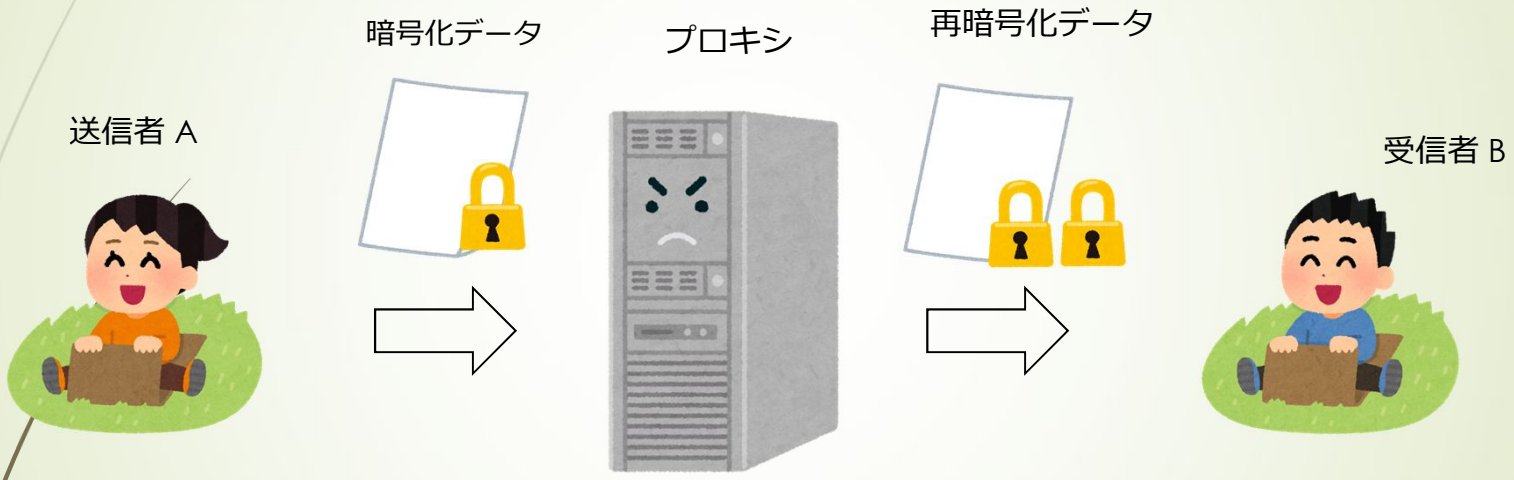
○ しかし, ここで一つ疑問が生じる…

疑問



・Bに共有されるのは暗号化されたデータ？
・B以外にも共有される？

リアルなプロトコル



○ 再暗号化鍵 … Aの秘密鍵とBの公開鍵を組み合わせたもの.
Bの秘密鍵で完全復号できるような形に変換する鍵である.

具体的なユースケース

○ クラウドストレージでのアクセス制御

1. データ所有者が自分の暗号鍵でファイルを暗号化してクラウドにアップロードする
2. 他のユーザーにアクセス権を与えたい場合，データ所有者はそのユーザーの公開鍵を使って再暗号化キーを生成する.
3. クラウドプロバイダ（プロキシ）は再暗号化キーを使ってデータを変換し,許可されたユーザーのみがアクセスできるようにする.

2. 未来の暗号技術 ~量子力学と暗号~

背景

○ 現代で用いられている暗号方式は完全無欠ではない

・ 現代の一般的なコンピュータを用いて現実的な時間内で解けない水準

無制限にお金/時間をかける ⇩ さらに進化したコンピュータ

破られる！！

○ 量子コンピュータの実用化が近づいてきている

量子コンピュータ

○ 量子コンピュータとは …　量子力学の性質を計算に利用したコンピュータ

・1つの量子ビットで1, 0を同時に表すことができる

・2030年頃までに, 現在主流のRSA暗号を数時間で解読可能な量子コンピュータが実現する可能性あり

△ store now decrypt later 攻撃 が提唱

攻撃者が今のうちから暗号化されたデータを収集し, 量子コンピュータの性能が向上した将来に解読を試みる攻撃.

○ 量子コンピュータでも解けない暗号(耐量子計算機暗号(PQC))が至急必要！

PQCのアルゴリズム

米国標準技術研究所(NIST)は標準化計画を2016年に発表.
2024年には以下の4つのアルゴリズムを選定.

	選定集の名称	FIPSの名称	ドキュメント
公開鍵暗号 鍵交換	CRYSTALS-KYBER	ML-KEM	FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard https://csrc.nist.gov/pubs/fips/203/final
デジタル署名	CRYSTALS-Dilithium	ML-DSA	FIPS 204 Module-Lattice-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/204/final
	SPHINCS+	SLH-DSA	FIPS 205 Stateless Hash-Based Digital Signature Standard https://csrc.nist.gov/pubs/fips/205/final
	FALCON	FN-DSA	(2024年度内の公開準備中)

・連邦政府機関はNISTの定めた技術的標準に従うことが法的に求められる.

・日本国内でも,金融機関等の当事者がPQC移行に向けて議論を開始.
→ 遠い未来の出来事ではなくなってきている.

NISTによるPQCの厳格な選定プロセス

○ NISTは公開メーリングリストでの議論を経る方式で選定を実施

・　第一段階（ラウンド1）：

2017年から始まり、公募にて69の提案が提出。暗号方式の多様性を確保するため、格子ベース、符号ベース、多変数多項式ベース、ハッシュベースなどの異なる方式を採用

・　第二段階（ラウンド2）：

候補が26に絞り込まれ、セキュリティ、効率性、暗号強度に関する詳細な分析を実施

・　第三段階（ラウンド3）：

2020年、暗号方式の安全性や実装効率を基にさらに7つのファイナリストに絞り込み

○ 最終ラウンドまで残ったが,強い関心が集中し,暗号が破られ.
PQC候補から脱落したアルゴリズムも多く存在する.

・ex) SIKE（Supersingular Isogeny Key Encapsulation）

量子暗号

○ 耐量子計算機暗号 … 量子コンピュータで現実的な時間で解けない暗号方式

○ 量子暗号 … 量子力学の性質を用いる暗号方式. 無制限にコストを導入しても, 量子コンピュータ以上の計算機が現れても破ることのできない安全性(無条件安全性)を満たす.

量子暗号 = ワンタイムパッド + 量子鍵配送 (QKD)

・ワンタイムパッドは, 1949年にクロード・シャノンによって無条件安全性を満たすことを証明されている.

・量子鍵配送は盗聴をされていないことを保証し, 無条件安全性を満たす.ワンタイムパッドの欠点である鍵共有を補う.

量子鍵配送の簡易的なプロトコル

○ 魔法の封筒を用いたアナロジー

・送信者をアリス, 受信者をボブ, 盗聴者をイブとする.

・アリスは, 魔法の封筒にランダムなbitを入れて, ボブに送信する.

・魔法の封筒とは …

△特別な呪文で封じることが可能な封筒. この呪文を解除するには, 同じ呪文を唱える必要がある.

△呪文は2種類存在. 送信前に,ランダムに一つ呪文を唱えることで, アリスは封筒を封じる.

△正しくない呪文を用いて開封を試みた場合, 中のbit情報はランダムに変更する.

以上の知識は公開情報である

量子鍵配送の簡易的なプロトコル

ボブ

アリス

1bitずつ魔法の封筒に入れて送信

呪文を設定する.設定した呪文,
送信時間を記録.

送信された封筒に対して, ランダムに呪文を選び
開封を試みる.その使用した呪文,観測結果,受信時間
を記録.

n bit分繰り返す

記録した呪文情報を交換し,呪
文が一致したbit情報のみを合
成する.

これをふるい鍵と呼ぶ.

量子鍵配送の簡易的なプロトコル

○ ふるい鍵からさらに秘匿性の高い鍵を抽出する

△ 光ファイバーによるビット誤り
△ イブによる盗聴

ふるい鍵　(ボブとアリス間で一致しているとは限らない)

誤り訂正

・サンプルビットを比較. 漏洩情報量(エラー率)を評価
・ボブとアリス間のふるい鍵の食い違いの訂正

完全一致した鍵

秘匿性増幅

・所定のアルゴリズムに従って鍵を圧縮
・漏洩情報量が多いほど, 得られる鍵は短くなる

さらに安全性の高い鍵 (共通鍵として採用)

まとめ

○ 現在

・ 次々と進化するIT技術に対応して，さまざまな暗号技術が開発・活用されている．

○ 未来

・量子力学を中心に，従来の暗号技術は大きな変革を迎えている．

付録：暗号技術の紹介スライド

以下のスライドは, 各メンバーが活動を通じて作成した
暗号技術の紹介スライドです.

準同型暗号

大久保研究室
M1
福井 恵悟

準同型暗号

■ 準同型暗号とは、データを復号化したまま計算や操作ができる技術

設定：貴重な情報や宝物を守るための宝箱があります。この宝箱には**秘密の魔法**という魔法がかけられており、中身を安全に守りながら、外部から**影の魔法**をかけることで、中身をより高い価値のものなどに操作できる。魔法をかけるには杖が必要となる。

DALL-Eで生成

準同型暗号

- **秘密の魔法**は、準同型暗号の「**暗号化**」
- 宝箱は封印され
- 鍵の所有者以外、中のもの見たり触ったりできない
  - AIや外部システムに処理を依頼する際に、中身の情報を漏らさずに済む
- **影の魔法**は、宝箱を開けずに、中身を触れることなく、内容や形を変えたり、**より価値のあるもの**にすることができる魔法
  - 暗号化されたままのデータを取り扱うことができる
  - 秘密の魔法が付与された宝箱であれば、だれでも影の魔法は使用可能

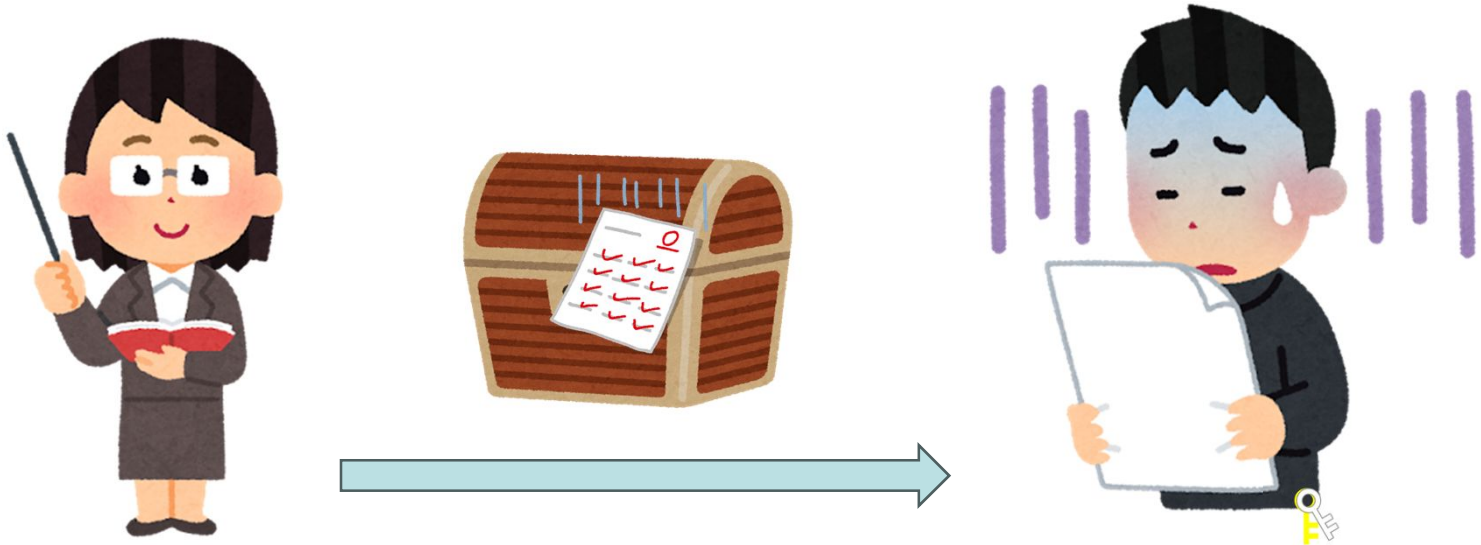
たとえば(1/2)

シナリオ: 数学の宿題をやって、それを先生に提出して採点してもらわなければいけない。しかし、間違いを見られたら恥ずかしいため、解答を見せずに採点だけしてほしいと考えた。

たとえば(2/2)

■ そこで準同型暗号の魔法によって採点だけしてもらう方法を思いついた

- まず**秘密の魔法**がかけられた宝箱に数学の宿題を入れ、**付属の鍵**で宝箱を締める
- 先生が宝箱を受け取り、**影の魔法**をかけることによって中身を見ることなく、そのまま中身を**採点結果に変える**
- かえってきた宝箱を、あらかじめ**自分の作った鍵**で開封し採点結果を確認する



準同型暗号の仕組み

■ 通常と同じように、鍵を使ってデータを暗号・復号化

- 平文xを用いて暗号化鍵で暗号化。暗号文$C_x = E(x)$を作成
- 復号鍵を用いて復号処理を行う。 $D(C_x) = x$を得る

■ さらに、暗号文同士を組み合わせて、暗号化したまま計算可能

- 二つの暗号文C_xとC_yから$C_{x+y} = E(x + y)$を計算
- 同様に、 $C_{x-y} = E(x - y)$も計算可能

準同型暗号の仕組み

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

採点方法

ある問題をx=42と回答した

暗号化$C_x = \mathrm{E}(x)=\mathrm{E}(42)$

正解yの暗号文$C_y = E(y)$を用意
生徒の暗号文C_xと正解の暗号文C_yから、平文が$x-y$となる暗号文C_{x-y}を作成し、C_{x-y}を生徒に返却

復号化
$D(C_{x-y})$

$x-y=0$なら正解、
$x-y\neq 0$なら不正解

準同型暗号の仕組み

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

採点方法（正解漏洩対策）

■ さっきのだと

C_{x-y}を生徒に返却

復号化
$D(C_{x-y})$

■ 対策

乱数rを設定
C_{x-y}から$C_{r(x-y)} = E(r(x-y))$
を計算、返却

復号化
$D(C_{r(x-y)})$

$r(x-y) = 0$なら正解、
$r(x-y) \neq 0$なら不正解

準同型暗号のメリット

■ プライバシー保護

- 個人情報を守りながらデータ共有ができるため、医療や金融分野で活用可能
- 例：先生は生徒の解答そのものを見ることなく採点する

■ 安全性

- 暗号化したまま計算ができるため、第三者にデータの内容が漏れない
- 例：暗号化された状態で処理されるため、解答漏洩のリスクが低い

■ 利便性

- データを暗号化したままで機械学習や統計分析に使えるため、セキュアなデータ活用が可能
- 例：先生は個別の生徒の解答にアクセスすることなく、平均点などの統計を見ることで、今後の宿題やテストに活用することができる

従来の暗号との違い

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

従来の暗号

データを使うには一度復号化する必要があった。

例：宝の中のものをいじるには、一度鍵で宝箱を開ける必要がある。

準同型暗号

データを復号化しなくても、AIなどを使って計算・解析することができるため安全

例：鍵がなくても宝箱の中だけをいじることができるので、誰にも見られることがない。

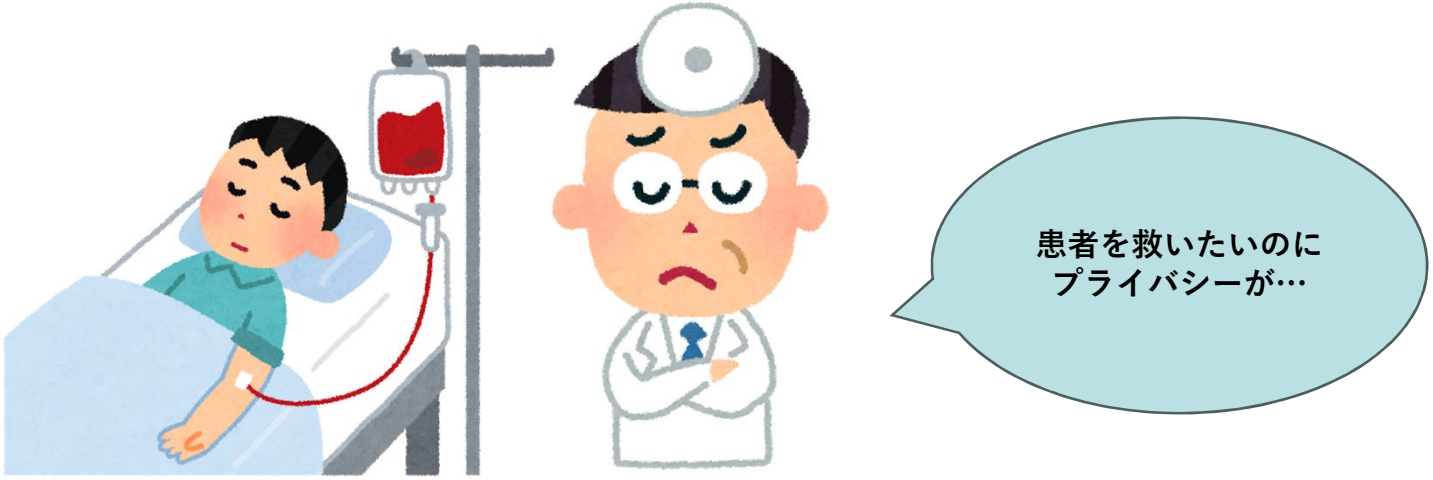
ユースケース(1/2)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 医療データの活用

- 医療データを学習し、患者の疾患予測に役立てたい
- しかし、個人情報も含まれるのでそのまま使うわけにはいかない

準同型暗号を活用

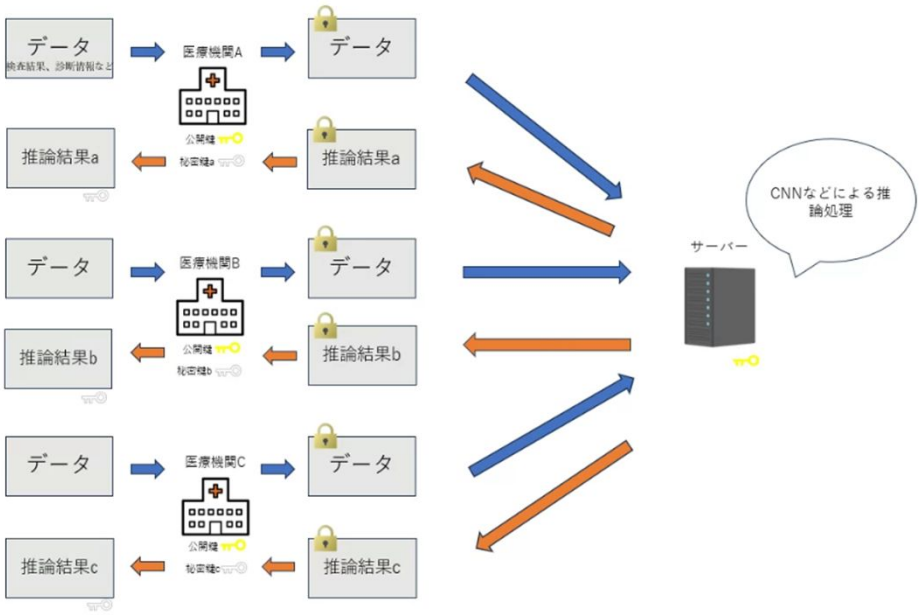


ユースケース(2/2)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 医療データの活用

実際の流れ



1. 診察データの暗号化
各医療機関が公開鍵を使って診断データを暗号化、サーバーに送信
2. 暗号化されたまま計算
サーバーに構築されたAIモデルを使って暗号化されたまま疾患を推論
3. 結果をもとの病院に送り返す
戻ってきた推論結果を秘密鍵を使って復号化しデータを見る

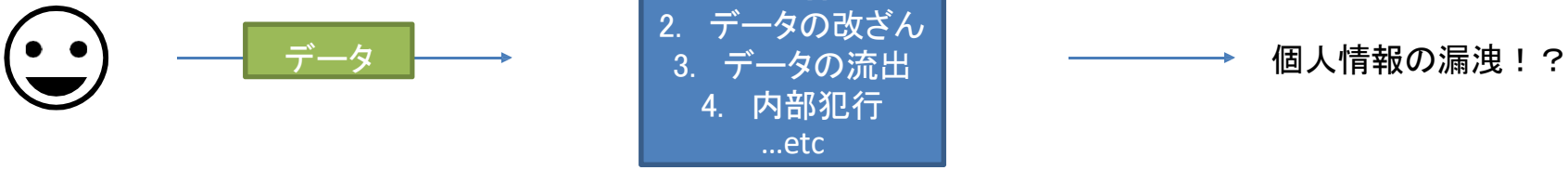
準同型暗号のデメリット

- 計算コストが高い
  - 通常のデータ処理に比べ、計算にかかる時間やリソースが増大
  - 例：秘密の魔法が付与された宝箱に影の魔法をかけるにはかけるための杖のコストや魔法の時間がすごくかかる
- 改ざんのリスク
  - 暗号文を改ざんされると、正しい結果が得られなく恐れがある
  - 例：秘密の魔法が付与された宝箱は誰でも影の魔法を使うことで中のものを操作することができてしまうため、そうすると正しい採点結果がでてこなくなってしまう
- 実用性の難しさ
  - 現在の技術では、計算コストやアルゴリズムの複雑さ、データサイズなどの問題により、用途が限られる
  - 例：高級な杖を持っていても、影の魔法を正確にかけるには訓練が必要でまた成功しても宝箱に収まりきらないといった問題が起きるため、大きな宝箱を持っていなければいけない

プロキシ再暗号化について

データ共有におけるセキュリティ問題

- あなたのデータが第三者に安心して共有できますか？
- 多数の利用者が存在するサービスは、攻撃の対象者になりやすく、データが流出したり、改ざんされたりするリスクが常に存在します。



プロキシ再暗号化による解決策

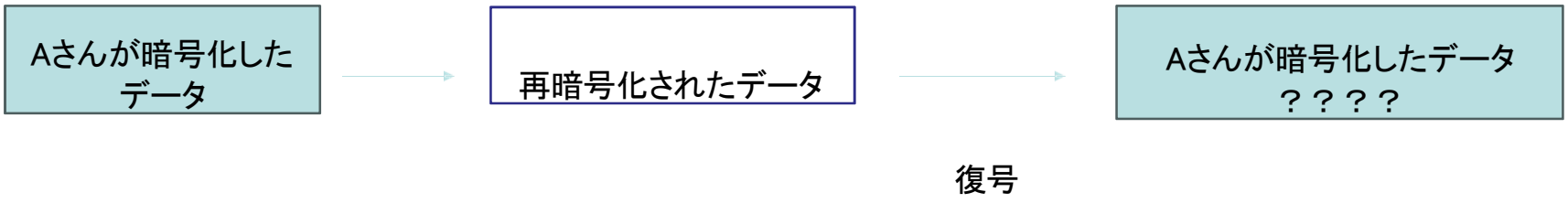
■プロキシ再暗号化は、データを安全に複数の第三者に共有できる方法。

◆一般的なプロキシはサーバーとの接続時にリクエストとレスポンスを中継する役割をもち、多様な機能を提供していますが、プロキシ再暗号化のプロキシ機能は"暗号文の再暗号化"を行います。そうすることで、暗号文を復号することなく変換できるため、プロキシや第三者がデータの内容にアクセスすることはできません。

ここで疑問…

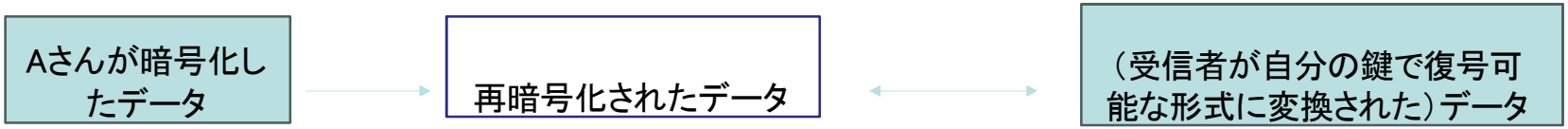
■「送信者の暗号鍵で暗号化したデータを再暗号化してそれを復号する。」

■プロキシが暗号化した文章が復号されるので、結局は送信者が暗号化したデータが出てくるのでは…？



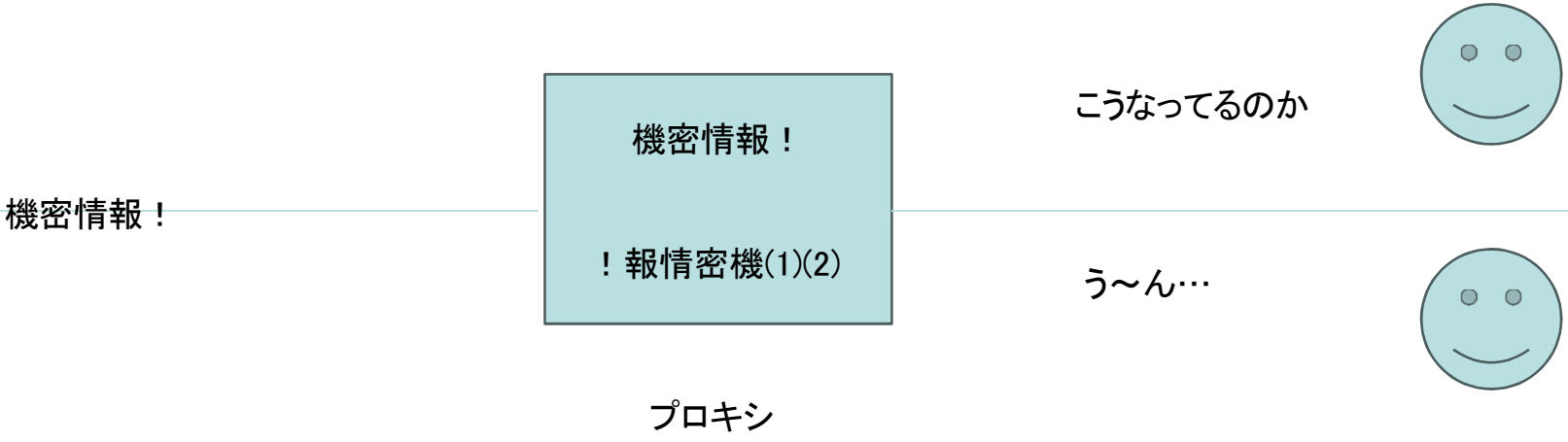
正しくは…

■再暗号化鍵がデータの再暗号化を行う役割で、送信者の複合鍵と受信者の暗号鍵を用いて、要求した受信者だけが複合可能な形式に変換する鍵である。



安全性

■プロキシが送信者から送られてくる暗号文を解読できない(1)
■プロキシが保有している再暗号化情報を公開しても安全であることを証明している。(2)

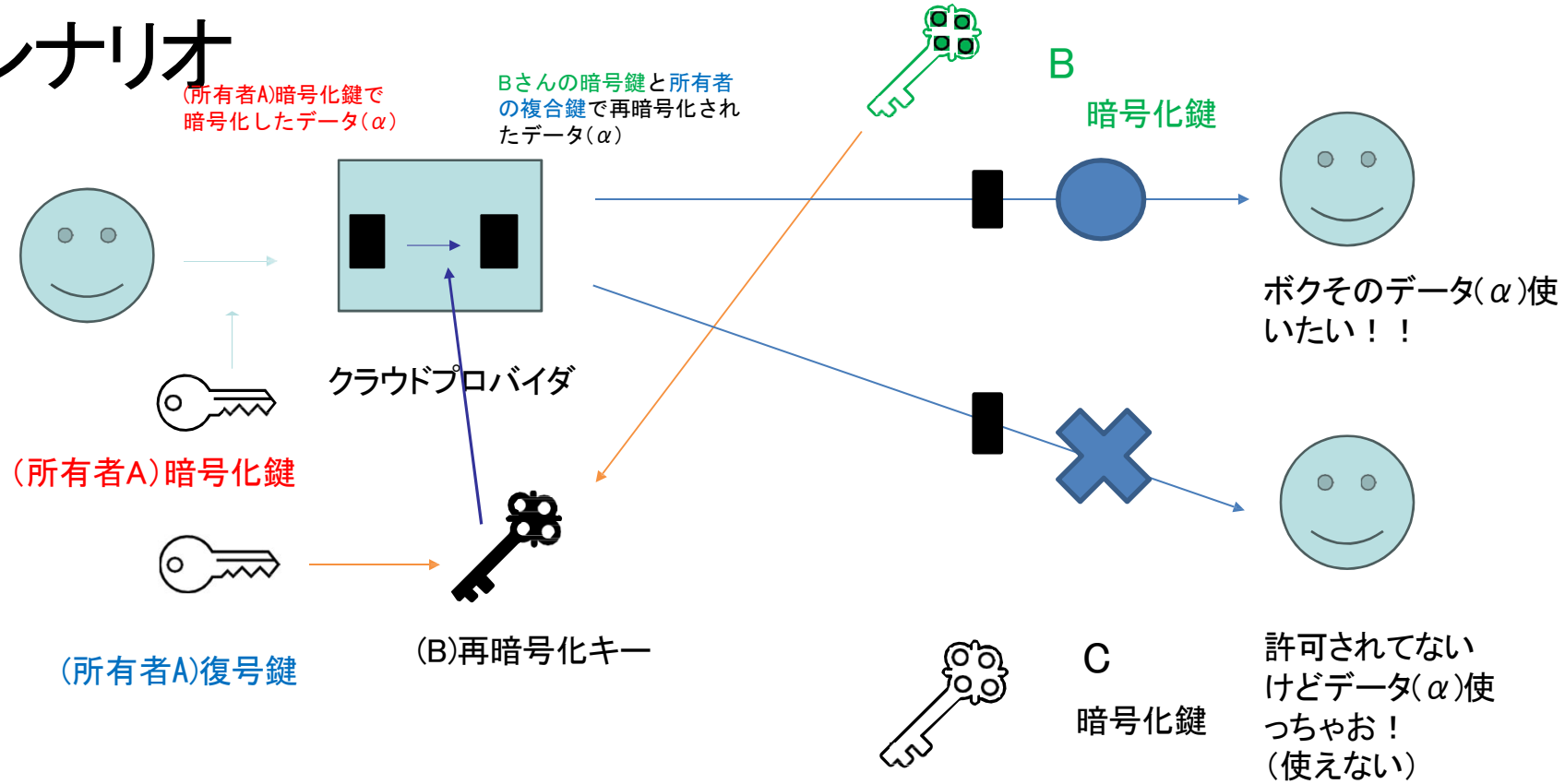


具体的なユースケースシナリオ

■クラウドストレージでのアクセス制御

1. データ所有者が自分の暗号鍵でファイルを暗号化してクラウドにアップロードする
2. 他のユーザーにアクセス権を与えたい場合、データ所有者はそのユーザーの公開鍵を使って再暗号化キーを生成する。
3. クラウドプロバイダ（プロキシ）は再暗号化キーを使ってデータを変換し、許可されたユーザーのみがアクセスできるようにする。

具体的なユースケースシナリオ



具体的なユースケースシナリオ

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- データ所有者　データを暗号化してクラウドに保存する。再暗号化鍵を生成する。
- Bさん(受信者)　データ所有者からアクセス権を与えられたユーザー。自身の秘密鍵で復号。
- クラウドプロバイダ　再暗号化鍵を使用してデータを変換するが、データ内容は閲覧不可。

具体的なユースケースシナリオ

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

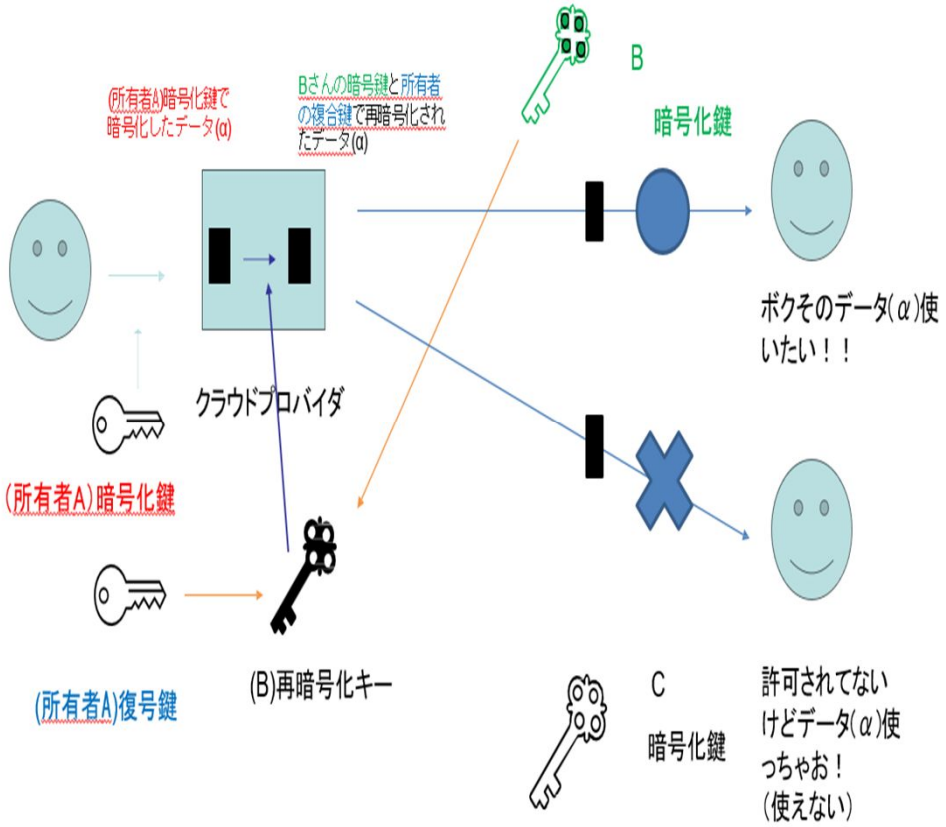
- 暗号化:送信者Aの公開鍵pkAを使って暗号化し、暗号文CAを生成する。
- CA = Enc(pkA,m)

- 再暗号化鍵生成:送信者Aの秘密鍵skAと受信者Bの公開鍵pkBを用いて、再暗号化鍵rkA→Bを生成する。
  $\mathrm{rk}_{A\to B} = f(\mathrm{sk}_A, \mathrm{pk}_B)$

- 再暗号化:プロキシが再暗号化鍵を用いて、暗号文CA を受信者用の形式CBに変換する。
- $C_B = g(\mathrm{rk}_{A\to B}, C_A)$

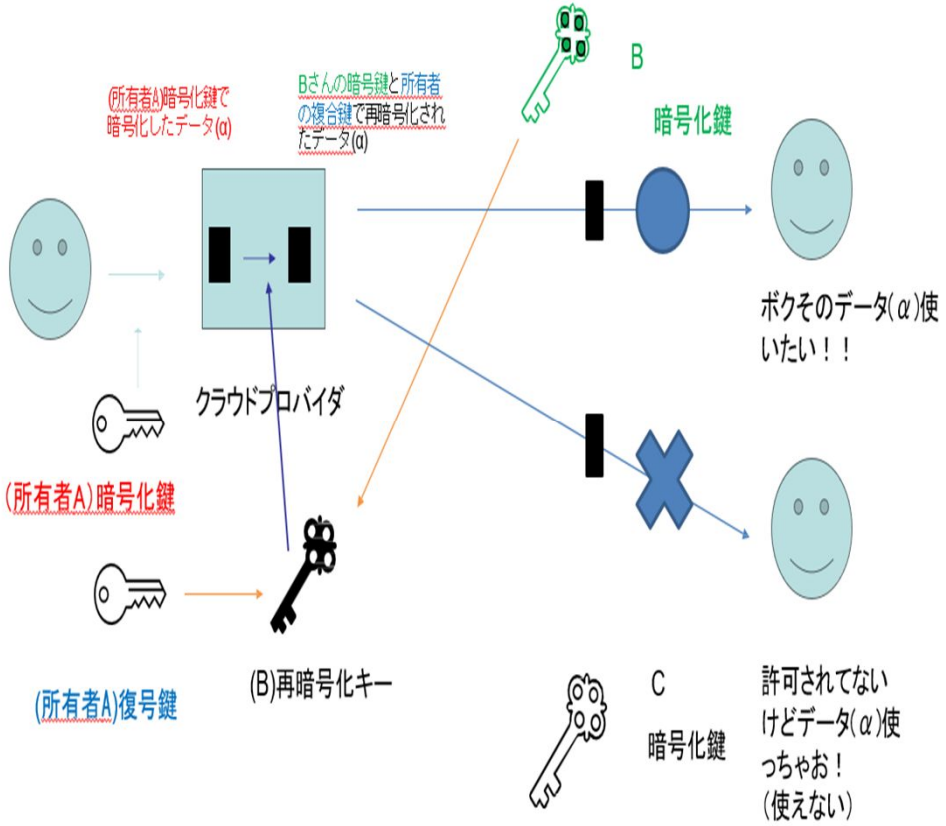
- 復号化:受信者Bは、自身の秘密鍵skBを用いて変換後の暗号文CBを復号し、元のデータmを取得する。
- $m = \mathrm{Dec}(skB, CB)$

具体的なユースケースシナリオ



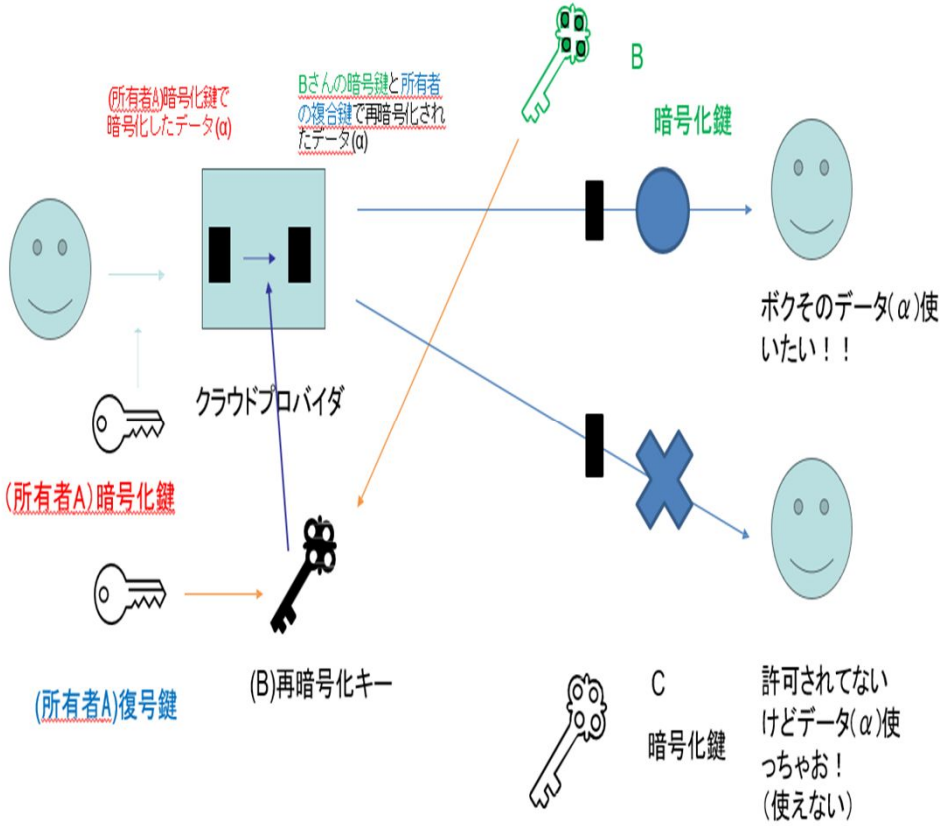
1. データの所有者が自身の暗号鍵を使用してデータをクラウドプロバイダにアップロードする。
2. 受け取り手Bさんの暗号化鍵と所有者の複合鍵を使って再暗号化鍵を生成する。
3. プロバイダは所有者の暗号化鍵で暗号化されたデータをさらに、再暗号化鍵で暗号化する。
4. その後、データが要求したAさんの手元に届き、自身の秘密鍵で復号する。

具体的なユースケースシナリオ



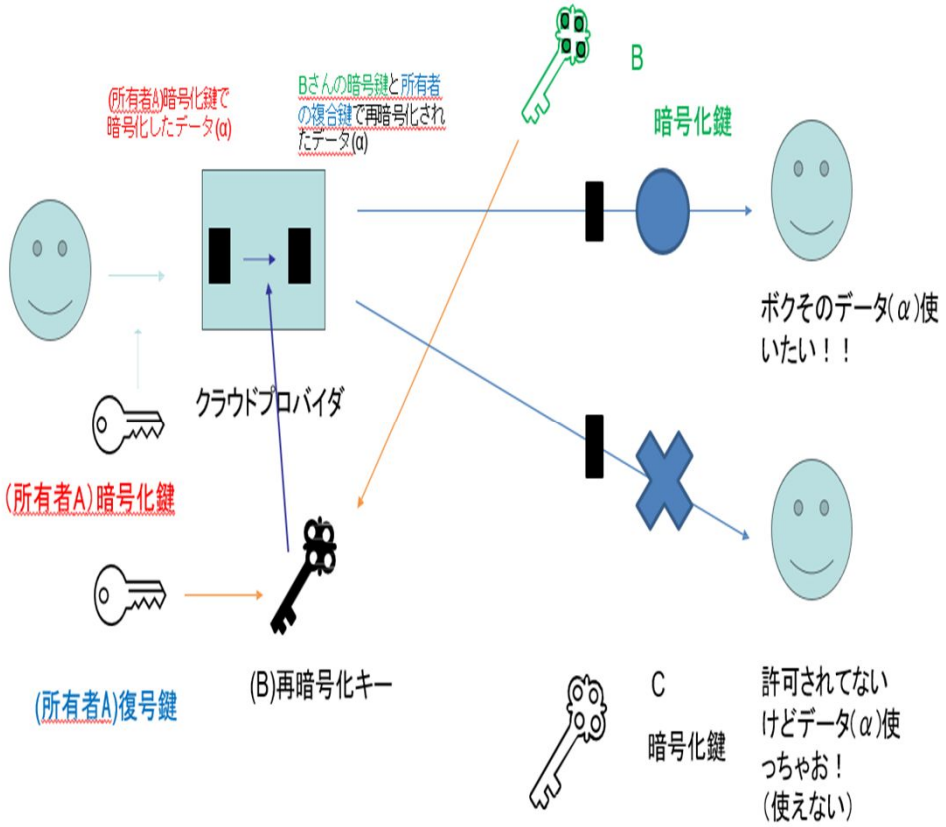
1. データの所有者が自身の暗号鍵を使用してデータをクラウドプロバイダにアップロードする。
2. 受け取り手Bさんの暗号化鍵と所有者の複合鍵を使って再暗号化鍵を生成する。
3. プロバイダは所有者の暗号化鍵で暗号化されたデータをさらに、再暗号化鍵で暗号化する。
4. その後、データが要求したAさんの手元に届き、自身の秘密鍵で復号する。

具体的なユースケースシナリオ



1. データの所有者が自身の暗号鍵を使用してデータをクラウドプロバイダにアップロードする。
2. 受け取り手Bさんの暗号化鍵と所有者の複合鍵を使って再暗号化鍵を生成する。
3. プロバイダは所有者の暗号化鍵で暗号化されたデータをさらに、再暗号化鍵で暗号化する。
4. その後、データが要求したAさんの手元に届き、自身の秘密鍵で復号する。

具体的なユースケースシナリオ



1. データの所有者が自身の暗号鍵を使用してデータをクラウドプロバイダにアップロードする。
2. 受け取り手Bさんの暗号化鍵と所有者の複合鍵を使って再暗号化鍵を生成する。
3. プロバイダは所有者の暗号化鍵で暗号化されたデータをさらに、再暗号化鍵で暗号化する。
4. その後、データが要求したAさんの手元に届き、自身の秘密鍵で復号する。

■クラウドプロバイダに平文を見せることなく、柔軟なアクセス制御が実現できる！

■必要な場合のみデータ所有者とデータ共有ができた。

耐量子計算機暗号の安全性について

アジェンダ

- 第1章：耐量子計算機暗号の概説と影響
- 第2章：選定プロセス
- 第3章：具体的な審査過程の紹介

第1章：耐量子計算機暗号の概説と影響

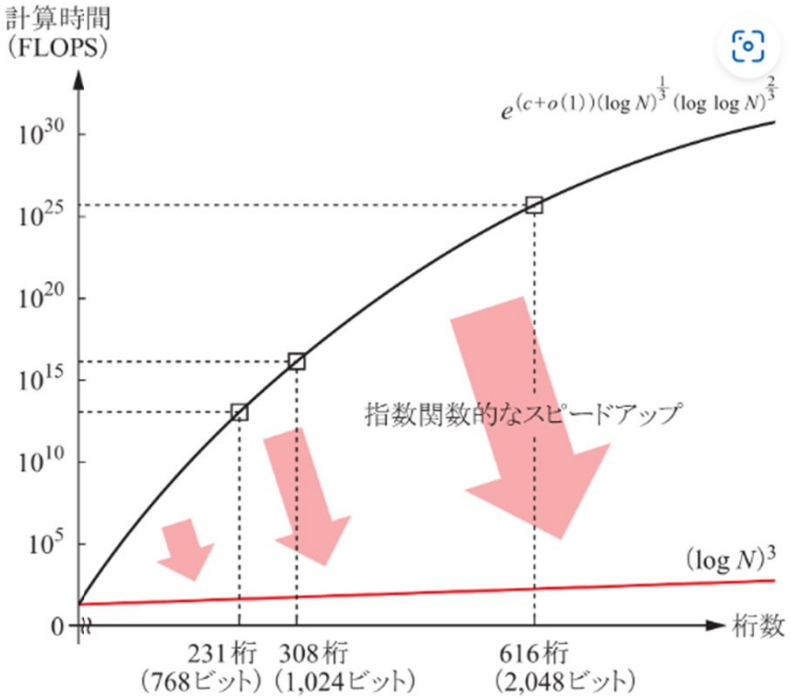
耐量子計算機暗号とは

耐量子計算機暗号(PQC: Post-Quantum Cryptography):
量子コンピュータでも破られない種別の暗号の総称

現代の通信を守るうえでは、暗号化技術が必須である。
例:オンラインバンキング・電子メール……SSL/TSL通信で暗号化されているため安全

広く使われるRSA暗号は、現代の計算では素因数分解を行うことに非常に長い時間がかかることを前提に用いられている
→しかし、量子コンピュータが実現した際には、RSA暗号が解かれてしまう

素因数分解の求解速度



量子コンピュータにて実行できる
“ショアのアルゴリズム“を用いると、
大幅に高速な時間で計算が解けることが知られている

↓

量子コンピュータ実現でRSA暗号での安全性が無効化される

※注：縦軸は対数

出典：高木 剛, 量子計算機時代のセキュリティ――耐量子計算機暗号の動向――”, 電子情報通信学会誌 Vol.106 No.11 pp.966-970 2023 年 11 月

暗号技術の危殆化

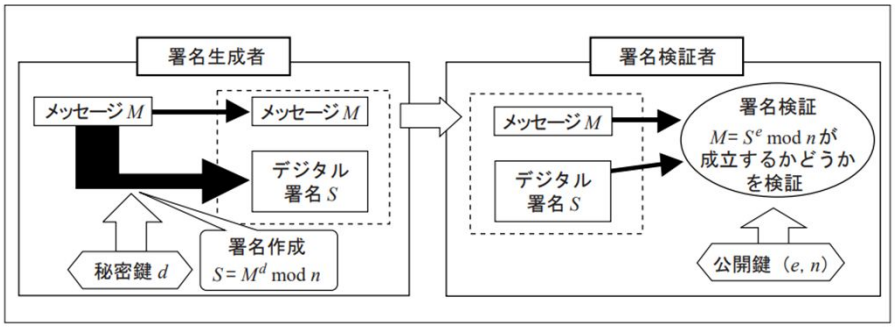
- 量子コンピューターの実現で、量子アルゴリズムの実用化促進
  他3つは効率化に資するが、「暗号」は解読されてしまうことが喫緊の課題

	適用シーン	関連する量子アルゴリズムの例（※）
最適化	サプライチェーンやロジスティクス（ルート最適化）、 金融（ポートフォリオ最適化、リスク分析）、 人やモノなどの配置（リソース管理、スケジューリング）など。	• 量子アニーリング • QAOA（Quantum Approximate Optimization Algorithm） • グローバーのアルゴリズム • QAE（Quantum Amplitude Estimation） • HHLアルゴリズム
機械学習	ヘルスケア（映像解析、患者特定）、金融（不正検知）、 広告配信（属性分類）など。 分類のためのサポートベクタマシンなどの機械学習、 学習モデル生成に利用できる。	• 量子機械学習 - サポートベクタマシン - クラスタリング - 量子ニューラルネットワーク - 量子強化学習
シミュレーション	触媒や電池用素材の探索（マテリアル・インフォマティス）、 医薬品（創薬）など。 量子力学的な状態をネイティブに操作する機能を利用する。	• VQE（Variational Quantum Eigensolver） • QPE（Quantum Phase Estimation）
暗号	安全保障（暗号解析、暗号通信） 金融（暗号通信）など	• ショアのアルゴリズム

出典：量子コンピュータ～2030年に向けたロードマップ～, 野村総合研究所(2022)

暗号技術解読による脅威

- 脅威1. デジタル署名の無効
  - 通信の際に真正性を保証しているデジタル署名が破綻し、HTTPS通信などをはじめ、多くのデジタル署名をもとにしている通信の安全性が担保されなくなる



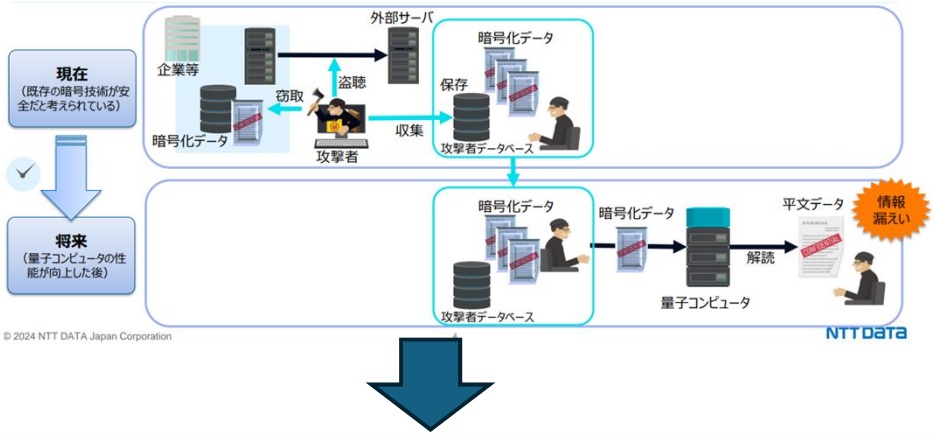
RSAデジタル署名の模式図

平文通信(HTTP)時代のように、現代の電子商取引やSNS、企業間の受発注など、広範な通信が危険にさらされ得る

出典:RSA署名方式の安全性を巡る 研究動向について(日本銀行金融研究所)

暗号技術解読による脅威

- 脅威2. 後年になって暗号情報が解読される
  - Store now, decrypt later 攻撃（Harvest now, decrypt later 攻撃とも）が提唱されている
    現在から暗号化済みデータを蓄積しておき、後年量子コンピュータによって解読すること



攻撃の優先度が低いと考えてしまい、現代では従来の暗号化通信を使っていても、
将来、機密情報が平文で解読　⇒**個人情報保護の非順守・社外秘漏洩に発展する**

場合によっては安全保障上の課題にも

出典：耐量子計算機暗号（PQC）に関する概況 等について（NTTデータ）