暗号・認証分科会

活動報告

01 暗号・認証分科会とは

02 活動内容

03 CTF神奈川 作問

04 活動テーマ

暗号・認証分科会とは

活動方針

一般の人々が暗号・認証の安全性の本質を理解できるよう説明手法を構築すること

安全・安心な情報化社会を実現するためには、情報システムに関わる人々が暗号・認証の安全性を適切に理解する事が非常に重要です。また、新たな暗号・認証技術の設計を行う際は、それらの技術の安全性を第三者に対して正確でなおかつわかりやすく説明をする必要があります。

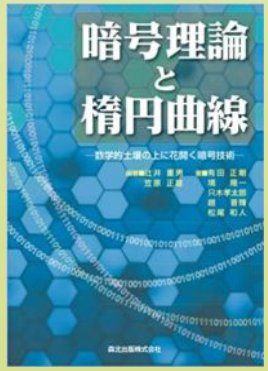
研究キーワード

暗号・認証に関する様々なテーマについて研究する事が出来ます

共通鍵暗号、**公開鍵暗号**、IDベース暗号、**電子署名**、**ハッシュ関数**、 鍵共有、マルチパーティプロトコル、情報量的安全性、計算量的安全性、証明可能安全性、 汎用結合可能性、暗号実装の安全性、CRYPTREC、 **量子暗号**、相手認証、生体・人工物認証、ヒューマンクリプト、匿名性、PKI、PGP、PAKE

活動内容

活動メンバー



研究リーダー
趙晋輝 先生

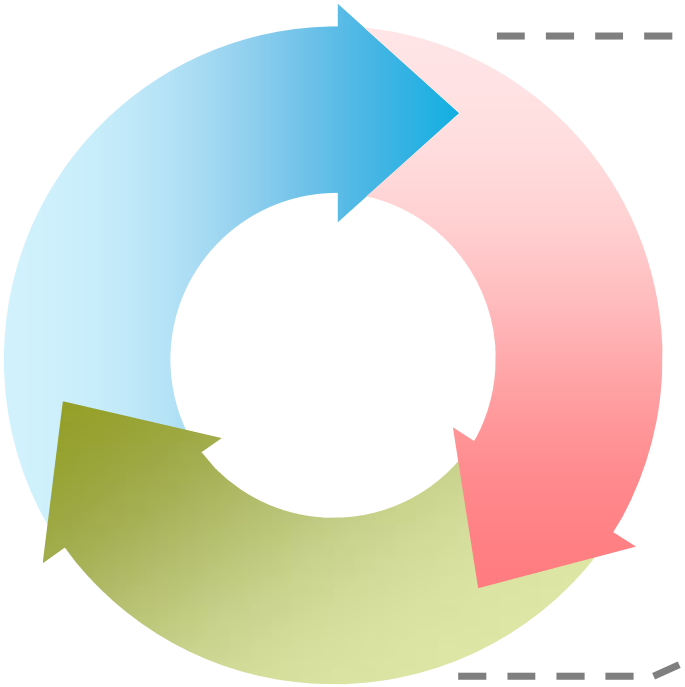
指導教員
花岡悟一郎 先生

メンバー
塩澤 響　西垣 佳亮　三平 大悟　登丸 尚哉

活動内容

活動方法

2週間に1回レポート提出



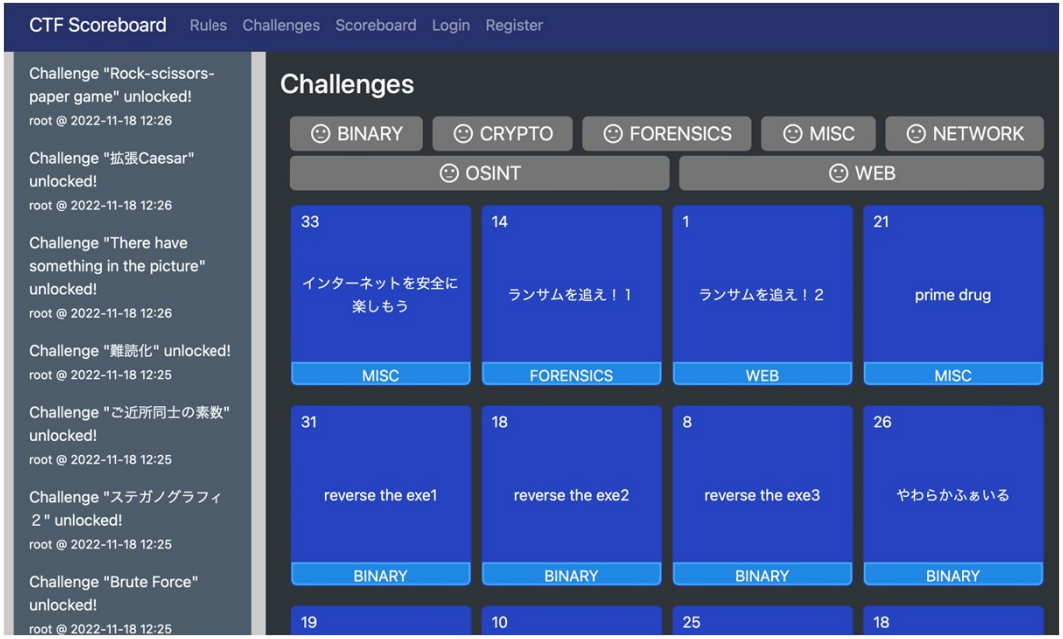
勉強内容を元に提出する
レポートを作成

提出レポートの添削及び
改善点の提示

修正内容についての質問や議論、
テーマについての勉強

CTF神奈川　作問

ネットワーク分科会と合同でCTF神奈川2022の作問を行った。



暗号分科会では以下の問題を作成、協力した

・拡張ユークリッドの互除法などを用いた脆弱RSA暗号への攻撃を実装する問題

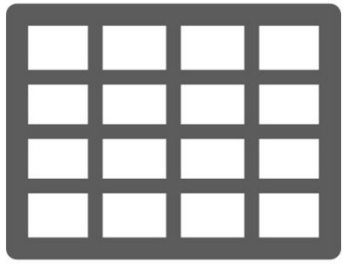
・ストリーム暗号の性質を利用し、平文の解読を行う問題

・zipパスワードを総当たりさせる問題

https://www.iisec.ac.jp/news/20221118news.html

活動テーマ

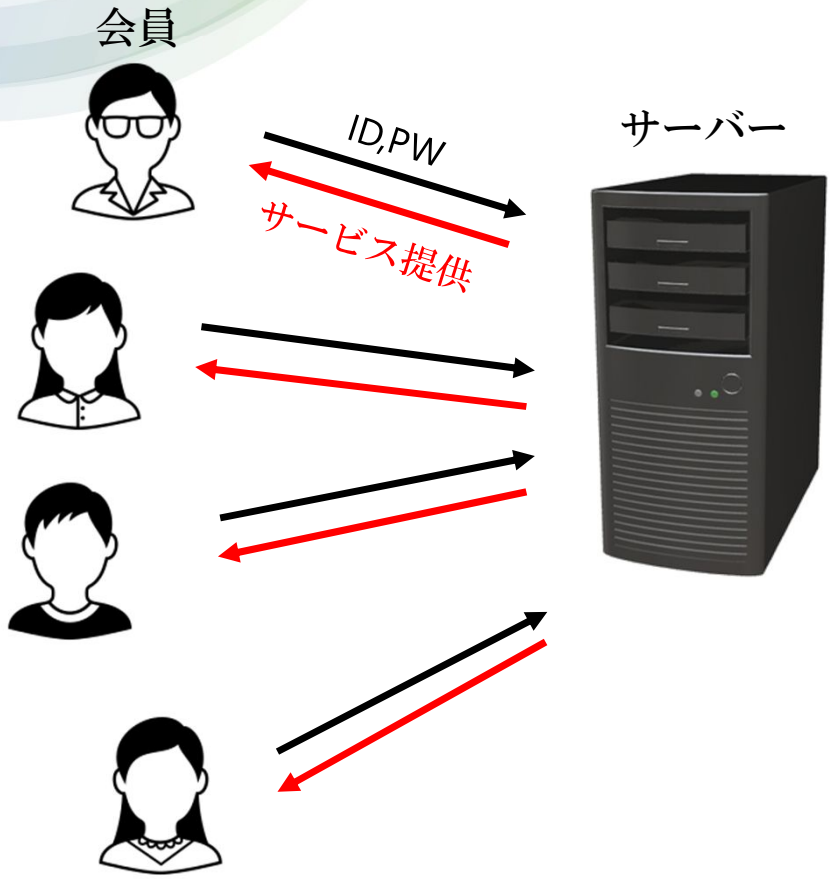
三平 大悟	検索可能暗号
西垣 佳亮	格子暗号
登丸 尚哉	グループ署名



グループ署名について

グループ署名が必要となった背景

- インターネットの普及に伴い会員制サービス体系が広がっている



しかし、サービス提供者は会員IDから利用時間、行動履歴などが特定可能である

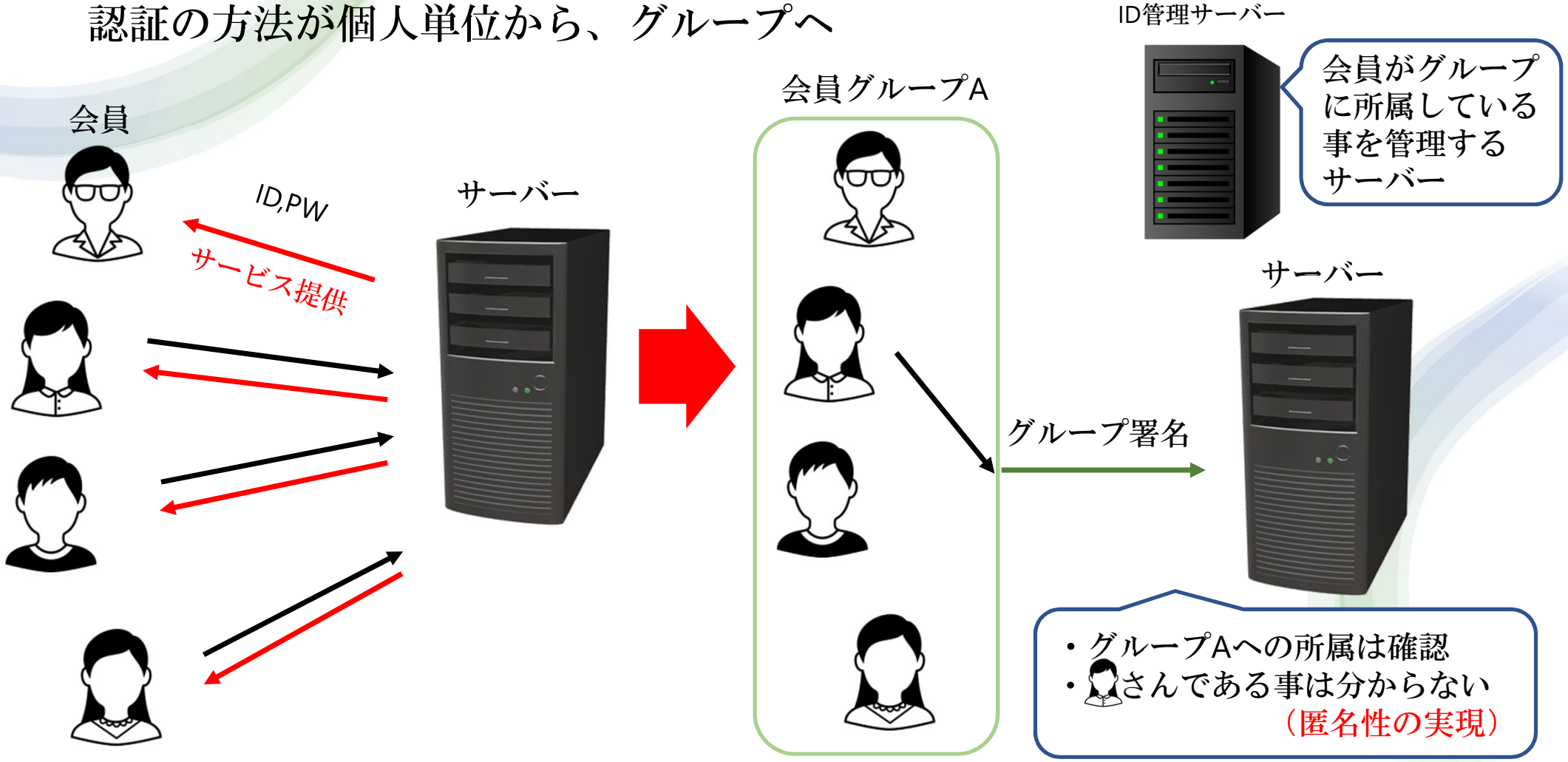
ユビキタス社会においてプライバシー問題に該当する可能性がある

会員名と紐付けするサービスではサービス提供者が会員IDで認証する事は必要

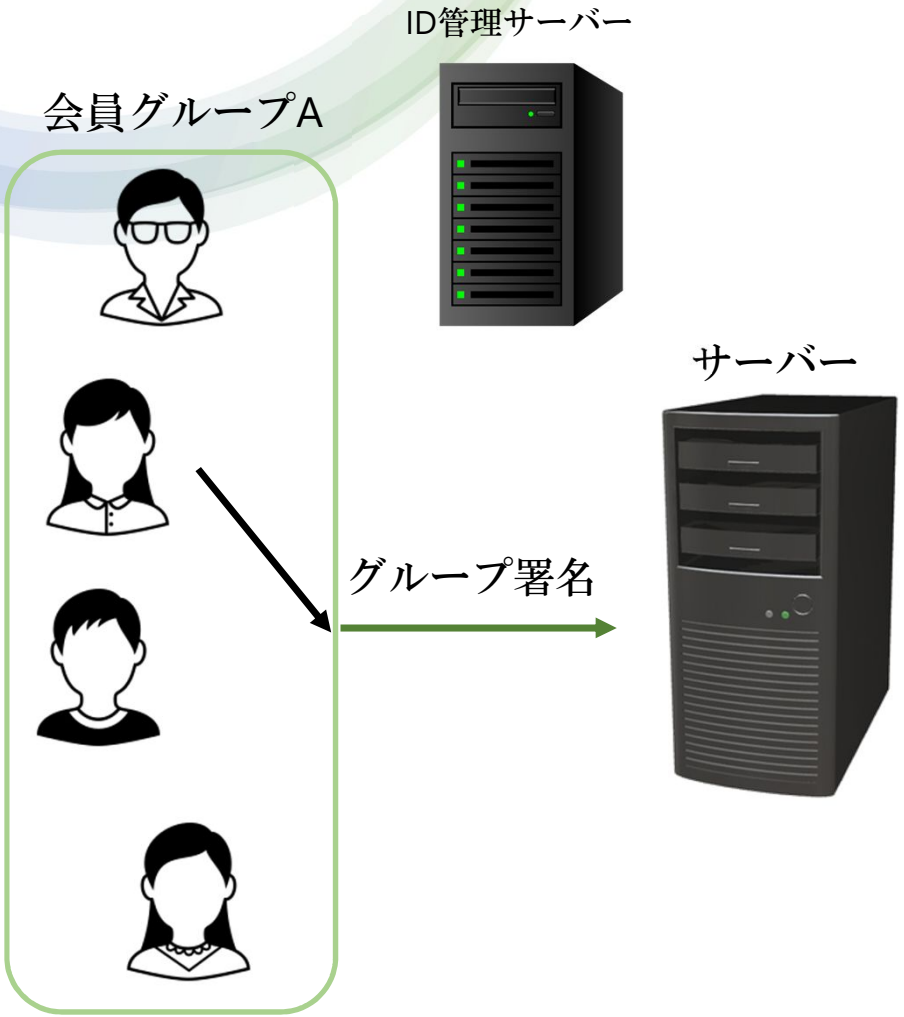
一方で紐付けが必要ない場合、会員個人ではなく所属しているグループで認証する事が可能

グループ署名が必要となった背景

認証の方法が個人単位から、グループへ



グループ署名の機能



・正当性
グループAに所属している会員なら必ずサービスを受けられる

・偽造不可能性
グループAに所属してない人はグループ署名が作成できず、サービスを受けられない

・匿名性
ID管理者以外、グループ署名から会員を特定できない

・関連付け不可能性
同一人物が複数回グループ署名を作成してもID管理者以外、会員を特定できない

・追跡可能性
ID管理者のみグループ署名から会員個人を特定できる

グループ署名を構成する技術：公開鍵暗号

暗号化を行う鍵 (公開鍵) と復号化を行う鍵 (秘密鍵) を異なる伴で行う暗号方式

③暗号文の送信

公開鍵暗号
復号化アルゴリズム

④暗号文と秘密鍵を用いて復号化アルゴリズムを実行し文書を復号

公開鍵暗号
暗号化アルゴリズム

②文書と公開鍵を用いて暗号化アルゴリズムを実行し暗号文を作成

①鍵生成アルゴリズムを実行し
公開鍵と秘密鍵を生成

公開鍵暗号
鍵生成アルゴリズム

暗号化を行う鍵 (公開鍵)

復号化を行う鍵 (秘密鍵)

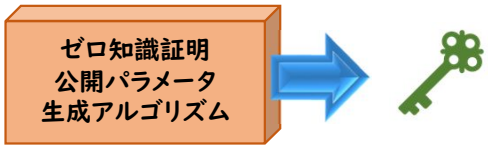
グループ署名を構成する技術：ゼロ知識証明

自分が秘密の情報を知っていることを, その情報自体を明かさずに相手に証明する手法

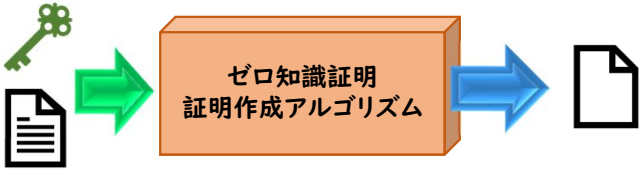
秘密の情報

③証明を送信

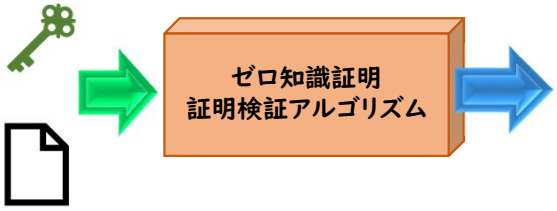
①公開パラメータの生成



②公開パラメータと秘密の情報から
証明作成アルゴリズムを実行し
証明を作成



④公開パラメータと証明から証明検証アルゴリズム
を実行し検証



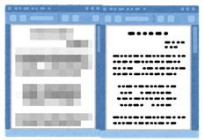
検証が通れば秘密の情
報を知っていると判断

ゼロ知識証明の応用例として次に挙げる
ディジタル署名技術がある

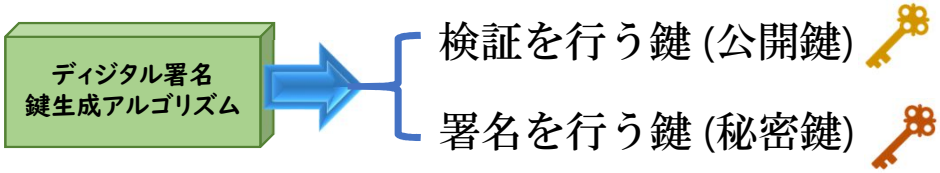
グループ署名を構成する技術：ディジタル署名

ディジタル署名とは紙の文書における押印やサインに相当する電子的な署名. 電子文書や情報の作成者を明確にし改ざんされていないことを証明するデジタル的な仕組み.

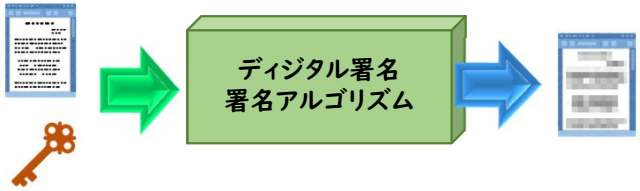
③文書と署名文を送信



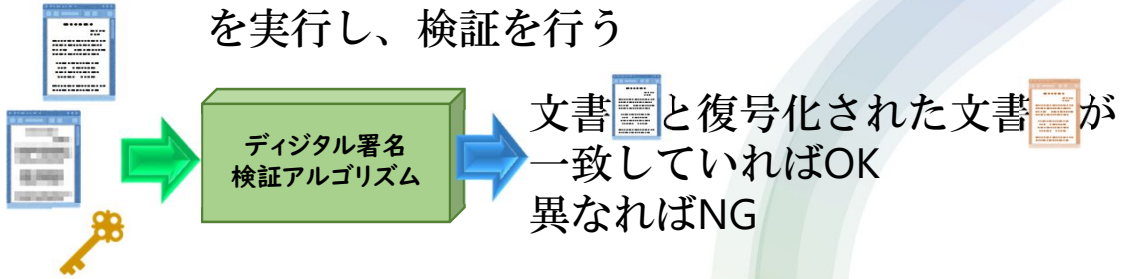
①鍵生成アルゴリズムを実行し検証鍵と署名鍵を生成



②送信する文書と署名鍵を用いて署名アルゴリズムを実行し、署名文を作成



④文書と署名文、検証鍵を用いて検証アルゴリズムを実行し、検証を行う



公開鍵、秘密鍵を用いる事で秘密鍵を開示すること無く秘密鍵を所持していることを証明できる。
また署名作成者本人が開示している公開鍵から検証を行う為、署名の本人確認が可能になっている。

グループ署名を構成する技術

従来のディジタル署名を用いた認証方式だと個人単位の検証鍵を公開する為、匿名性を保持できない

検証鍵と署名鍵の対応を1対1から1対nにする事で、1つの検証鍵で複数の検証が可能になる

ID管理サーバーが会員の管理を行う事で実現出来る点

- グループで一つの検証鍵、会員それぞれの署名鍵の対応を実現可能
- 個人を特定出来るデジタルIDは匿名性の観点からサービス提供者へ明かせない秘密の情報の一つとなる。デジタルID をID管理サーバーが発行し、会員がディジタル署名を作成する事で、サービス提供側には一切の個人を特定出来る情報を開示する事無く、秘密の情報 (今回はグループに所属している事を証明するディジタルID)を保持している事を証明する事が出来る。

グループ署名の仕組み：登録

①登録を申請

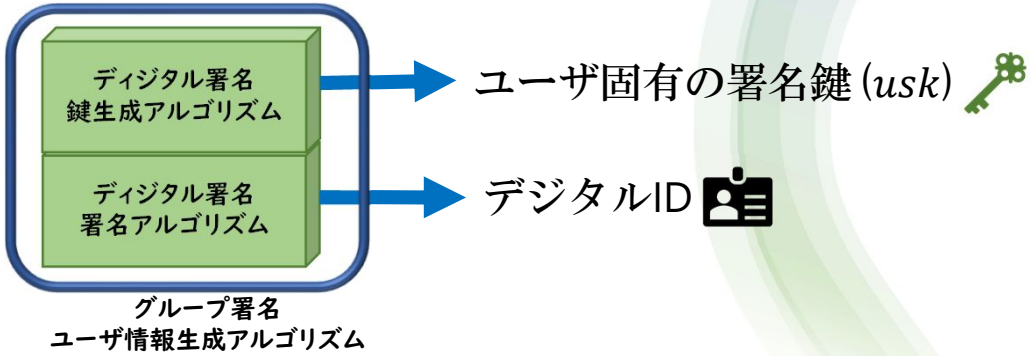
③署名鍵(usk)と
デジタルIDを送信

⓪グループ固有の公開鍵と秘密鍵を作成

・公開鍵暗号を利用する目的について

グループ署名には匿名性と追跡可能性が求められる。GMが管理する公開鍵暗号をデジタルIDに利用する事でこれらの機能を実現する役割を持つ。

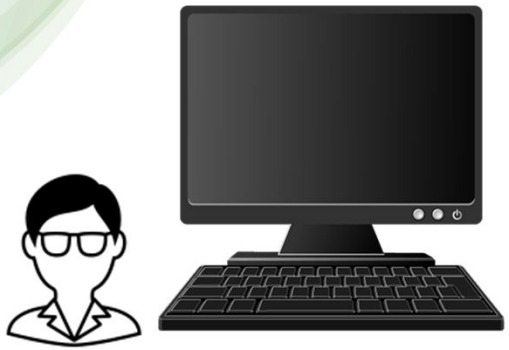
②検証鍵がgpkとなる、ユーザ毎の署名鍵とデジタルIDを作成



グループ署名の仕組み：署名

ユーザ

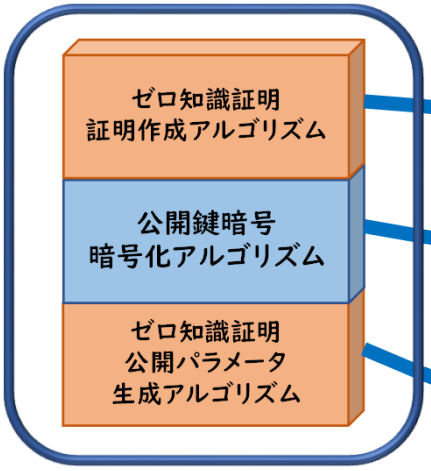
署名鍵(usk)



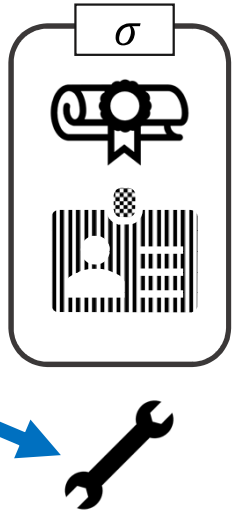
・ゼロ知識証明を利用する目的について

グループ署名には正当性と偽造不可能性、関連付け不可能性が求められる。ゼロ知識証明がこれらの機能を実現する役割を持つ。

④メッセージMに対してusk、gpk、デジタルIDを用いてグループ署名σを作成する



グループ署名
グループ署名生成アルゴリズム



グループに所属している事の証明書

gpkを用いたデジタルIDの暗号文

検証の際に利用する公開パラメータ

グループ署名の仕組み：検証

ユーザ

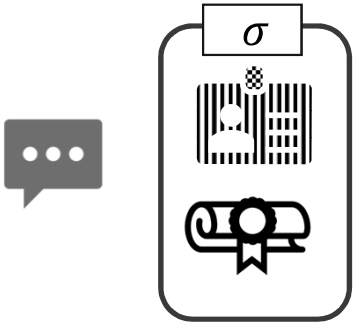
署名鍵 (usk)
公開パラメータ

ID管理サーバー (GM)

GM公開鍵 (gpk)
GM秘密鍵 (gsk)

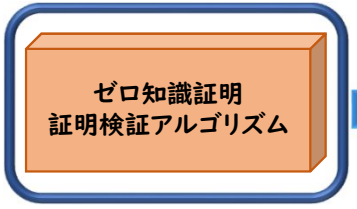
デジタルIDが暗号文のままグループに所属しているかの判断が可能なので匿名性が保たれる

⑤メッセージMと署名σを送信



サーバー

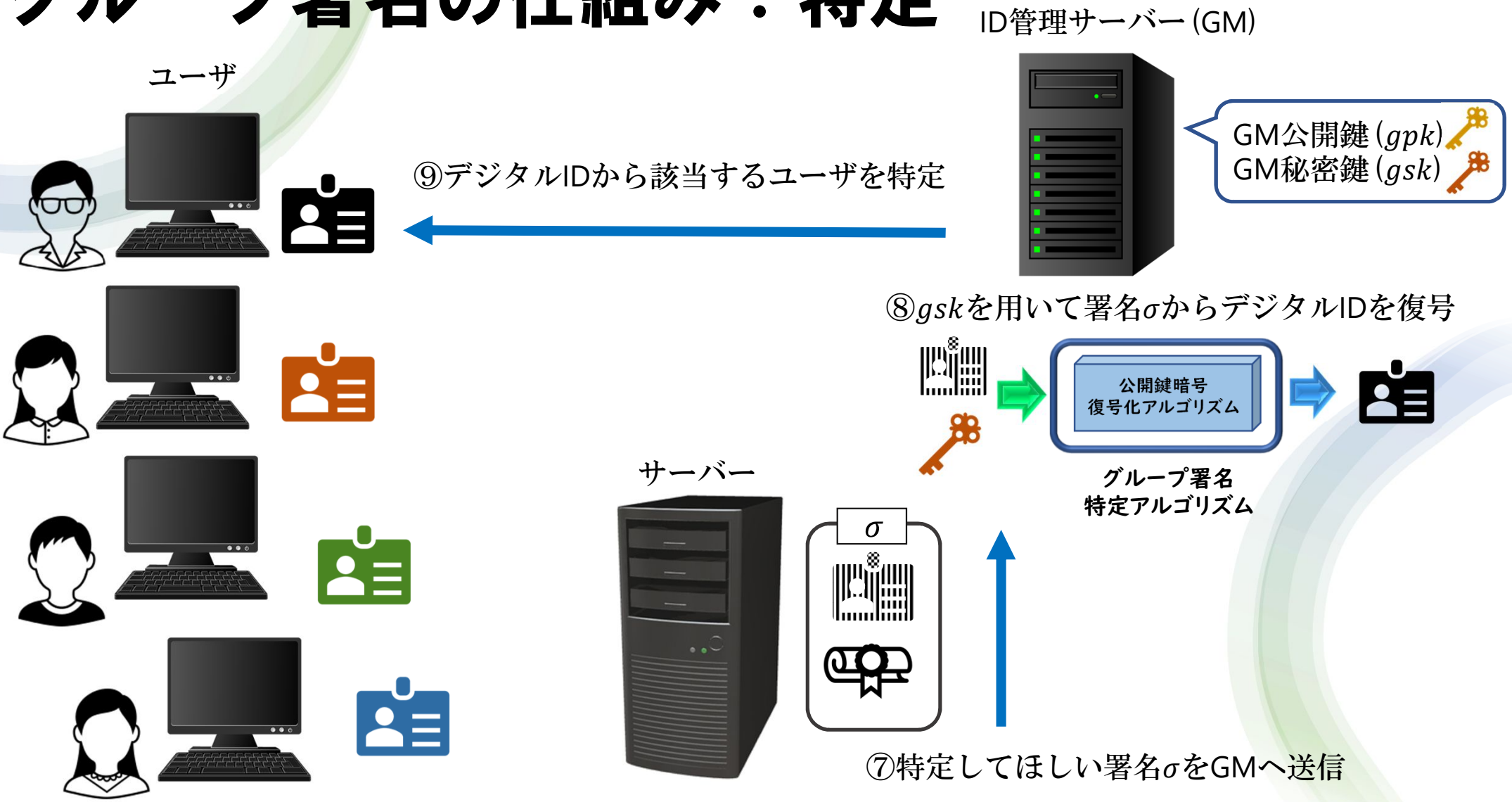
⑥署名σから証明書とgpk、公開パラメータを用いて検証を行う



グループ署名
検証アルゴリズム

検証結果が正しければグループに所属していると判断しメッセージを受領

グループ署名の仕組み：特定



背景から見るグループ署名

現状の問題点

会員制サービス体系の普及により
サービス提供側が会員の利用時間、
行動履歴が特定可能な状況はユビキタス社会においてプライバシー問題に該当する可能性がある。

求められる事柄

個人単位ではなく、サービスを利用しているグループ単位で認証をする事でサービス提供側に個人を特定される事なく、サービスを利用したい。

グループ署名によって
・従来の1対1の認証ではなく1対nの認証が実現されていることから、グループ単位の認証が可能
・GMがユーザとグループを管理していることから、サービス提供側に個人情報がわたることはない
・単に匿名にするだけでなく特定したいユーザがいた場合GMを経由して特定することが出来る

グループ署名の機能の実現性

・正当性
仕組み②で作成される署名鍵とデジタルIDが正しい組ならば④で作成される証明書の検証⑥の結果が必ず正しいと出力される。

・偽造不可能性
署名鍵とデジタルIDが正しい組でなければ検証⑥の結果は正しくないと出力される。

・匿名性
デジタルIDに対してGMの公開鍵暗号を利用する事で、GM以外はグループ署名σ内にあるデジタルIDの暗号文を復号することが出来ない。

・関連付け不可能性
④で実行される署名アルゴリズム内では乱数値などが利用されるため、複数署名間での関連付けを行うことは出来ない

・追跡可能性
デジタルIDの暗号文はGMの公開鍵で暗号化されているので、GMのみが復号することが出来る。またデジタルIDはユーザ固有なので必ずグループ署名σを送ってきたユーザを追跡することが出来る。

・安全性
強RSA仮定やDDH仮定などが元で上記の機能要件が満たされている。またペリングを利用したBBS署名も提案されており、q-SDH仮定やDLDH仮定に基づく安全性で署名サイズも小さくなる。

検索可能暗号について

目次

検索可能暗号とは

暗号化された大量のデータの保管やキーワード検索のアウトソース化を安全に実現するための技術

背景

近年、クラウド・サービスを利用した業務のアウトソース化が進んでいる。このとき、外部事業者に機密性の高いデータを預託する場合、預託する前にデータの暗号化を行い、機密性を確保することを考える。しかし、単純な暗号化のみをしてデータを預けてしまうと、預託したデータから必要な情報を抽出・検索することができなくなってしまう

⇒検索可能暗号を利用することで、外部事業者にデータの内容を知られることなく、データの保管および検索を実施できる

検索可能暗号とは

実際のセキュリティインシデント

・アメリカの金融会社で、独自に運用していたWAFの設定ミスが原因で1億600万人を超える情報漏洩が発生した。サイバー攻撃者による攻撃で、脆弱になったAWSのEC2が不正アクセスを受け、大規模な情報漏洩に至った。

・ポートが閉じていると思っていたが、ポートを開放したままにしていたことに気付かず、不用意なポートの開放が原因で不正アクセスを受けてしまった。

引用元：https://www.rworks.jp/system/system-column/sys-entry/21978/

保護対象となるデータ

預託するデータ(ファイル)・キーワード

想定される攻撃者

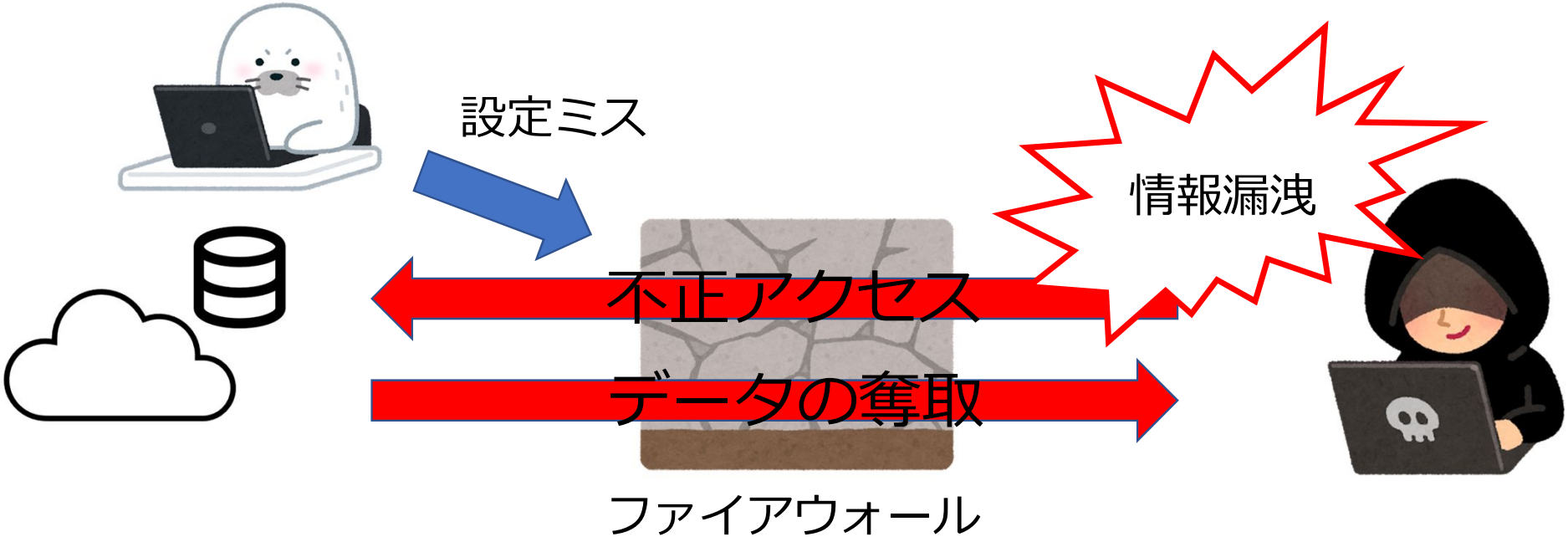
通信路を観測できる第三者・外部事業者

想定される攻撃

不正アクセス、情報漏洩

検索可能暗号とは

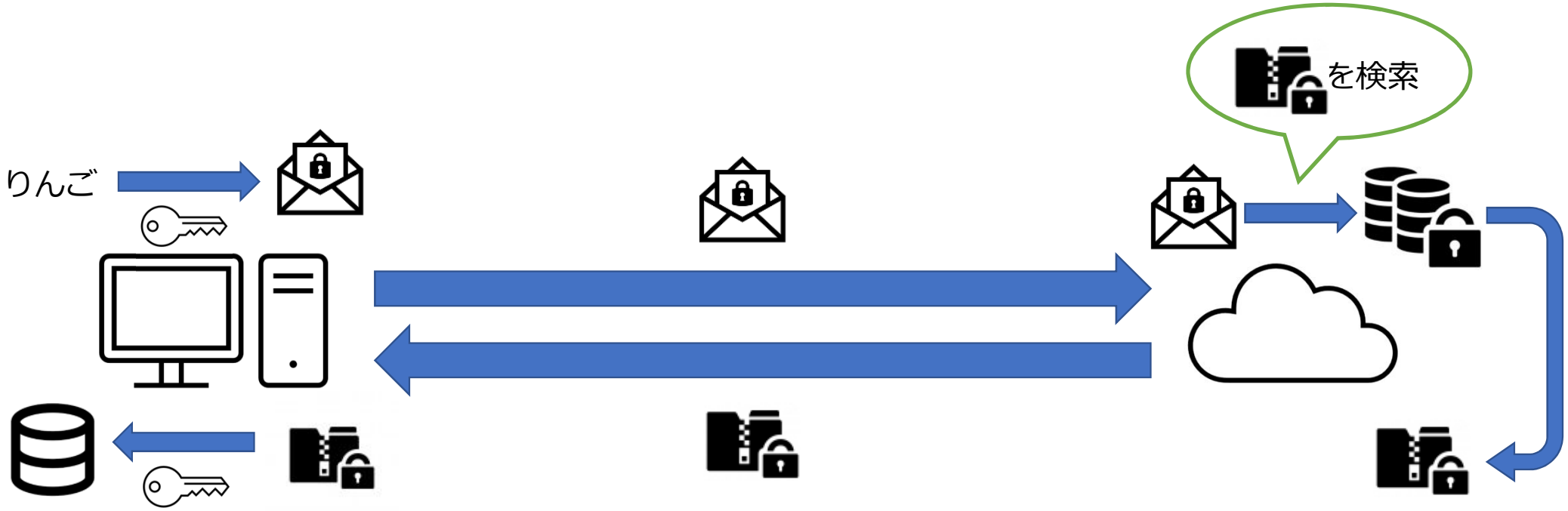
紹介したセキュリティインシデントの共通点



・情報漏洩は、「外部事業者の設定ミス」による脆弱性を狙った「外部からの不正アクセス」により発生した
⇒攻撃者を「外部事業者」と「第三者」に設定し、安全性を考える

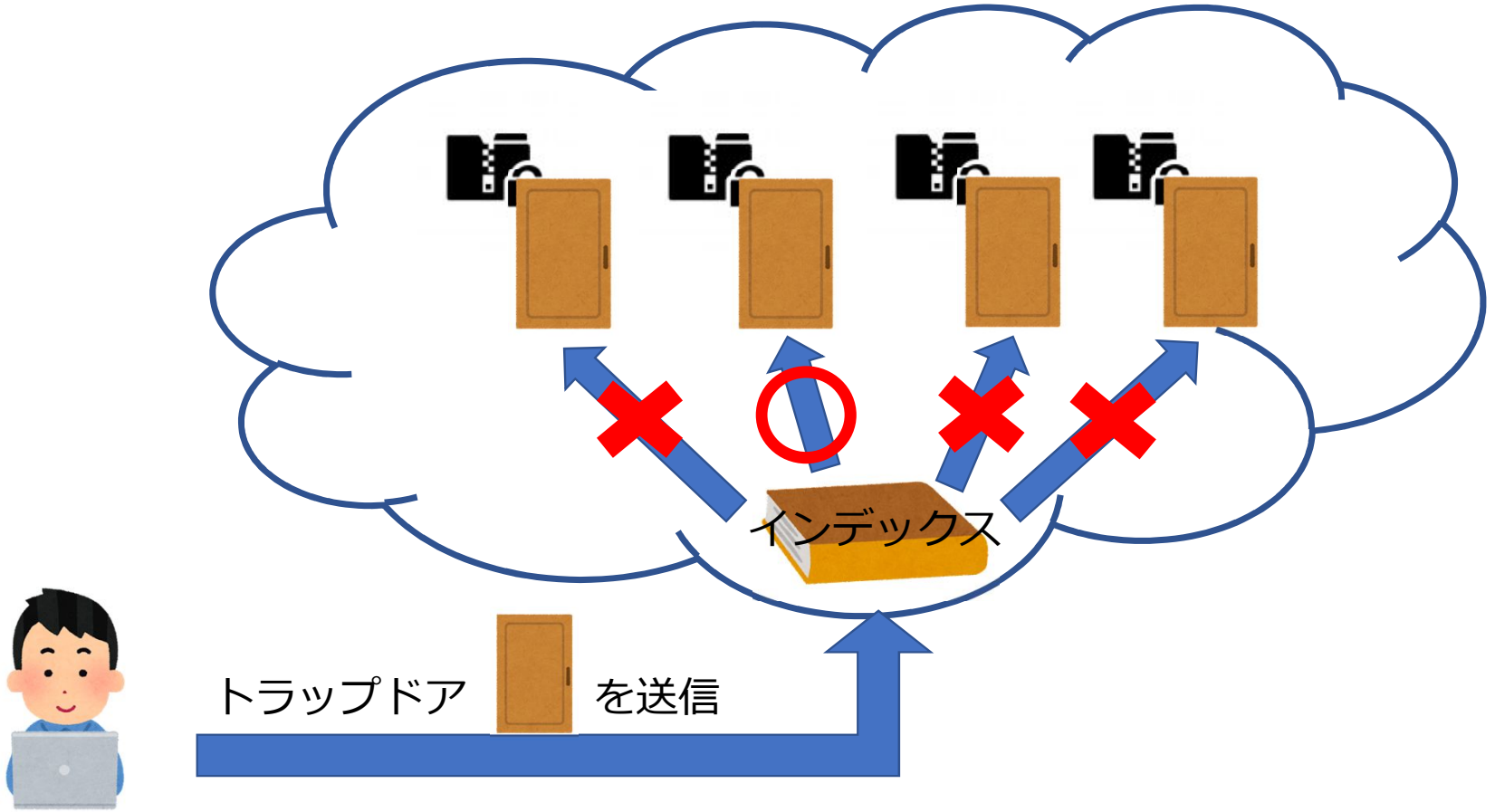
機能

暗号化されたデータと暗号化された検索ワードが**暗号化されたままの状態**で結び付くことができる機能



仕組み　具体的な実現方法

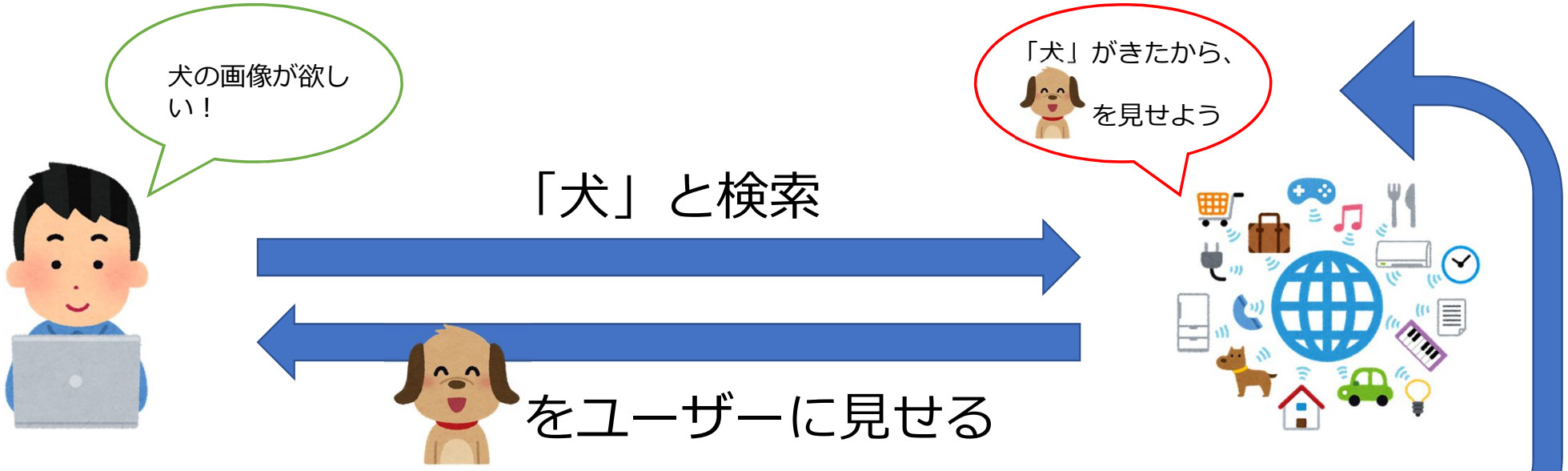
データそのものではなく、暗号化されたキーワード(トラップドア)と暗号文の対応関係を示したインデックス(索引)を介して、暗号文に対応したトラップドアを検索する



仕組み　具体的な実現方法

インデックスとは？

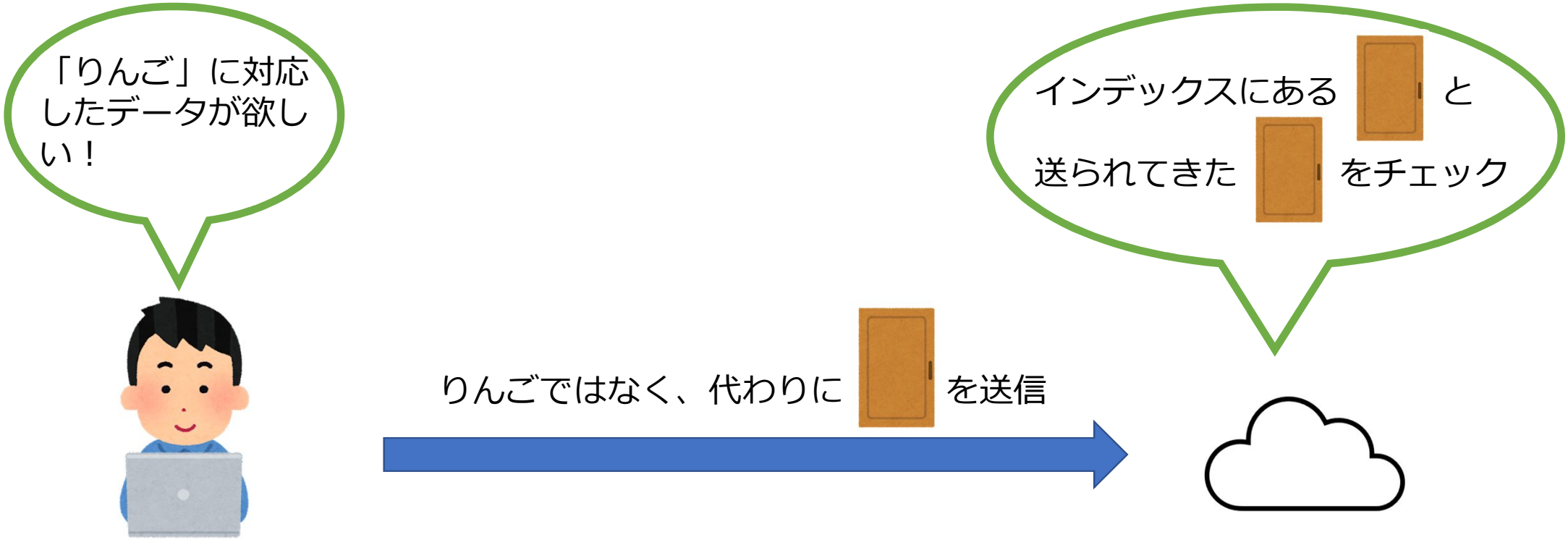
・・・預託したいデータと，データを検索するためのキーワードの対応関係を示したもの



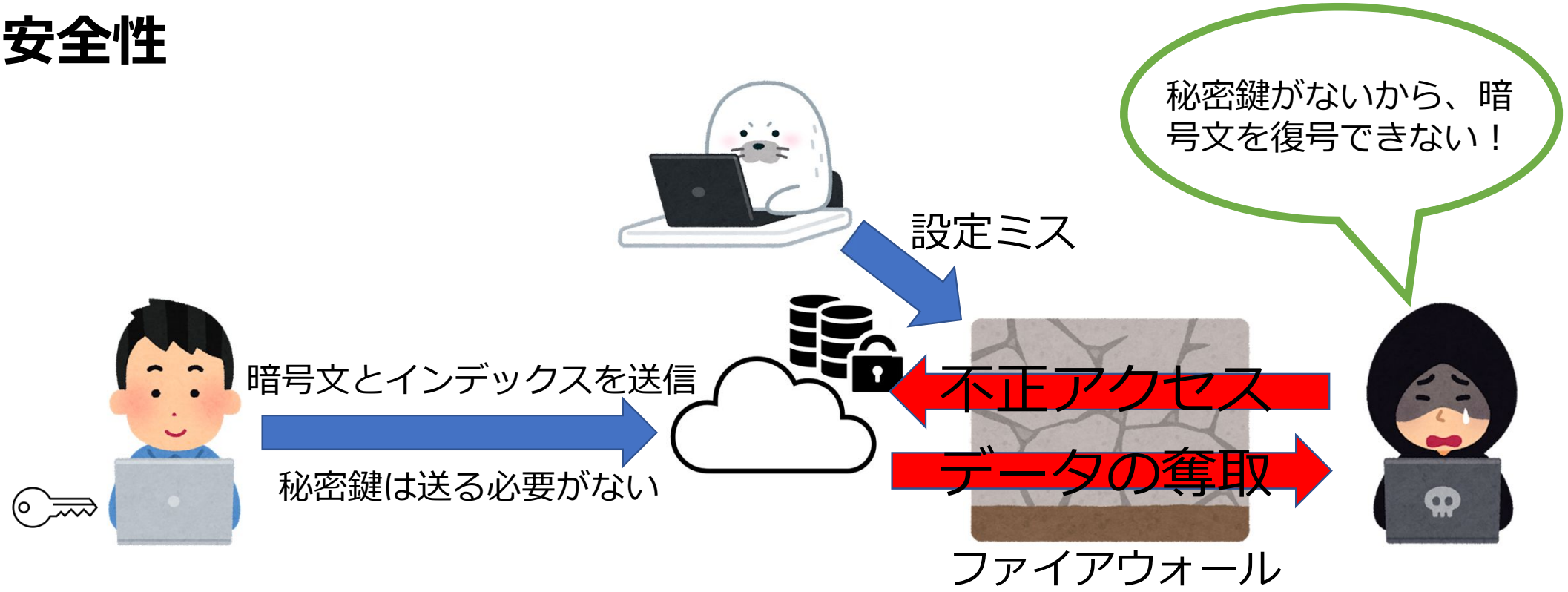
この処理を，データが暗号化された状態のまま実現するためのもの

仕組み　具体的な実現方法

トラップドアとは？
・・・キーワードがサーバーから見えないようにデータを検索するためのもの



安全性



「外部事業者の設定ミス」による脆弱性を狙った「外部からの不正アクセス」が発生しても、情報漏洩には至らない

外部事業者と通信路を盗聴できる第三者にデータの内容を知られることなく、データの保管および検索を実施できている(機密性を確保できている)

Adobe Acrobat Document

格子暗号

西垣佳亮

2023 年 1 月

中央大学大学院理工学研究科情報工学専攻

量子計算機の出現が暗号に及ぼす影響

量子計算機は，古典計算機では現実的な時間内で解けなかった問題も，古典コンピュータより短い時間で高い確率で解を出すことができる．

アルゴリズム	計算量 (n はビット数)	解ける問題	影響を受ける代表的な暗号
Shor のアルゴリズム	n の多項式時間	離散対数問題 素因数分解問題	ElGamal 暗号 DH 鍵交換 楕円曲線暗号 RSA 暗号
Grover のアルゴリズム	$O(2^{n/2})$	探索問題	共通鍵暗号

現代の標準暗号の安全性はいずれ崩れ去る

量子計算機の開発動向

1999 年 NEC 基礎研が世界で初めて超電導の量子ビットを開発

2019 年 IBM が世界初の商用量子ゲート計算機を発表．27 qbit を持つ．

2020 年 IBM が 65 qbit の量子ゲート計算機を建造．

2021 年 IBM が 127 qbit の量子ゲート計算機を建造．

いずれ来る危殆化

現在使われている RSA-2048 を現実的な時間で解くには 2000 万 qbit の量子ゲート計算機が必要と見積もられ，量子ゲート計算機がその規模で実現されるのは 2030 年ごろと予想されている．

耐量子暗号の標準化

NIST による PQC 標準化は 2022 年 7 月に第 3 ラウンドが終了し，4 つの耐量子暗号アルゴリズムが標準化されることになった．

CRYSTAL-Kyber LWE 問題を安全性の根拠に持つ公開鍵暗号アルゴリズム

CRYSTAL-Dilithium LWE 問題を安全性の根拠に持つ電子署名アルゴリズム

FALCON NTRU 問題を安全性の根拠に持つ電子署名アルゴリズム

SPHINCS+ ハッシュ関数を用いる電子署名アルゴリズム

有望な暗号方式に **LWE** 問題と **NTRU** 問題を安全性の根拠にしたものがある．それらはいずれも格子暗号という部類のもの．

LWE 問題 i

まずは適当な n 変数一次多項式を n 本用意し，それらを $h_1, h_2, \cdots, h_n$ とする．各 h_i は係数 c と絶対値の小さなノイズ e を用いて $h_i = \sum_{j=1}^{n} c_j x_j + e_i$ となる．

LWE 問題とは，これらの多項式の値

$$\begin{cases} h_1(x_1, \cdots, x_n) = b_1 \\ \quad \vdots \\ h_n(x_1, \cdots, x_n) = b_n \end{cases} \tag{1}$$

が b_i と定まっているとき $x_1, \cdots, x_n$ を求める問題である．

LWE 問題 ii

$$\begin{cases} h_1(x_1, \cdots, x_n) = b_1 \\ \vdots \\ h_n(x_1, \cdots, x_n) = b_n \end{cases} \rightarrow$$

$$A\boldsymbol{x} + \boldsymbol{e} = \boldsymbol{b}$$

但し $A = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}$, $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$,

$\boldsymbol{e} = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$, $\boldsymbol{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$

多項式の表現を行列に書き直すと格子暗号と呼ばれる所以がわかる．LWE 問題は $\boldsymbol{b}$ に最も近い A の列ベクトルが生成する格子 $L(A)$ の中の点を求める問題に書き換えることができる．

LWE 問題 iii

CVP : Closest Vector Problem

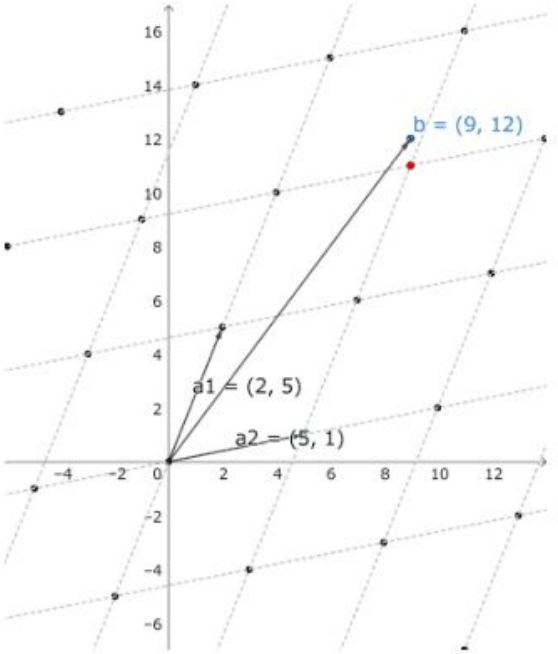
n 次元の基底 A が与えられ，ユークリッド空間 E^n のある点 $\boldsymbol{b} \in E^n$ に最も近い格子点 $\boldsymbol{v} \in L(A)$ を求める問題.

例

$$A = \begin{pmatrix} 2 & 5 \\ 5 & 1 \end{pmatrix}$$

$$\boldsymbol{x} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

$$\boldsymbol{e} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



LWE 問題　iv

SVP : Shortest Vector Problem

n 次元の基底 A が与えられ，ユークリッド空間 E^n の原点 O に最も近い非零格子点 $\boldsymbol{v} \in L(A)$ を求める問題．

γ-近似 SVP

基底 A から生成される格子 $L(A)$ の非零最短ベクトル $\boldsymbol{u}$ について $|\boldsymbol{v}| \leq \gamma \cdot |u|)$ となるベクトル $\boldsymbol{v}$ を求める問題．

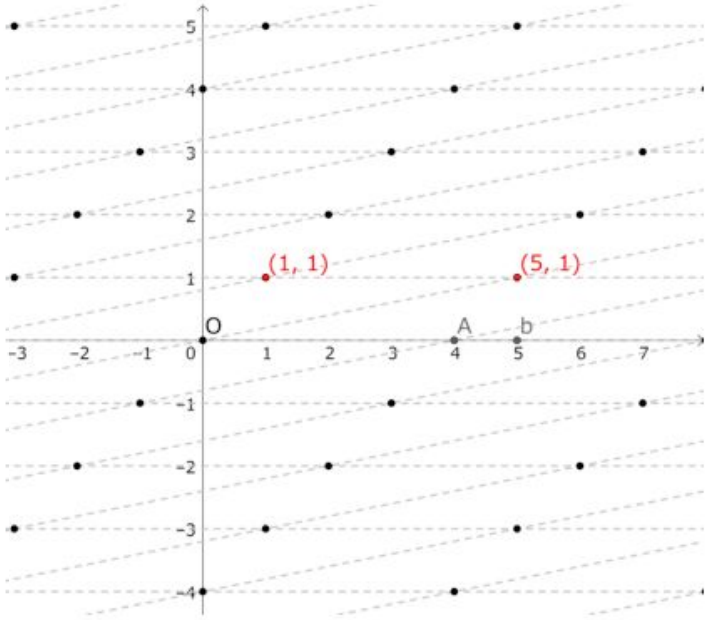
CVP は基底に別のベクトルを付け足すことによって高次元の空間に格子を埋め込み SVP に変換できる．

新しい基底は $\hat{A} = \begin{pmatrix} A & \boldsymbol{b} \\ \boldsymbol{0} & 1 \end{pmatrix}$ として作る．

LWE 問題 v

例

1 次元の CVP を 2 次元の SVP に埋め込む例.

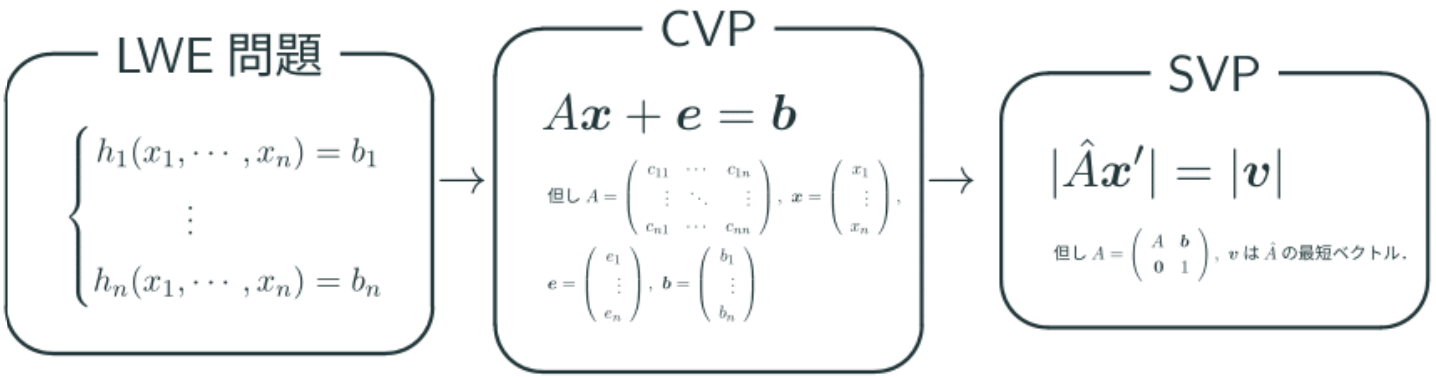


$$A = (4)\,,\ \boldsymbol{b} = (5),$$

$$\hat{A} = \begin{pmatrix} 4 & 5 \\ 0 & 1 \end{pmatrix}$$

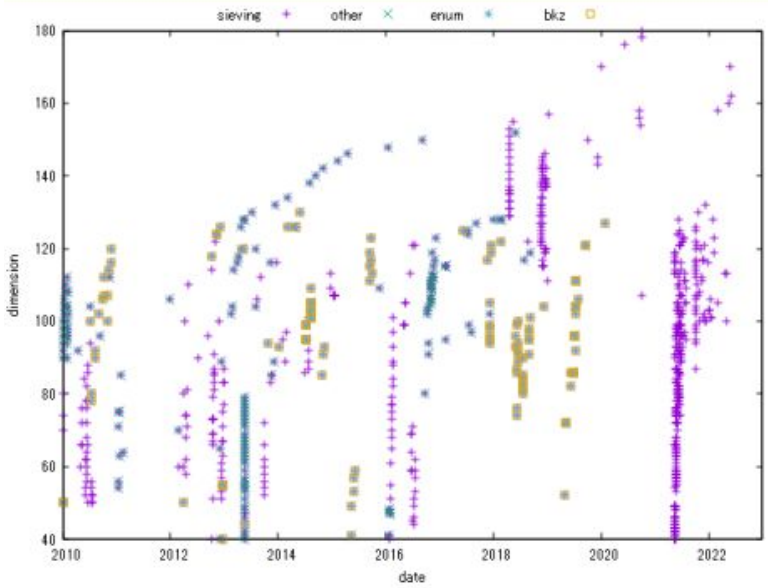
$\left\{ \begin{pmatrix} 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \end{pmatrix} \right\}$ により生成される格子の最短ベクトルは $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ になる. $\boldsymbol{e} = (1)$ になる.

格子暗号解読の難しさ



LWE 問題は SVP に帰着できる．SVP は NP 困難であることが知られており，難しい．実際に 2 次元より大きい SVP を解くには，基本的には全探索を行うことになる．

SVP challenge



SVP Challenge で解かれた次元数

2018 年，2021 年に多くの記録が更新されている．特に，Sieving は殆どの次元で他のどのアルゴリズムよりも優秀な結果を残している．

Enumration 初期の記録を生み出した手法．基底ベクトルの組み合わせを効率的に全探索する．

Sieving 2018 年から現在にかけて記録を多く生み出した手法．格子点を大量に用意して，原点へ向けて凝縮させていく．

格子暗号の安全性

SVP Challenge の結果から，LWE 問題を安全性の根拠とする暗号の安全なパラメータが決定できる．現在の格子暗号は 500 次元から数千次元あれば実用に耐えうる速度と安全性を兼ね備えるとされている．