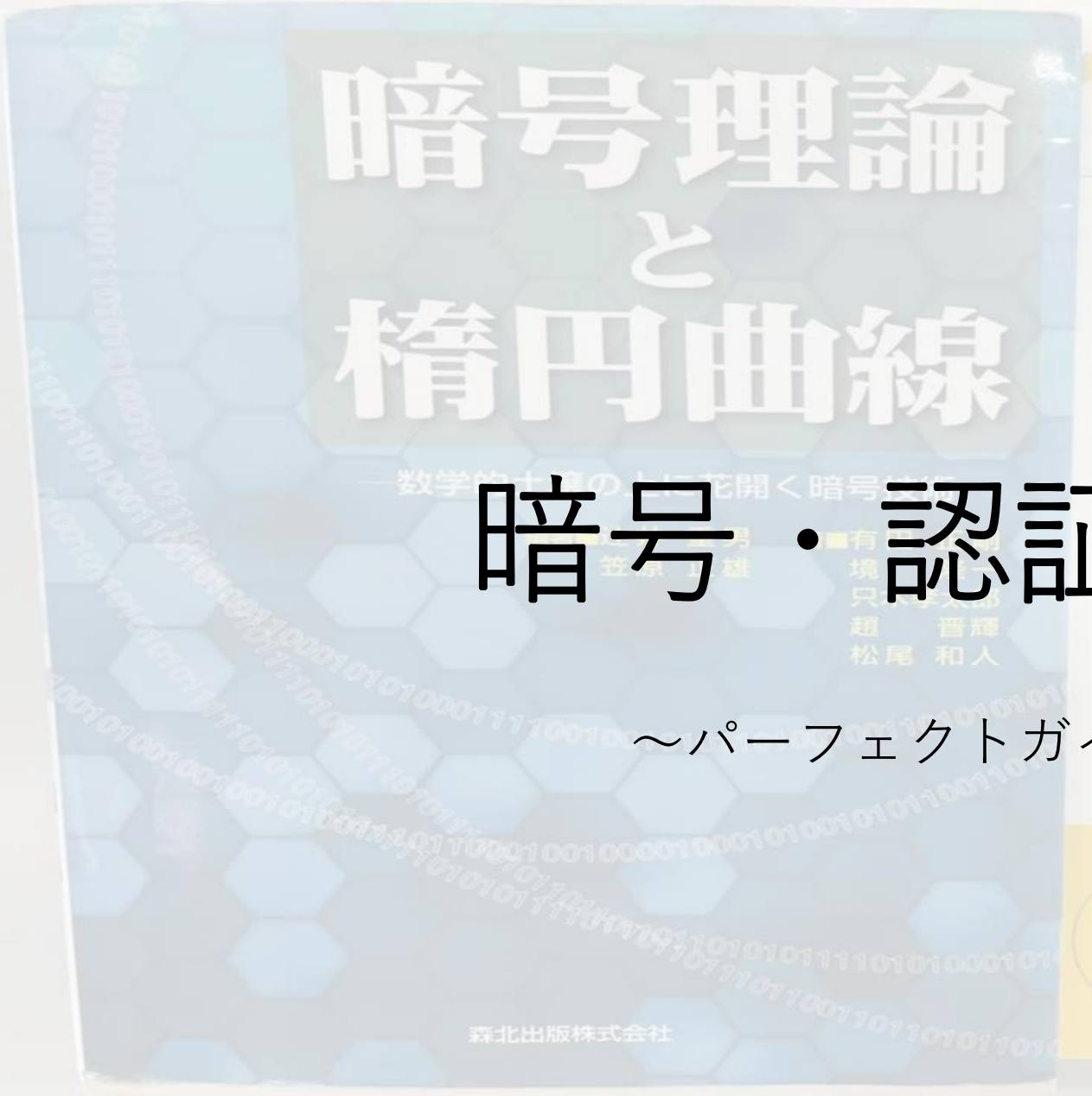


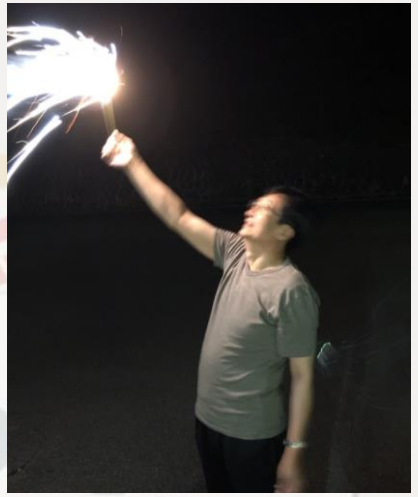
暗号・認証分科会

～パーフェクトガイド～

活動紹介

- 暗号・認証分科会とは
- どのような活動をしているか
- ２０２１年活動テーマ紹介
  - 傅 豪：静脈認証技術
  - 塩澤 響：楕円曲線暗号を使用したDSAの変種の電子署名方式のECDSA
  - 土屋 璃和登：放送型暗号
  - 森田 匡博：認証付き暗号

暗号・認証分科会とは



活動目的

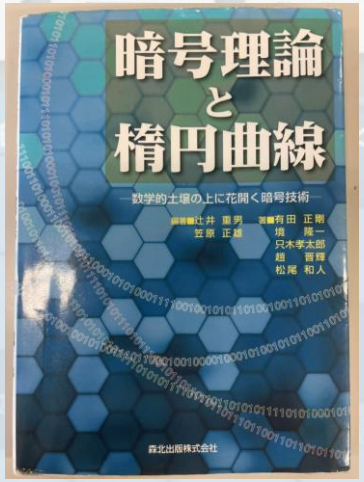
最先端にまでわたる暗号・認証技術を整理・体系化し、それに基づいて、**一般の人々が暗号・認証の安全性の本質を理解できるような説明手法を構築していくことを目標とします。**特に、安全性の厳密な定義の仕方と、それらの定義に関する安全性の証明のための具体的な手順について演習を行います。さらに、これを CRYPTREC （総務省・経済産業省暗号技術検討会）のガイドライン等に反映させ、暗号・認証技術 の適切な利用の推進に繋げたいと考えています。

研究キーワード

共通鍵暗号、公開鍵暗号、**楕円暗号**、IDベース暗号、電子署名、**ハッシュ関数**、
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、**鍵共有**、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

活動メンバー

研究リーダー
趙　晋輝



指導教授
花岡　悟一郎

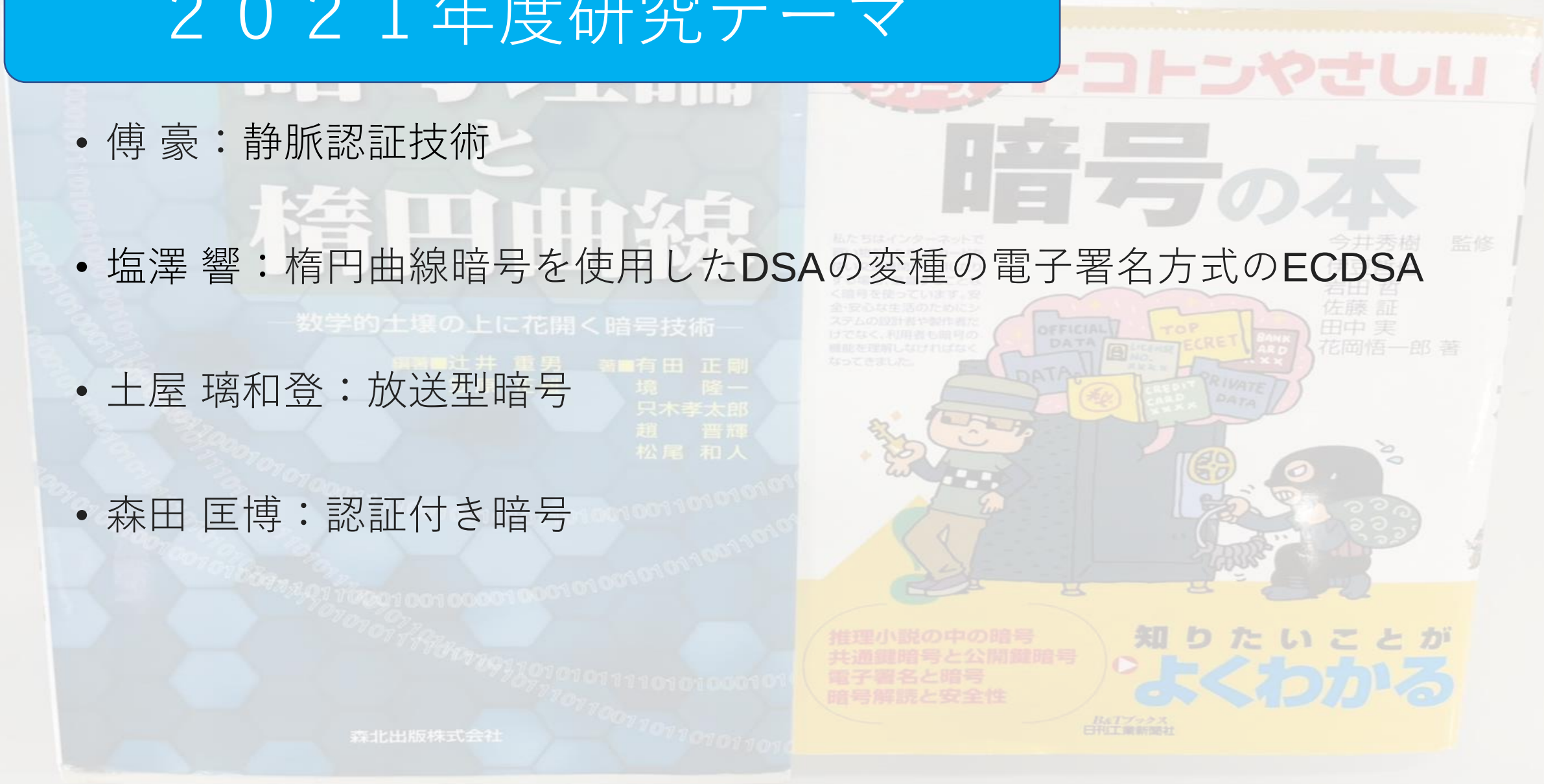
メンバー
傅 豪　塩澤 響　土屋 璃和登　森田 匡博

どのように活動しているのか？

二週間に一回提出

２０２１年度研究テーマ

- 傅 豪：静脈認証技術
- 塩澤 響：楕円曲線暗号を使用したDSAの変種の電子署名方式のECDSA
- 土屋 璃和登：放送型暗号
- 森田 匡博：認証付き暗号



ECDSAとビットコイン

21N00038K 塩澤　響

ECDSAとは

楕円曲線暗号を用いたDSAの変種の電子署名方式。

DSAで使用する暗号化や署名生成のアルゴリズムに楕円曲線を利用

特徴

・DSAと比較して約1/10のデータ長で同レベルの安全性がある。
・ビットコインなどの暗号通貨ではトランザクションの検証に使用される。

メッセージ: m

公開情報

曲線パラメータ: a, b
ベースポイント: G
素数: p

秘密鍵 $1 \leq k \leq p-1$

秘密鍵: n, k(一時的)

公開鍵

公開鍵: $W = nG$

メッセージのハッシュ値: f $f = h(m)$

署名 $V = kG = (x, y) \Rightarrow c = x \bmod p$

kGのx座標: c
検証用の値: S $S = k^{-1}(f + nc) \bmod p$

取得情報

公開情報: a, b, G, p
公開鍵: $W = nG$
署名: c, S
メッセージ: m

(1) メッセージmのハッシュ値を計算する

$$f = h(m)$$

(2) 取得した情報から楕円曲線上のx座標を求める

$$Q = \frac{fG}{S} + \frac{cW}{S} \bmod p = \frac{fG + cW}{S} \bmod p$$

$W(= nG,)\ S(= \frac{f+nc}{k})$ を代入する

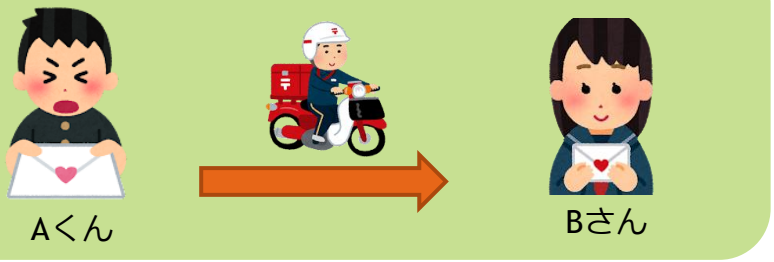
$$Q_x = \frac{fG+cW}{S} \bmod p = \frac{k(f+cn)}{f+nc} G \bmod p = kG \bmod p$$

(3) 求まったx座標とcが一致するかで検証を行う

$Q_x = c$ ⇨ OK
$Q_x \neq c$ ⇨ NG

少し考え方を変えてみましょう

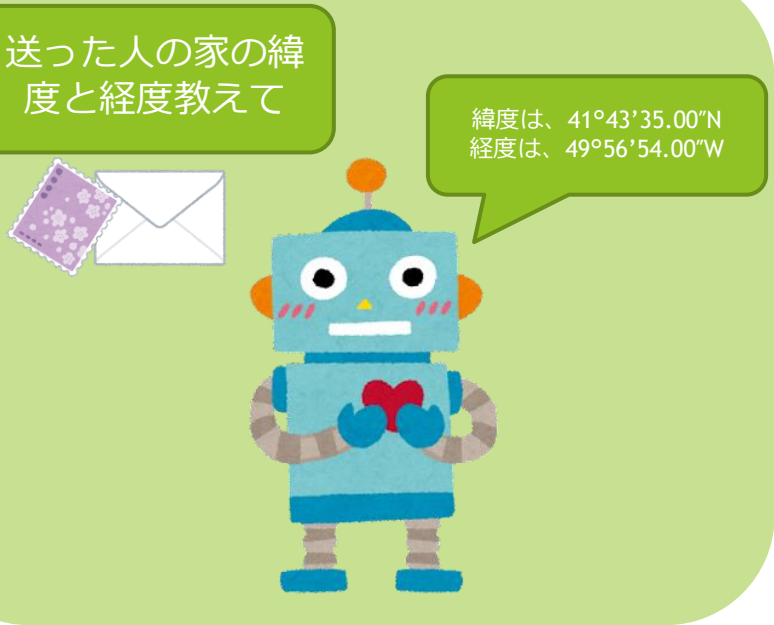
①



AくんがBさんにラブレターを書きました。

Bさんは本当にAくんが書いたのか確認しようと思いまいした。

②



確認するにはロボットを使います。

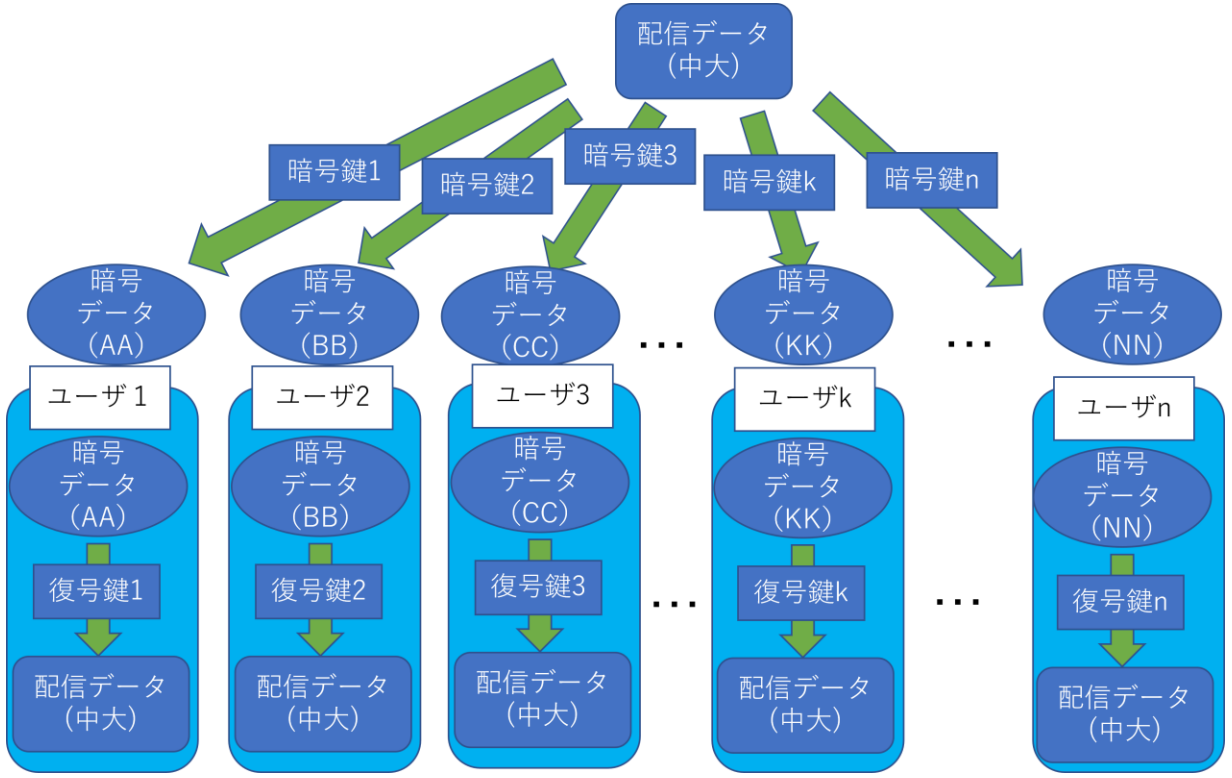
このロボットは、手紙と手紙についている切手を渡すと送った人の家の緯度と経度を教えるすごいロボットです。

放送型暗号

暗号・認証分科会所属　21N100013E 土屋璃和登

最も理想的なものは

個別に暗号化



しかし、個別に行うと

数が多いため、
帯域を圧迫し
てしまう

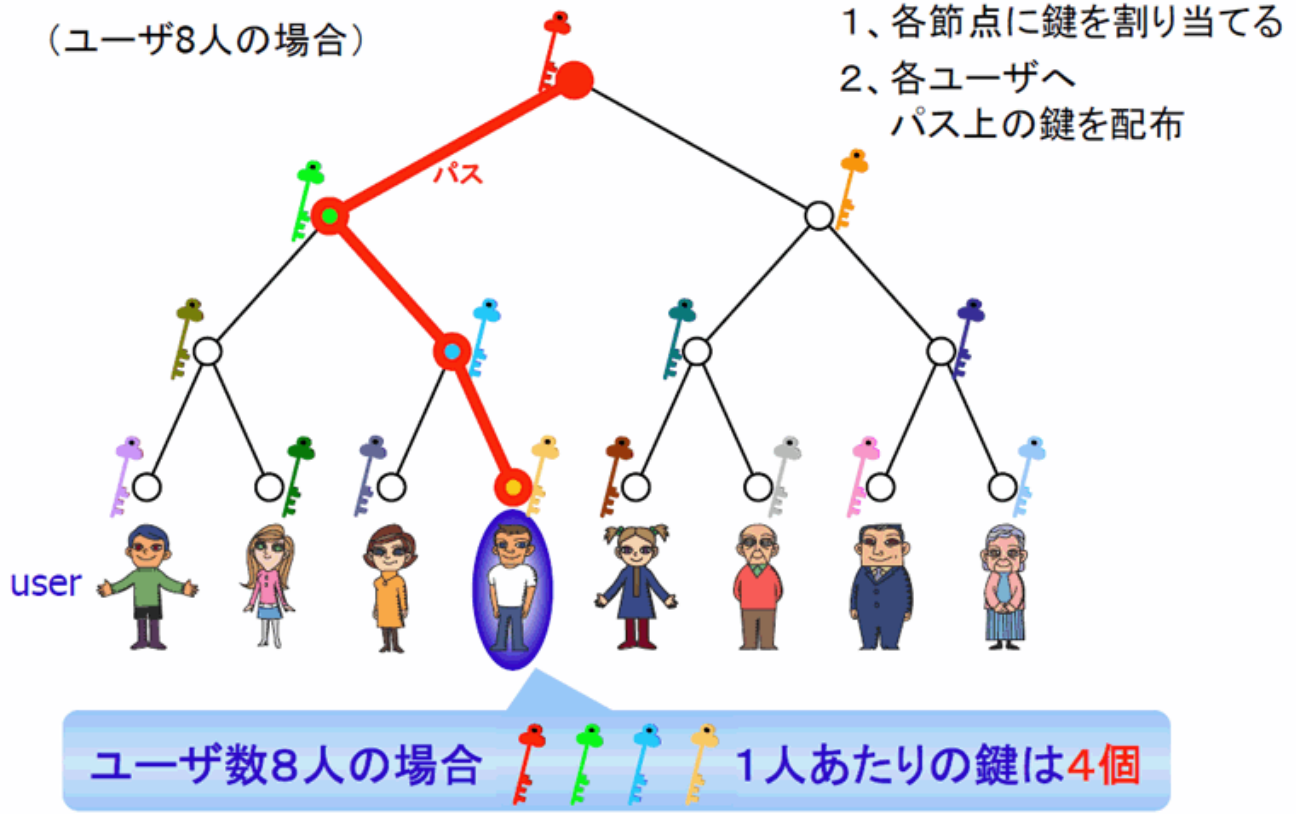
そこで

Complete Subtree Method(以下CS法)
と
Subset Difference Method(以下SD法)
を用いる.

CS法　ツリー構造と鍵の配布

①すべての節点と葉に異なる鍵を割り当てる.
②各ユーザに二分木の根から自分の葉までのパス上の鍵を配布する.

ユーザがn人の場合,
鍵の配布は$n * (\log_2 n + 1)$



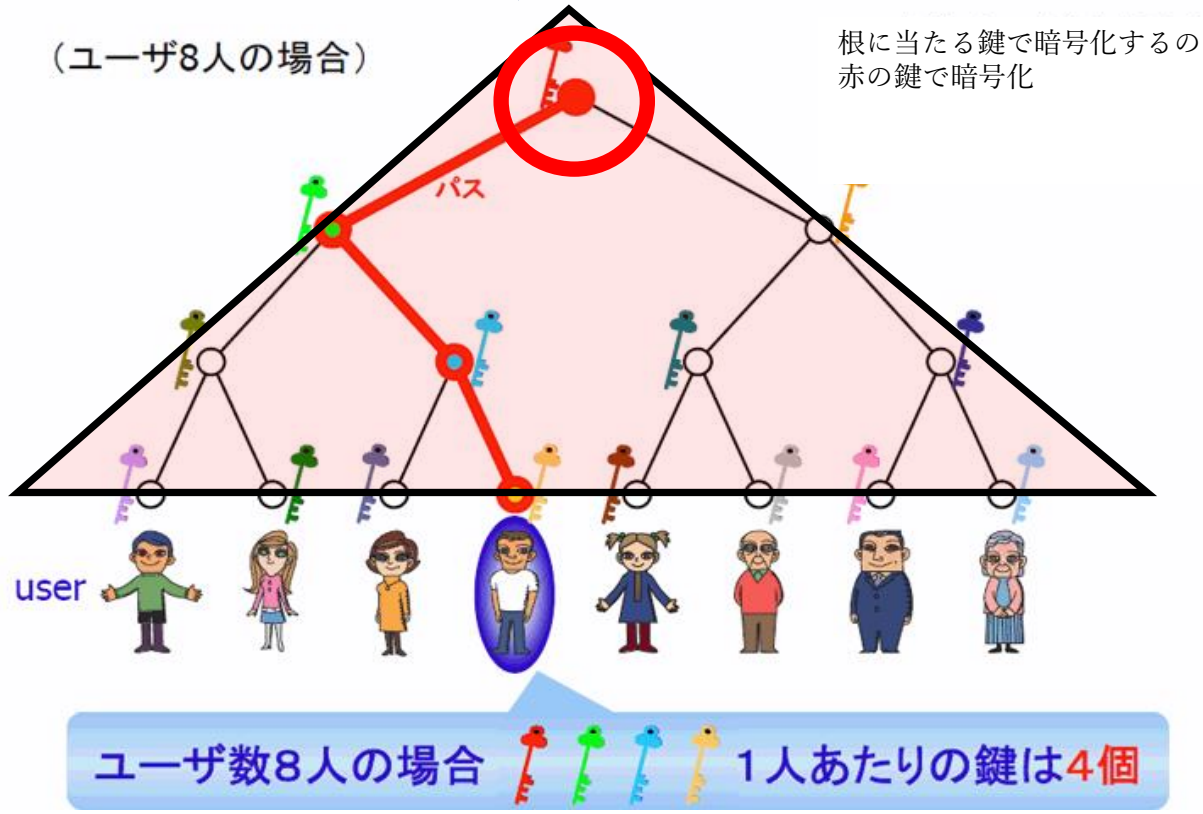
CS法　暗号化

配信データはすべてのユーザが所有する鍵で暗号化を行う。

ユーザは所有する鍵の中から対応する鍵で復号化する.

ユーザがn人の場合,
鍵の配布は$n * (\log_2 n + 1)$
配信するものは1個の鍵で暗号化すればよい.

不正ユーザがいない時、
必要な鍵は根である一つ
となる.

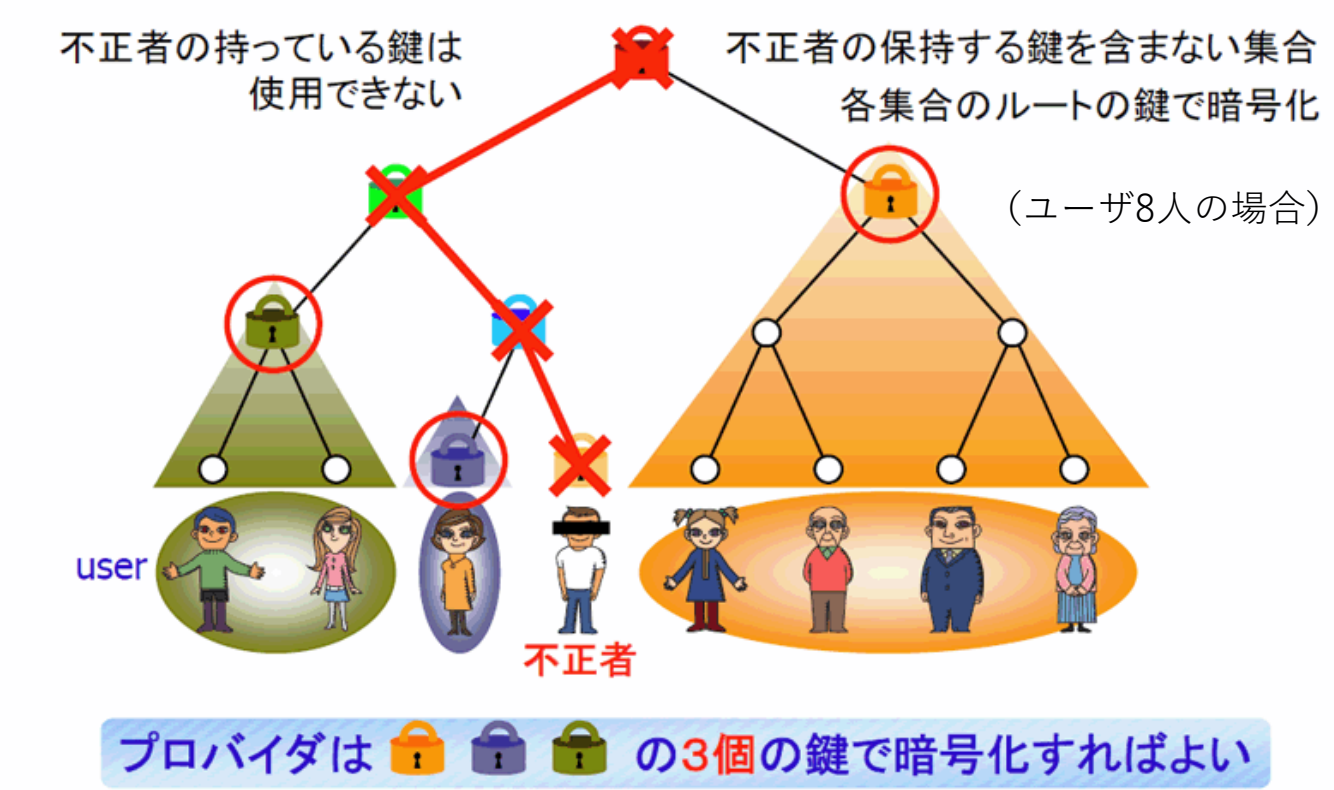


CS法　安全性（不正ユーザあり）

①不正者が所有するすべての鍵を削除する.

②不正者が持つ鍵を含まない集合の根にある鍵で暗号化を行う.

ユーザがn人,不正ユーザ1人の場合,
配信するものは（$\log_2 n$)個の鍵で
暗号化すればよい.
また不正ユーザが2人以上の場合は不正者を含む集合の位置により暗号化にかかる鍵の数が定まっていく

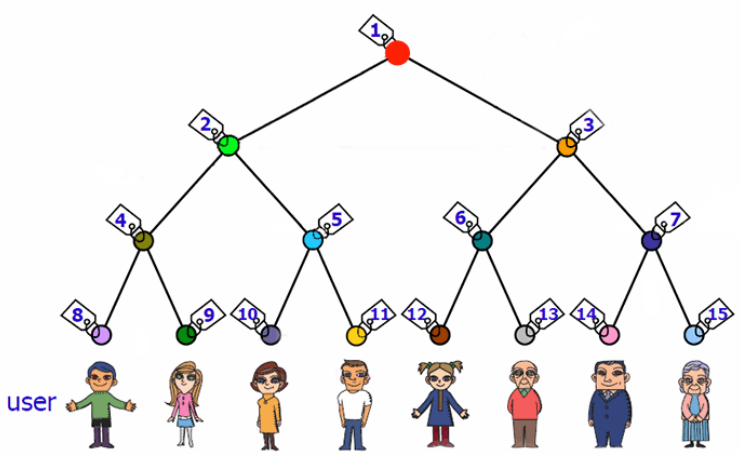


CS法と個別の暗号化の比較

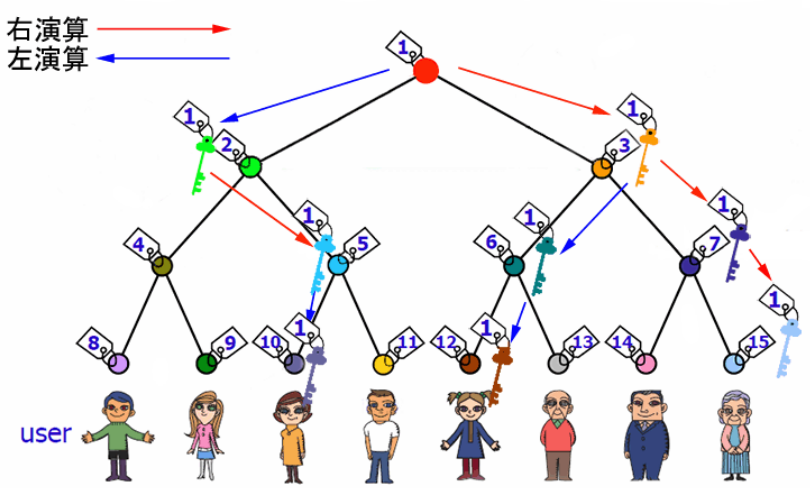
CS法は必要な暗号鍵の数を
不正者が含まれない集合の数
に削減でき，
かつ不正者は復号化できない

SD法　ツリー構造と鍵の配置

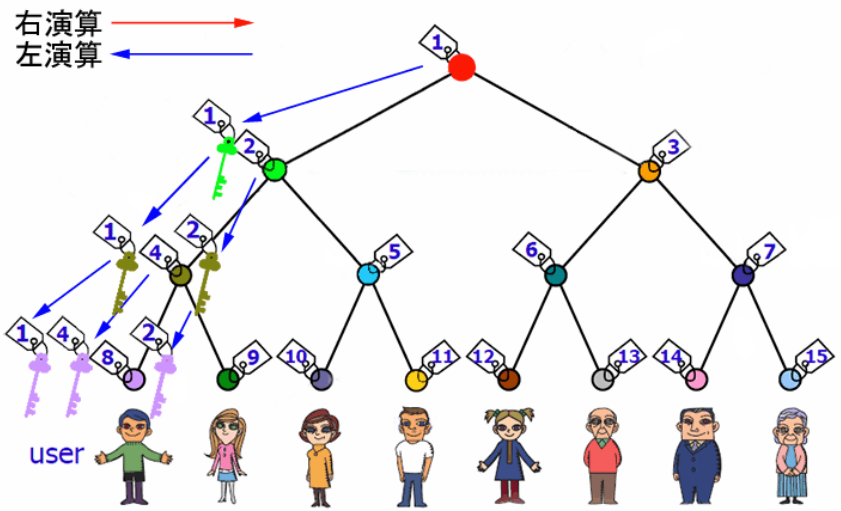
（ユーザ8人の場合）



①



②



③

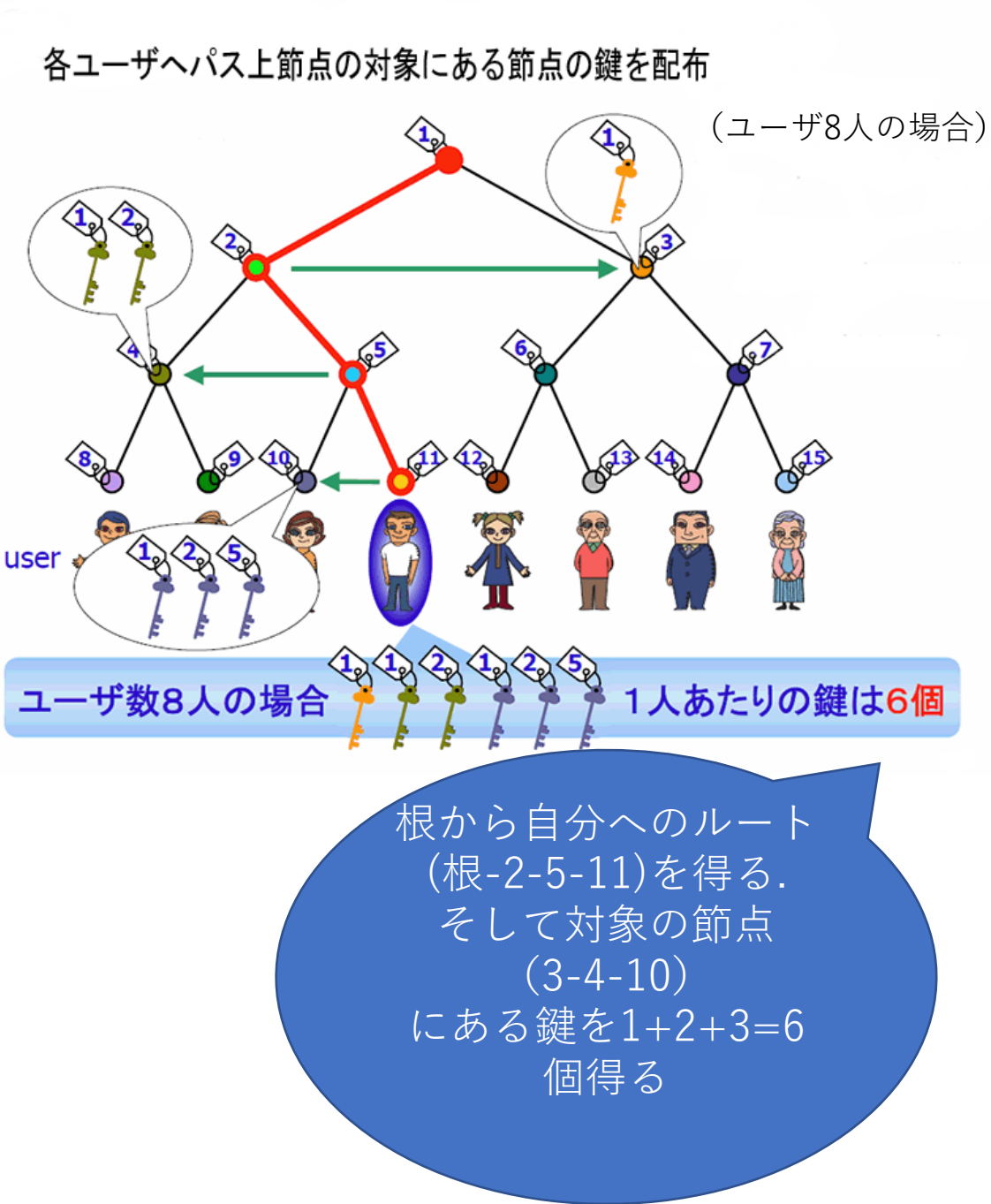
（ラベル1からとラベル2からの一部を記載）

①各接点にラベルを割り当てる.
②キー生成を上位ラベルから右演算と左演算を用いて生成する.
　この演算は葉まで一方向性ハッシュ関数を用いて行う.
③　②の操作を下位がいるラベルのすべてで行う
この結果, 深さkのノード（節点または葉）にはk個のキーが配置される.

SD法　鍵の配布

- まず, 二分木上でユーザから根までのパスを得る. その後, パス上節点の対象位置にある節点のキーをユーザに配布する.

ユーザが深さ n にいる場合,
$\sum_{i=1}^{n} i$　個のキーが配布される.



SD法　集合の定義

- まず「不正者集合」と「外側集合」について以下のように定義する.
- 「不正者集合」を不正者のみを含む集合と定義する.
- 「外側集合」を不正者集合を一つだけ含む一番大きい集合とする.

「不正者集合」
不正者のみを含む集合

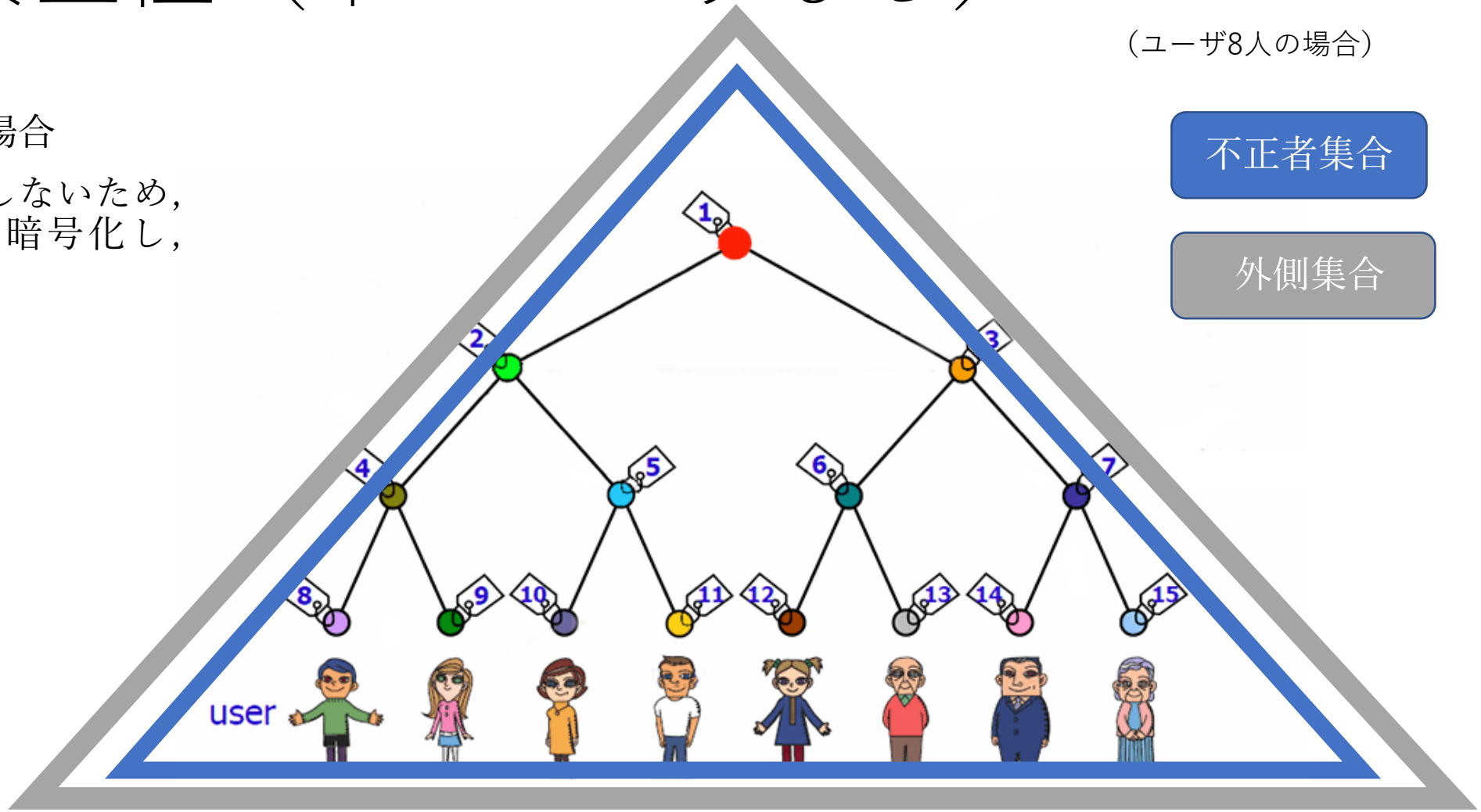
「外側集合」
不正者集合を一つだけ含む一番大きい集合

SD法　安全性（不正ユーザなし）

（ユーザ8人の場合）

- 不正者がいない場合

不正者集合が存在しないため，
全員の持つキーで暗号化し，
データを送る．



不正者集合

外側集合

SD法　安全性（不正ユーザあり）

（ユーザ8人の場合）

- 不正者がいた場合

まず不正者集合と外側集合を作成する.

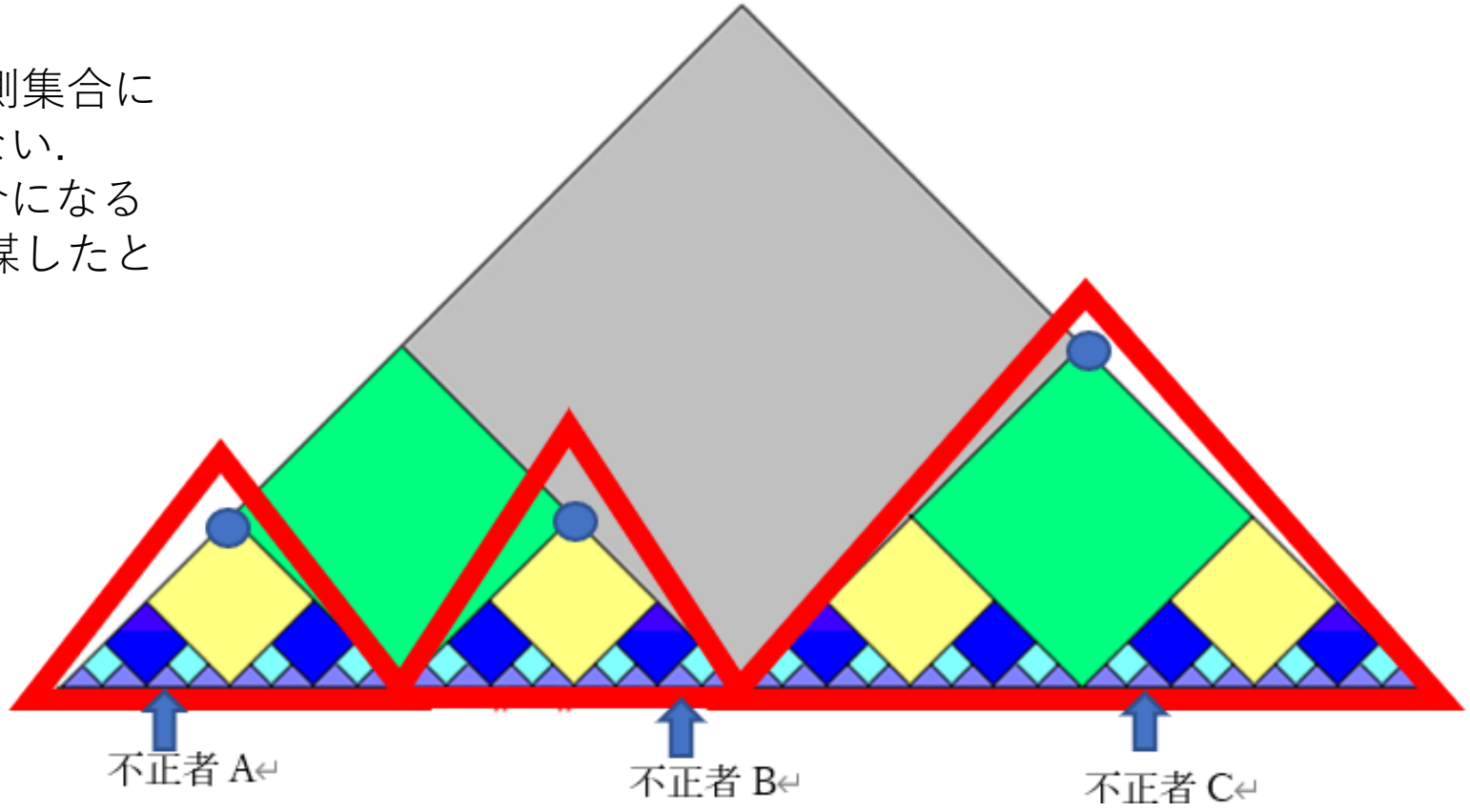
その後，外側集合の根のラベルから不正者集合の根のラベルへ作成した鍵で情報を暗号化する.

暗号に必要な鍵は不正者がいる場合、その分布で異なる

復号化する際は，親の鍵を知っていれば鍵を求めることができる.

SD法　復号化について（不正ユーザ複数の場合）

不正ユーザが複数いる場合,外側集合には不正者集合を一つしか含まない.
外側集合同士の和集合は空集合になることから,不正ユーザ同士が共謀したとしても安全性は担保される.



SD法とCS法の比較

SD法はCS法と比較して
暗号化の回数が少なくなる.
一方でユーザに配布する
キーの数は増加することが
わかる.

結論

理想は個別に暗号化して送信すること。
現実的でないので、CS法やSD法を用いる

CS法は暗号化の鍵が増える一方でユーザたちが所持する鍵の数が少ない

SD法は暗号化の鍵の数は多いもののユーザの所持する鍵の数が増える

静脈認証技術の現状と展望

FU Hao 暗号認証分科会
中央大学大学院

静脈認証技術とは

人体の皮膚下にある静脈形状パターンに基づく個人認証技術

特性

- **不可視性** 静脈は皮膚の下にあるもの
- **唯一無二** 本人しか持たない身体的特徴
- **安定性** 年齢変化と皮膚上の汚れの影響を受けず
- **非接触** 機器との接触必要なく、衛生面・心理的安心感が高い

利用現状

- 様々な分野で利用が広がっている
- 2020年11月に、60ヵ国の9400万人が使用中
- 認証機器の小型化と認識精度向上が進行中

銀行、オフィス、
住宅、政府機関…

本人拒否率： 0.0001%
1万人程度で認証可能

応用実例

みずほ銀行は2006年8月より、静脈認証を
二段階認証手法として、キャッシュカードの
偽造・盗難を防止できるサービスを提供

将来の可能な応用例

レジなし店舗

1. 商品を見つけ
2. バーコードをスキャン
3. 出口に静脈認証を行う
4. 設定された方法で決済
5. 買い物完了

富士通/ローソンレジなし実験店舗

https://pr.fujitsu.com/jp/news/2020/02/18-1.html

認証付き暗号について

森田 匡博

目次

- 認証付き暗号とは
- 認証付き暗号の仕組み
- 認証付き暗号の安全性

認証付き暗号とは①

メッセージの暗号化と認証を同時に行うことが可能な暗号技術のこと

活用事例

主に安全性を必要とするサービス全般(通信など)
OpenSSHでは6.1からAES-GCMのサポートを追加した

認証付き暗号とは②

メッセージの暗号化と認証を同時に行うことが可能な暗号技術のこと

暗号化

ある手順に従って、あるメッセージを元が分からないものに置き換える方法

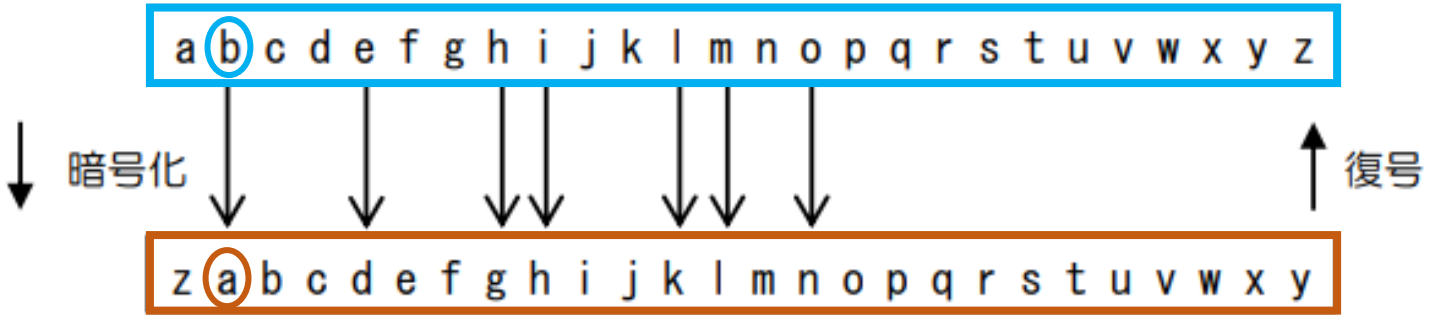
認証

貰った情報が正しいのかどうか、あるいは他者が成りすましていないかを検証すること

認証付き暗号の仕組み①

共通の決まりに従ってデータ(メッセージ)を別の物に変換する

例えば、「アルファベットを1文字ずらす」という決まりに従うと、変換の図は以下のようになる



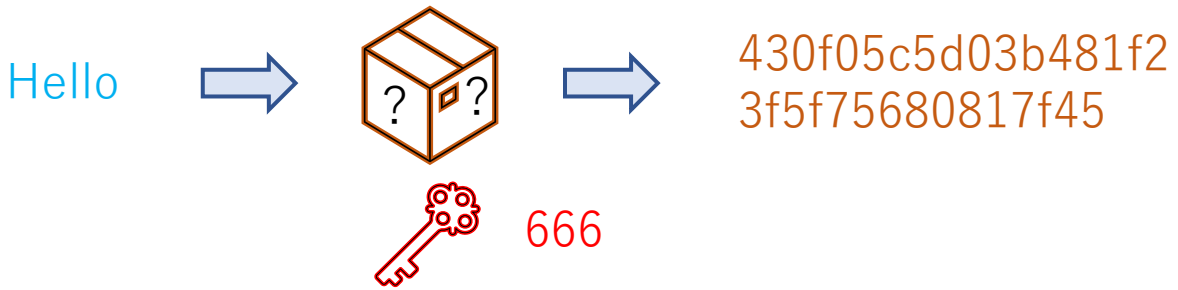
つまり、「b」を送る際は「a」に、「a」を受け取った際は「b」に変換される
よって「Hello World」という文字を送る場合、受信者は「Gdkkn Vnqkc」を受け取る
この場合、共通鍵は「1」となり、これを共通鍵暗号方式と呼ぶ

認証付き暗号の仕組み②

ハッシュ関数を用いてデータに対する固定長のコード(MAC)を求める

ハッシュ関数という、入力に対して適当な値が返ってくる関数を用いる

認証付き暗号に使用されるハッシュ関数の一例として、MD5を用いたものを下図に示す



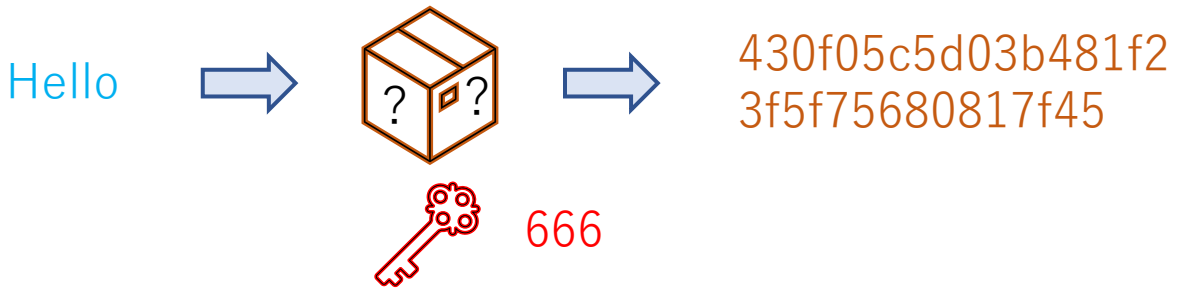
ここでは、「Hello」のコードを求める場合、鍵に「666」を用いて関数に入力すると、「430f05c5d03b481f23f5f75680817f45」が返ってくる

ハッシュ関数を用いて求めたコードをHMAC(Hash based Message Authentication Code)という

認証付き暗号の仕組み③

MACを元に、データ(メッセージ)の認証を行う

Aが送信したいデータ「Hello」とそのMAC 「430f05c5d03b481f23f5f75680817f45」をBに送り、Bがデータから同様の鍵でMACを計算する



同じく「Hello」のコードを求める場合、鍵に「666」を用いて関数に入力すると、「430f05c5d03b481f23f5f75680817f45」が得られ、受け取ったMACと一致しているのでデータの改ざんがないことが分かる

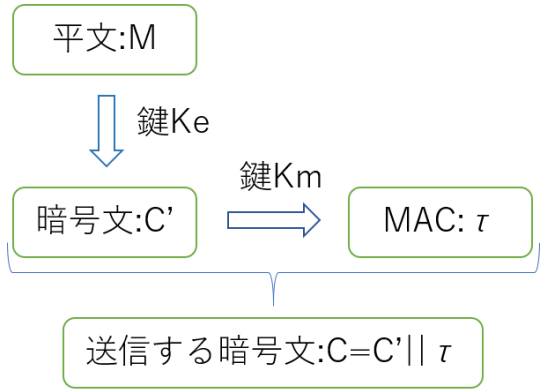
なので、この動作が認証の機能を果たしている

認証付き暗号の仕組み④

共通鍵暗号とMACの二つを組み合わせて、送信する

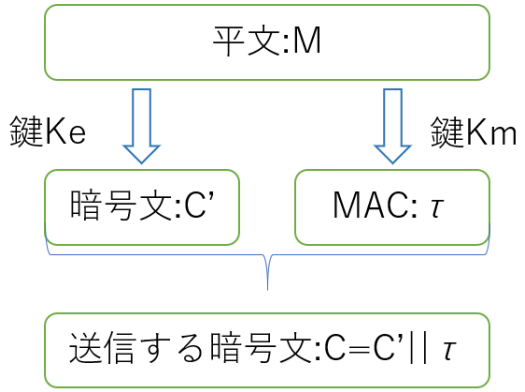
組み合わせ方として、以下の3通りの方法がある

・Encrypt-then-MAC(EtM)



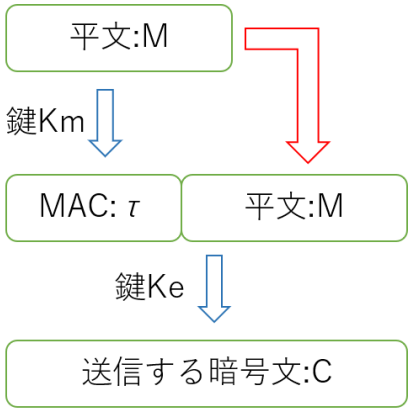
暗号化してからMAC

・Encrypt-and-MAC(E&M)



暗号化とMACを同時に

・MAC-then-Encrypt(MtE)

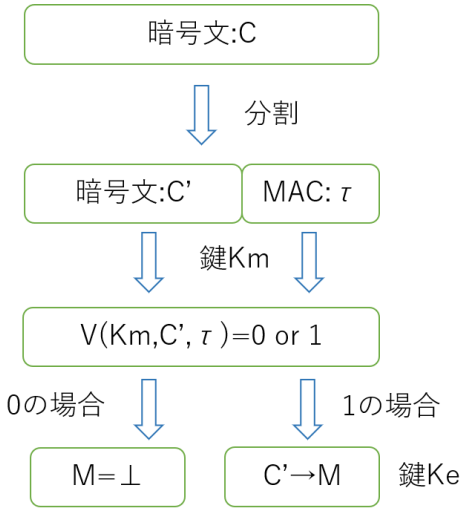


MAC求めてから暗号化

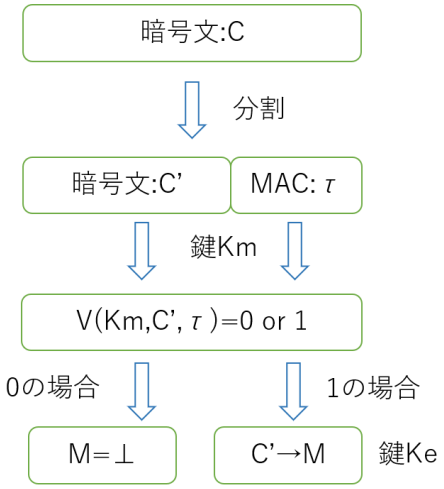
認証付き暗号の仕組み⑤

暗号文から各方法に応じてMACを求め、認証する

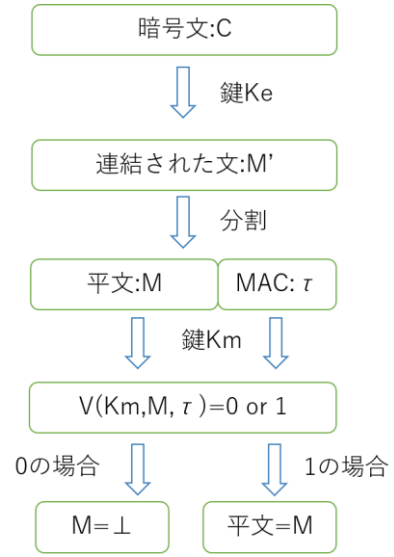
・Encrypt-then-MAC(EtM)



・Encrypt-and-MAC(E&M)



・MAC-then-Encrypt(MtE)



認証付き暗号の安全性①

・秘匿性と完全性を満たす
…暗号文から平文の情報を得られない安全性と任意の暗号文を生成することが困難であるという安全性

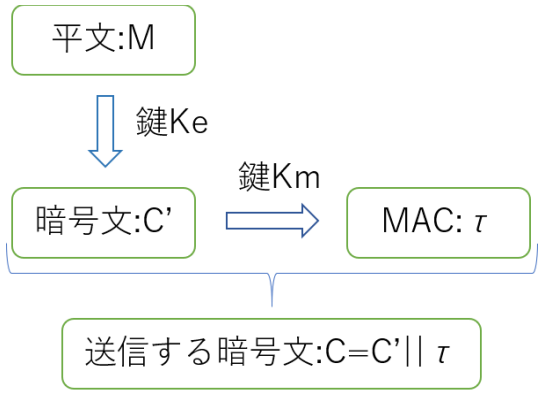
これらを満たすために、MACの生成に用いるアルゴリズムにも、新たなメッセージとMACのペアを見つけることが計算上不可能であることが必要条件になる

何故安全性を満たすのか

受信者が分割した文から計算したMACと送られた暗号文に付属していたMACを比較する
一致しない場合、復号されず平文の秘匿性と完全性の両方が満たされる

認証付き暗号の安全性②

・厳密に安全だと言えるのはEncrypt-then-MAC(EtM)方式のみである



何故安全性を満たすのか

暗号文Cを差し替えても、MACも合致するように差し替えないと一致せず認証が失敗するため秘匿性と完全性の両方が保たれる

ありがとうございました