本人限定情報開封機能の導入に向けて

第10回 社会情報流通基盤研究センター・シンポジウム

東京工業大学 科学技術創成研究院
未来産業技術研究所/社会情報流通基盤研究センター

小尾高史

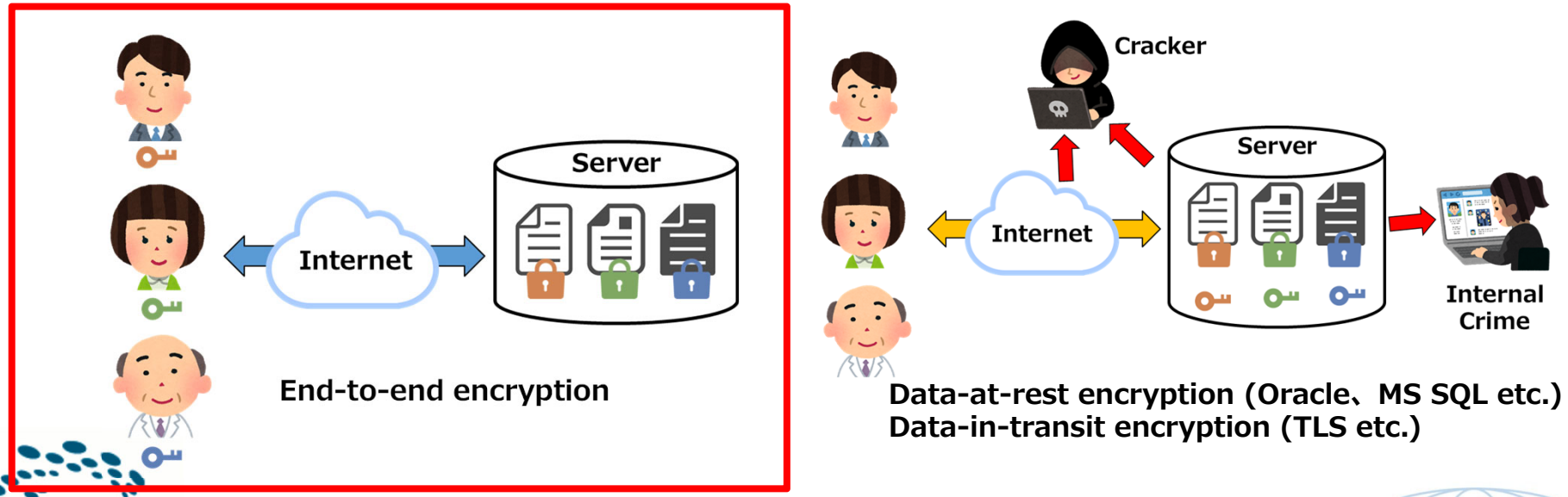
ウィズコロナに向けたセキュリティ対策

- NRI Secure Insight2020によると2020年に国内で発生した情報漏洩事故の第1位が、電子メール・FAX・郵便物等の誤送信、誤配送
- テレワークなど情報通信技術を活用した働き方が拡大しており、また、副業・兼業や雇用によらない働き方も更に広がる可能性があるため、情報の所在を問わないセキュリティ対策が必要
- ウィズコロナにおいて、人同士の接触状況、患者の行動に関する情報を収集することは感染の拡大回避に繋がる一方で、個人のプライバシーを侵害するおそれがあることから、安全な形で個人データを利用する仕組みの検討が必要

ニューノーマル時代に対応する
ゼロトラストモデル導入の推進

End-to-end encryption(E2EE)

- 利用者のみが鍵を持つことで、サービスの管理者、インターネットサービスプロバイダ、その他第三者が勝手にデータを復号することを防ぐ技術
- インターネットを経由して送受信しているデータを途中で傍受されたり、サーバに保存中のデータを盗まれても、復号できず、セキュリティとプライバシーを保護



保存データ利用時のE2EEと一般例の比較

次期公的個人認証サービス

- 現在のマイナンバーカードは発行開始から5年を経過
- 「デジタル社会の実現に向けた改革の基本方針 (令和２年 12 月 25 日閣議決定）」に、次期カード仕様の設計が検討課題として明記
- JPKIにおいては、暗号の危殆化への対応が必要
  - RSA2048bitの新規利用期間は2030年まで（NIST SP800-57）
  - 鍵長の拡大による処理時間増加を懸念

- 楕円曲線暗号への移行を検討
- 電子署名、利用者証明に加えて、
  第3の機能（電子文書の暗号化・復号）追加を検討

電子文書の暗号化・復号機能

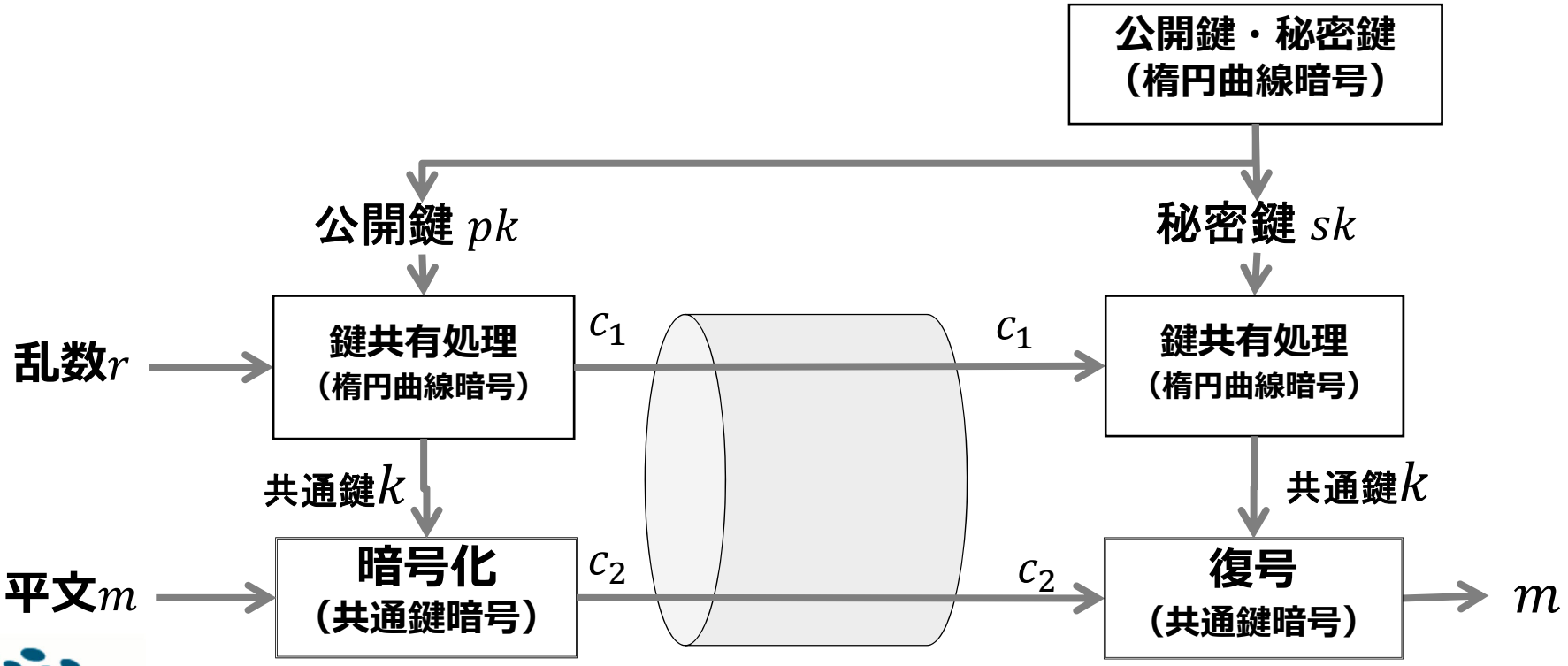
- 行政、医療等の分野の更なるデジタル化において、機微な個人情報を含む様々な情報のやり取りをオンライン化するニーズが増大
- 当該情報を安全・確実に、特定の相手方本人のみが開封することができる電子的手法（Digital Envelope using End-to-end encryption）
- 医療分野などに適した電子文書の暗号化・復号機能の仕組みを検討
- 単なる暗号化・復号ではなく、より多くのユースケースへ対応可能な仕組みを検討

エストニアでの利用例

- 罰金等の通知 (法執行機関から市民)
- 法執行機関のデータ交換
- 裁判所や犯罪捜査で必要な重要情報のやり取り
- 内部告発 (市民から法執行機関へ)
- 一時的な医療健康データの転送
- 契約書や金融取引明細などの送付
- 市民間の機密文書の交換
- システム管理者によるパスワードの転送

楕円曲線暗号による電子文書暗号化

- 電子文書の暗号化には通常ハイブリッド暗号を利用
- 楕円曲線暗号で共通鍵を共有し、電子文書をこの共通鍵を用いて暗号化



楕円曲線暗号の鍵

RSA暗号の鍵

公開鍵

暗号文 $C = M^{e} \bmod n$

平文

秘密鍵

$M = C^{d} \bmod n$

nのサイズ＝鍵長

楕円曲線暗号の鍵

（素数pで決められる素体の場合）

楕円曲線 $\mathrm{E}: \mathrm{y}^2 \equiv x^3 + ax + b \bmod p$

を満たす素体上の点（有理点）の数（位数）

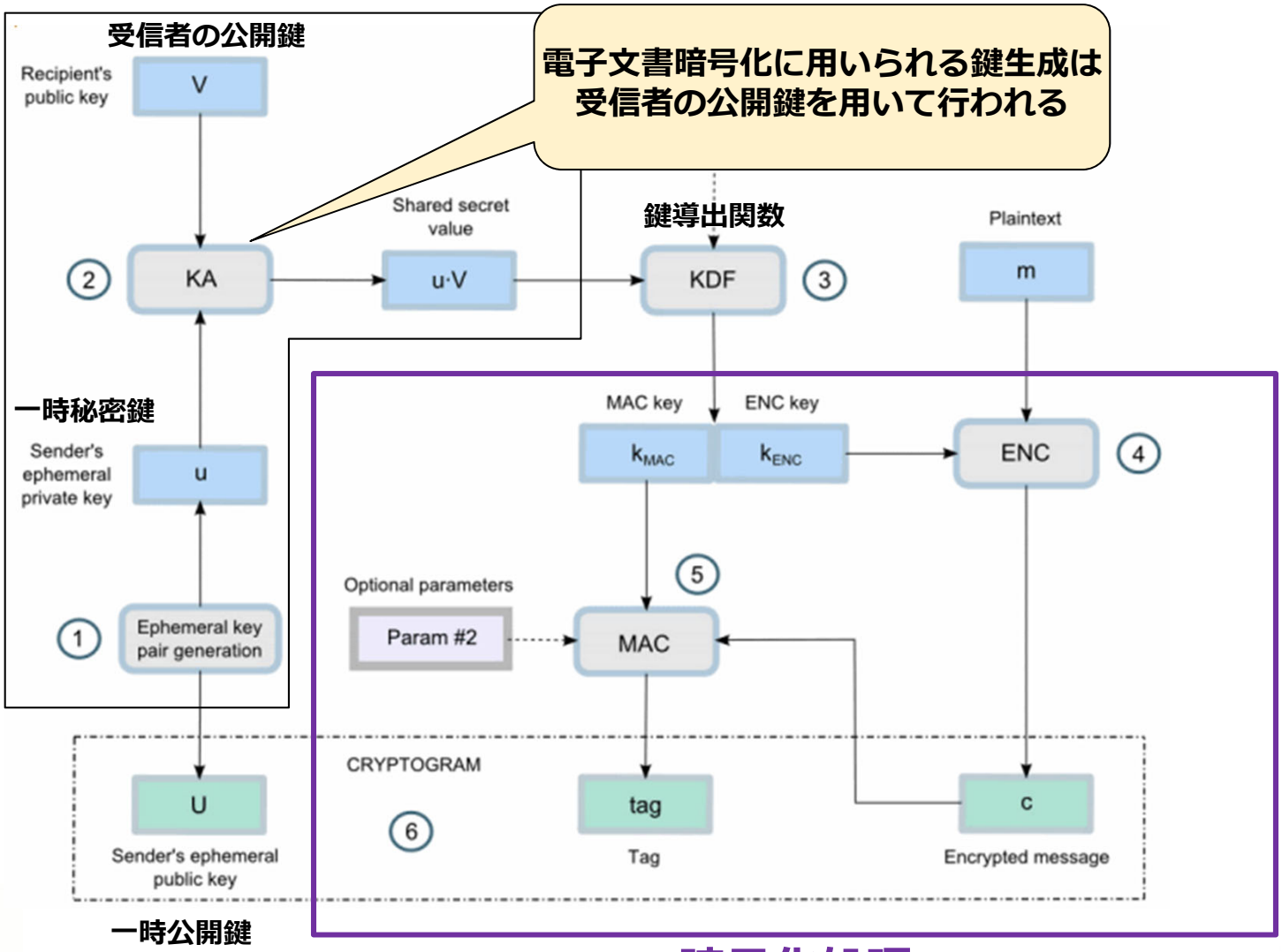
*#E*のサイズ=鍵長

秘密鍵 ： d　　公開鍵 ： $d*G$　G：基準点（楕円曲線上の点）

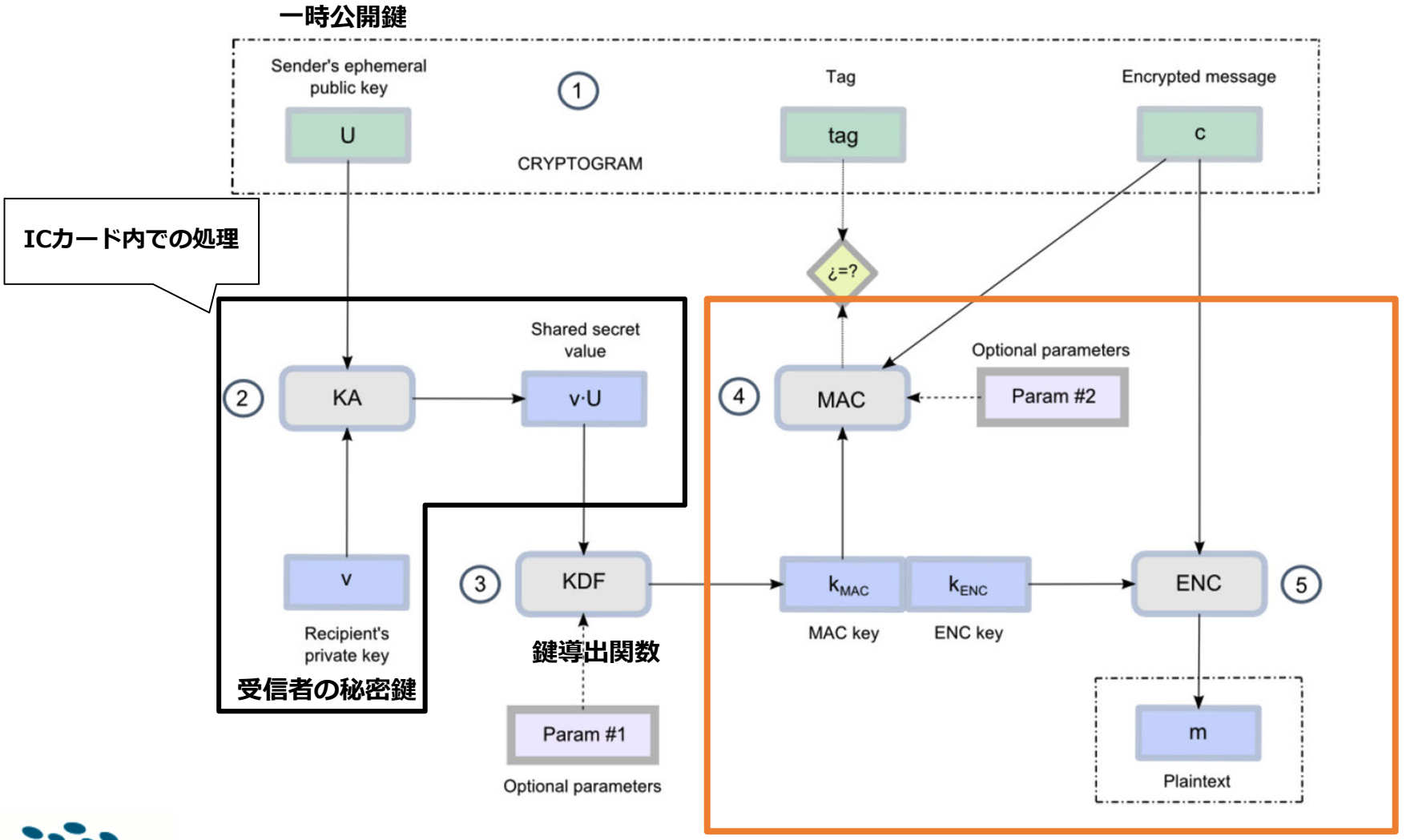
楕円曲線暗号によるハイブリッド暗号

- **共通鍵を共有する方法の候補**
  - ECIES-KEM
    - エストニアでの電子文書暗号化・復号に利用
    - 乱数と受信者の公開鍵を用いて共有鍵生成
    - 電子政府奨励暗号リストに含まれない
  - PSEC-KEM
    - 2001年NTTにより開発
    - 共有鍵は乱数から生成
    - 電子政府推奨候補暗号リストに含まれる

ECIES-KEM + DEM（暗号化処理）

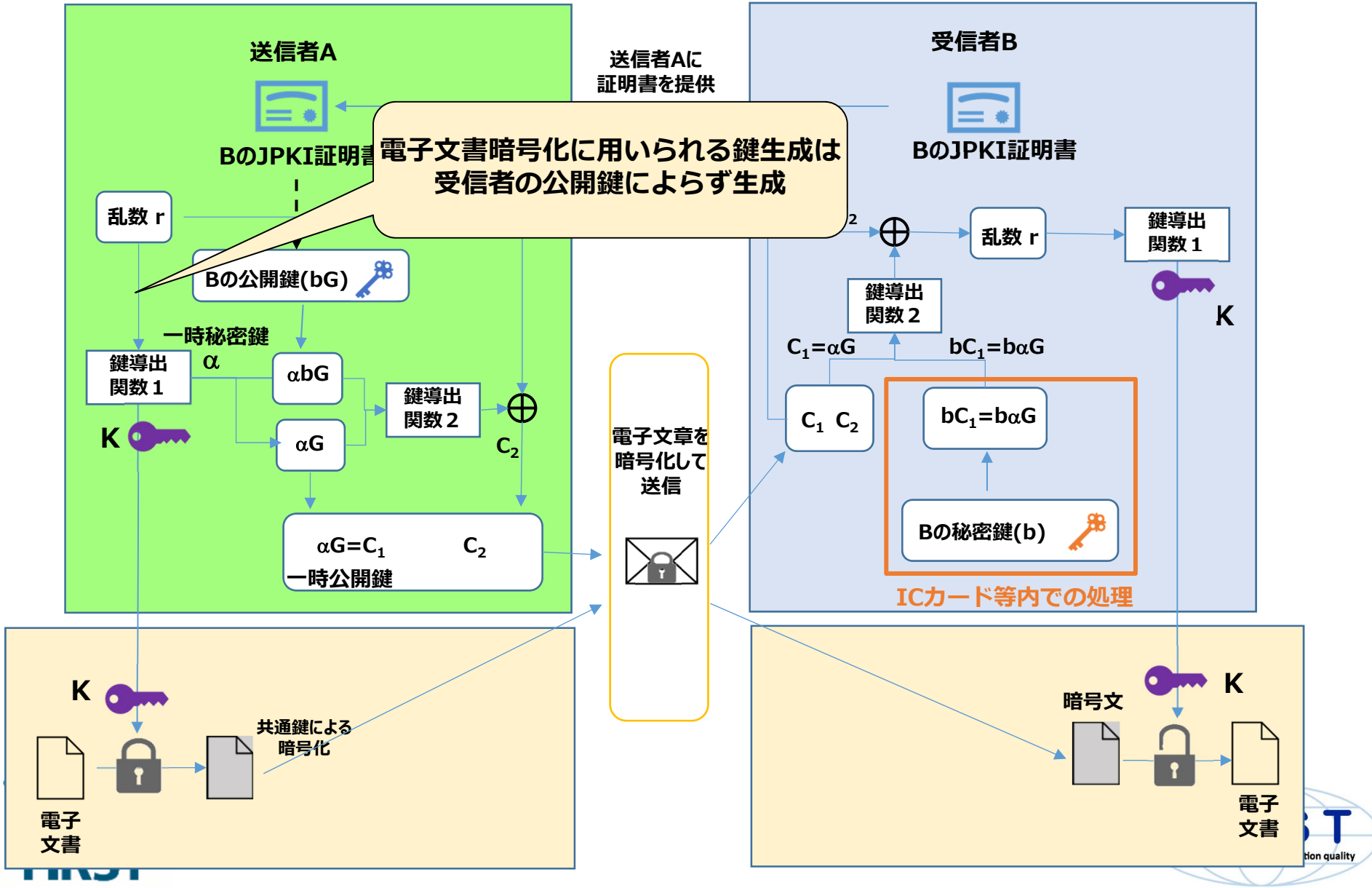


ECIES-KEM + DEM（復号処理）



復号処理

PSEC-KEMを利用したハイブリッド暗号



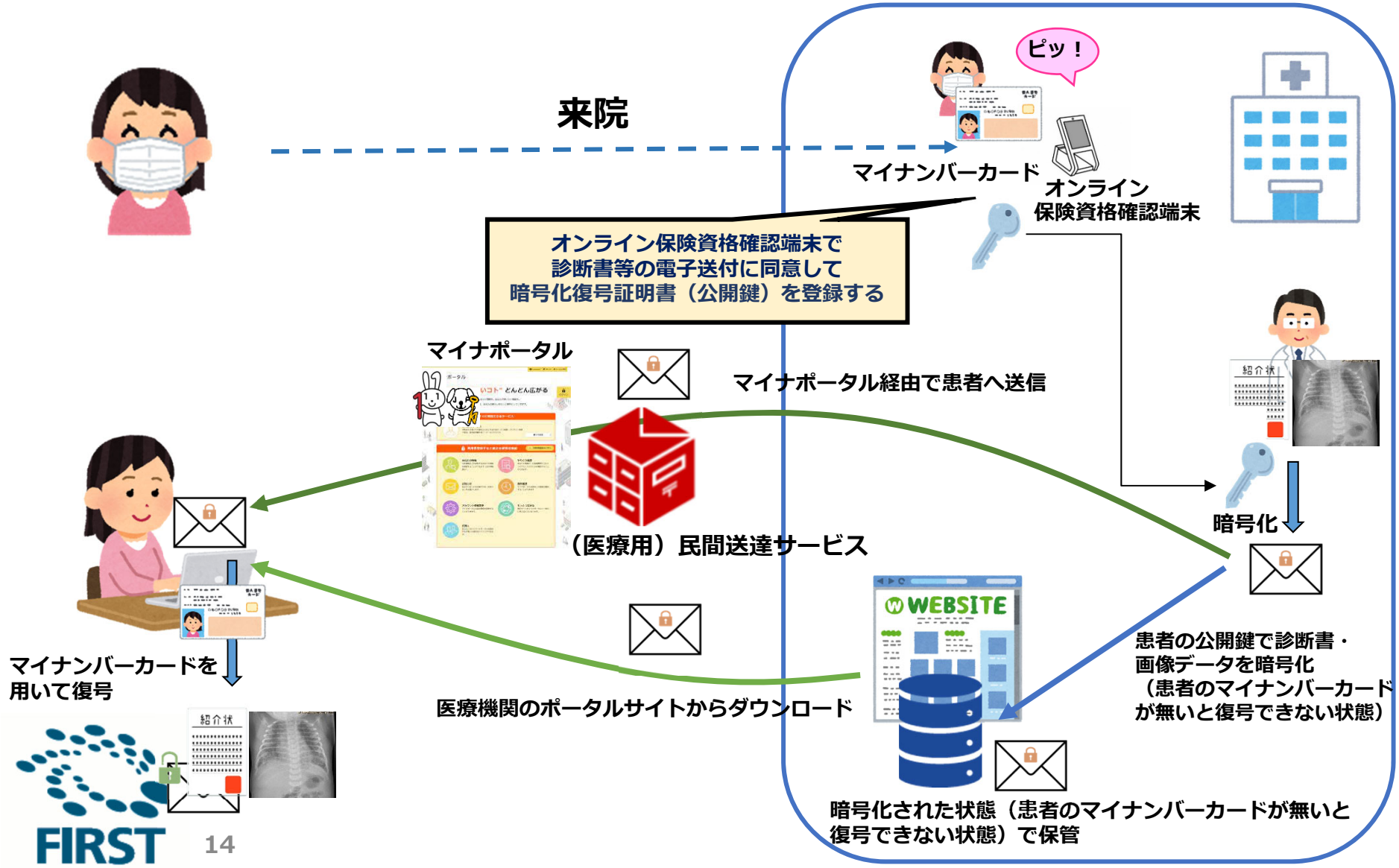
電子文書の暗号化方法

- エストニアでは、W3C XML-Encをベースとした CDOCと呼ばれる独自のファイルフォーマットを利用
- ファイルの暗号化自体は、AES-256-GCMを利用（TLSで一般的に利用される認証・暗号化手法）
- 一般的には、電子署名を付したファイルを暗号化するため、マルウエア対策等を別途考える必要がある
- One-Pass Key Establishmentを利用するため、Forward secrecy（前方秘匿性、秘密鍵が漏洩した場合過去にさかのぼってすべての暗号文が解読されない性質）の確保が困難

→　秘密鍵の管理は非常に重要

医療分野での利用例

医療機関から患者への診断書や画像データの安全な提供

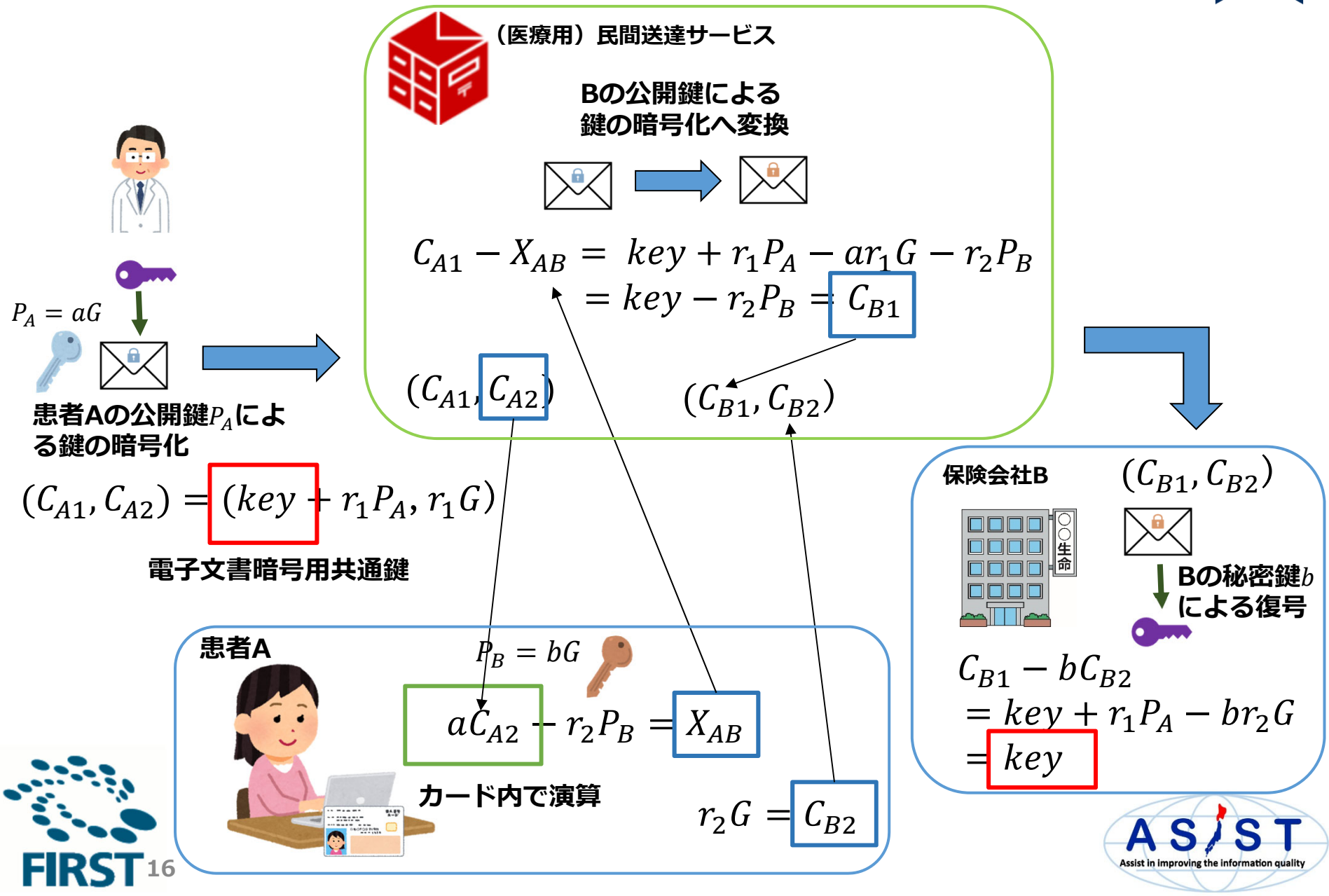


利便性向上に向けて

様々な利用に対応するための拡張機能を検討

- **代理人再暗号**
  - 暗号化された電子文書等を復号することなく再暗号化することで、データ漏洩等が発生した場合でも平文の漏洩を防止
- **秘匿検索**
  - 暗号化されたままの文書のキーワード等を検索できるようにすることで、受信者側の利便性を向上
- **秘密計算**
  - 医療データ等を暗号化したままで分析

代理人再暗号


（医療用）民間送達サービス
Bの公開鍵による
鍵の暗号化へ変換
$C_{A1} - X_{AB} = key + r_1 P_A - ar_1 G - r_2 P_B$
$= key - r_2 P_B = C_{B1}$
(C_{A1}, C_{A2})
(C_{B1}, C_{B2})
$P_A = aG$
患者Aの公開鍵P_Aによる鍵の暗号化
$(C_{A1}, C_{A2}) = (key + r_1 P_A, r_1 G)$
電子文書暗号用共通鍵
保険会社B
(C_{B1}, C_{B2})
Bの秘密鍵bによる復号
$C_{B1} - bC_{B2}$
$= key + r_1 P_A - br_2 G$
$= key$
患者A
$P_B = bG$
$aC_{A2} - r_2 P_B = X_{AB}$
カード内で演算
$r_2 G = C_{B2}$

秘匿検索

H_1は、$Keyword$からEへのハッシュ関数
h_2 は、有限体から整数へのハッシュ関数
e(,)は、ペアリング

$Keyword : w$

$Trapdoor(a, w) = aH_1(w)$

カード内で演算

検索（Trapdoorの送付）

（医療用）民間送達サービス

$PEKS(P_A, w) = (rG, h_2(e(H_1(w), rP_A)))$

キーワードw自体は分からない

$h_2(e(aH_1(w), rG)) = h_2(e(H_1(w), arG)) = h_2(e(H_1(w), rP_A))$

一致

$Keyword : w$

患者の公開鍵を用いてキーワードwを暗号化

$P_A = aG$

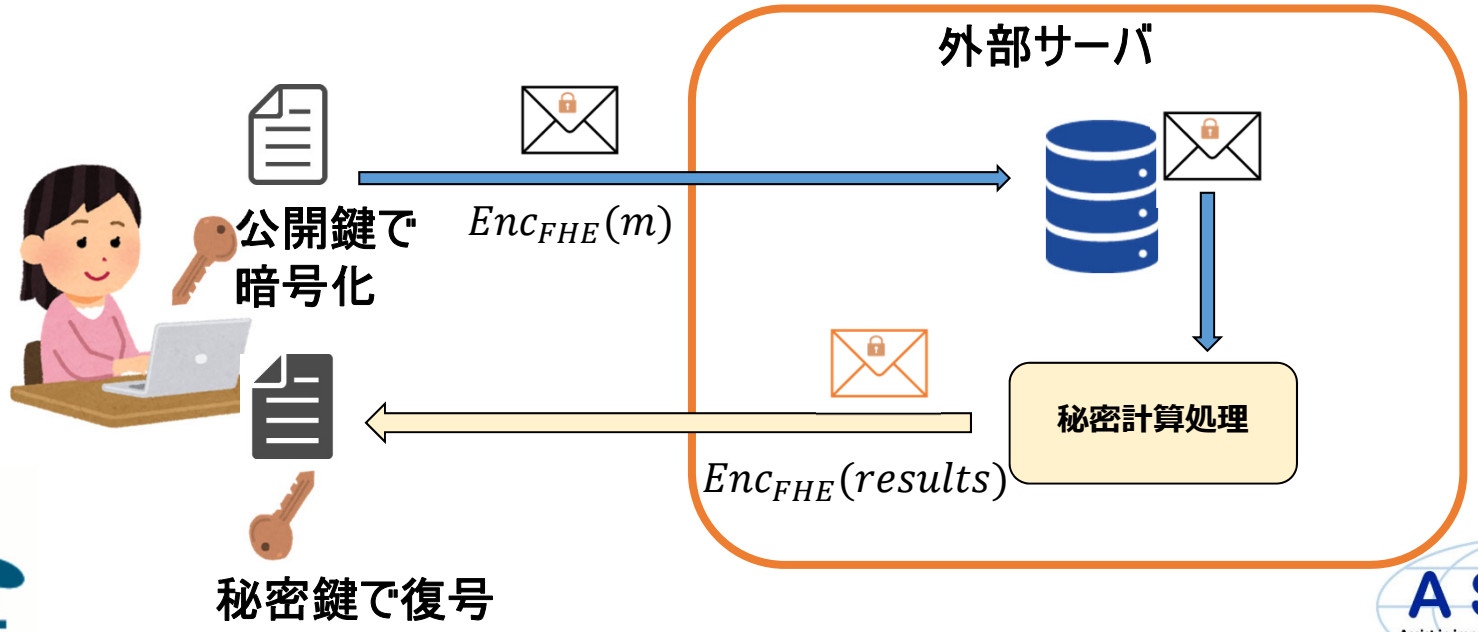
$PEKS(P_A, w) = (rG, h_2(e(H_1(w), rP_A)))$

乱数

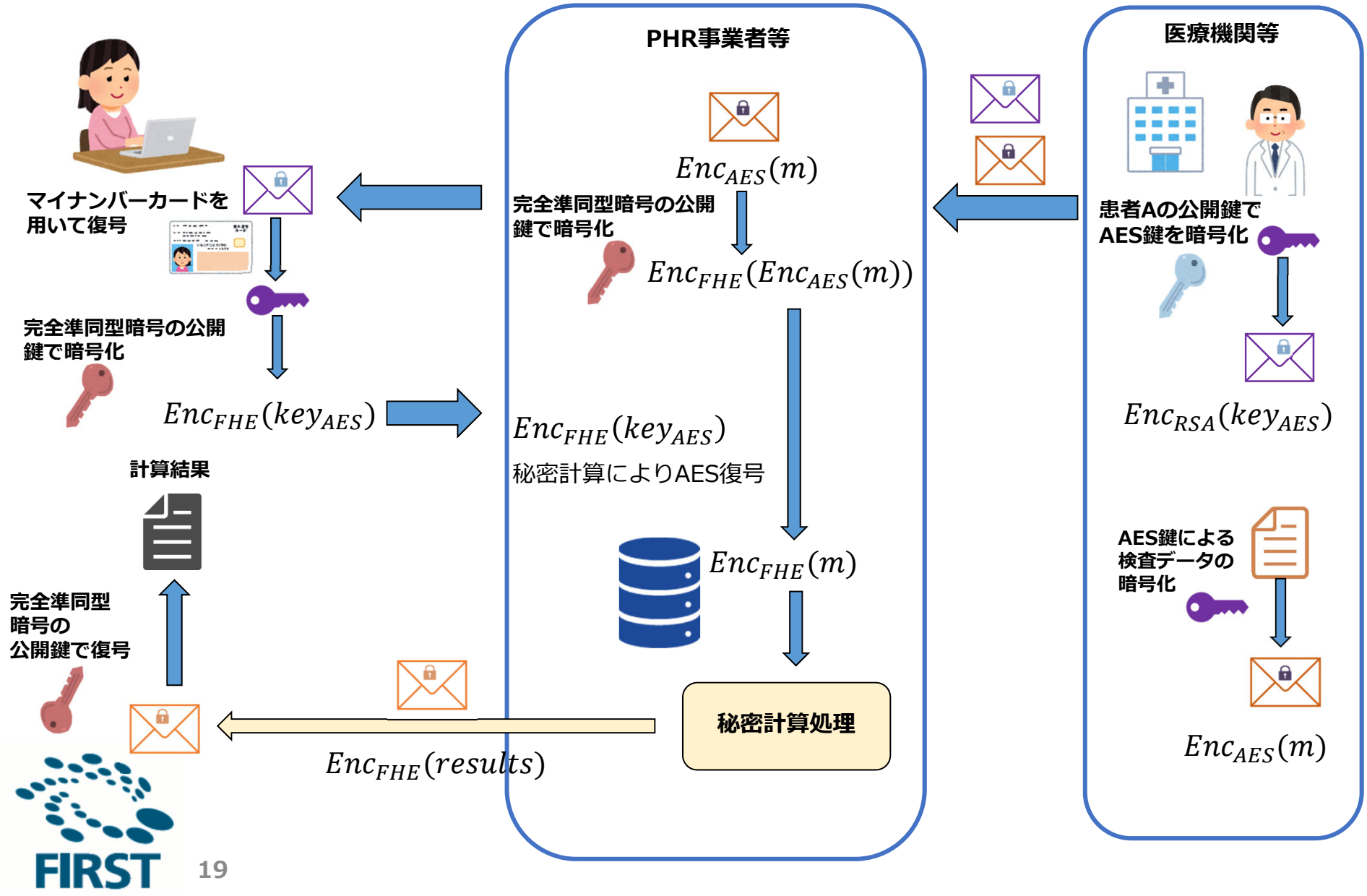
ペアリングを利用するため異なる楕円曲線が必要

秘密計算

- **秘密計算の代表的方法**
  - 秘密分散＋マルチパーティ計算
  - 完全準同型暗号(Fully Homomorphic Encryption, FHE)
    - 暗号化したまま、XOR、AND計算が可能 -> AESの復号可能
    - 機械学習への応用が可能



秘密計算


PHR事業者等
医療機関等
マイナンバーカードを
用いて復号
完全準同型暗号の公開
鍵で暗号化
$Enc_{FHE}(key_{AES})$
$Enc_{AES}(m)$
完全準同型暗号の公開
鍵で暗号化
$Enc_{FHE}(Enc_{AES}(m))$
$Enc_{FHE}(key_{AES})$
秘密計算によりAES復号
$Enc_{FHE}(m)$
秘密計算処理
$Enc_{FHE}(results)$
計算結果
完全準同型
暗号の
公開鍵で復号
患者Aの公開鍵で
AES鍵を暗号化
$Enc_{RSA}(key_{AES})$
AES鍵による
検査データの
暗号化
$Enc_{AES}(m)$

まとめ

- ポストコロナに向けたセキュリティ対策として、E2EEが重要になる
- 我が国における電子文書に対するE2EEの実現方法としては、JPKIの活用が有効と考える
- 同様の考え方は電子文章の交換だけでなく、様々な応用が考えられるため、特に医療分野での更なるユースケースの検討が望まれる

Tokyo Tech

Thank you