2025年度 新技術説明会

省力デバイス用“高速・軽負荷”非対称暗号アルゴリズムの開発

東京理科大学　工学部　情報工学科
准教授　藤沢 匡哉
助教　Ahmad A. Aminuddin

2025年11月11日

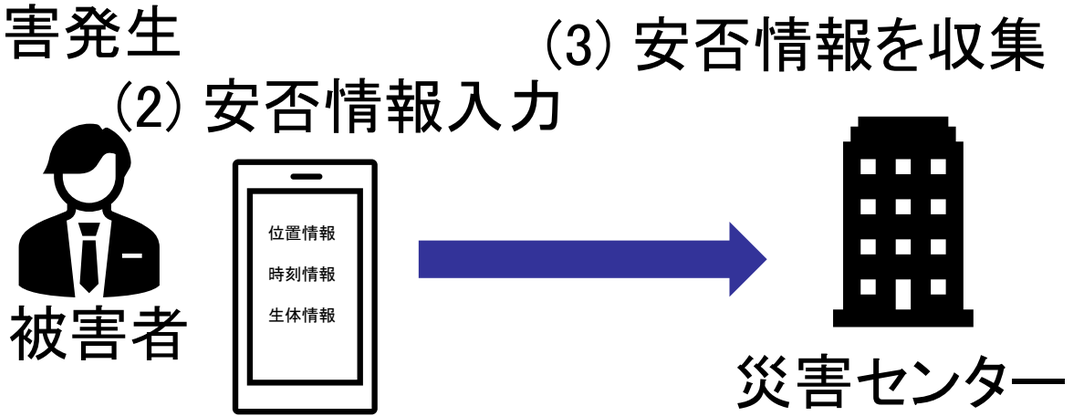
目次

研究背景：安全な情報共有

■ 通信技術の発展によって普及が進む，IoT機器や位置トラッカーなどの小型通信端末の登場により，データの収集・共有が簡単になる．

■ 例えば，携帯電話やスマートウォッチなどのIoT機器を用いて，

- □ 生体情報を計測
- □ 位置情報の確認
- □ 行動の遠隔モニタリング
- □ **災害時の安否情報送信**



■ IoTによる個人データの共有において，**通信の効率と機密情報の保護を両立できる仕組みが必要**

研究背景：小型デバイスに適する暗号方式

■ 災害時のような電源の確保が困難な応用では，徹底した省電力が必須

■ 計算資源・メモリやバッテリー容量などが小さい**非力なデバイス**において**消費電力を抑える**ために，

① 安全性 （確率的暗号）

② 暗号化処理負荷が小さい （低計算量）

③ 暗号文サイズが小さい （低通信量）

④消費電力が小さい

を満たす方式が望ましい．

■ これらの条件を満たすと，IoT小型デバイスにも効率的に利用できる．

従来技術 (1/2)

■ 安全な情報共有を実現する代表的な手法は以下の3つある:

表1　従来技術の比較

	公開鍵暗号	共通鍵暗号	秘密分散
目的	秘密情報を保護する		
計算量	高い	低い	**低い**
通信量	**低い**		高い
安全性	計算量的[1]		**情報理論的**

[1]計算量的:解読に必要となる計算量が，現実的な時間内に達成できない

高速計算，低通信負荷と高信頼性を
全て満たす方式はないのか?

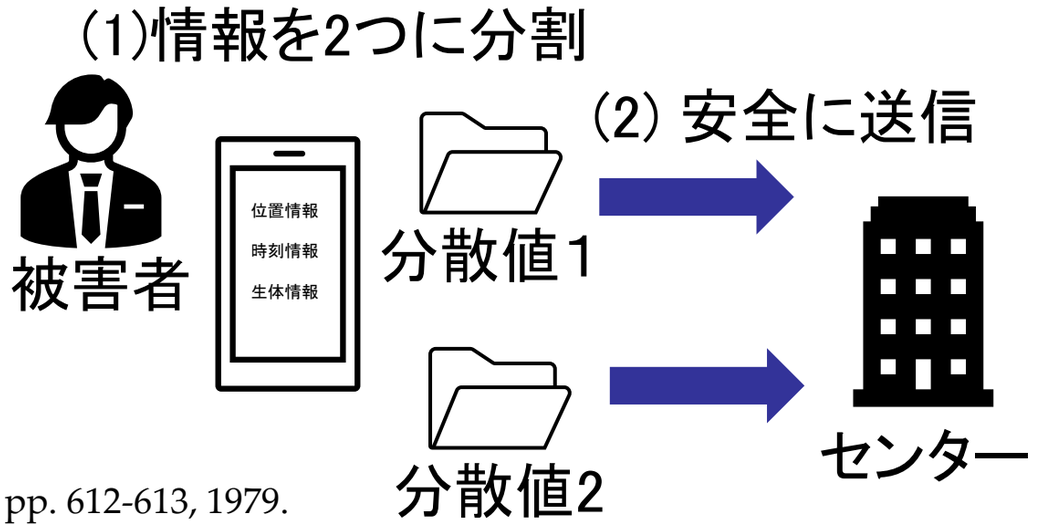
従来技術 (2/2)

(k, n)しきい値秘密分散

- 秘密情報 s を n 個の異なる値（以降，分散値）に変換し・保存する技術[1]
- n個の分散値のうち，
  - k 個集めれば，秘密情報を復元できる
  - k 未満の分散値より，秘密情報が漏洩しない

⇒ **情報理論的安全性**を実現する

- しかし，$k > 1$ にする必要なため，鍵暗号方式に比べて，通信量が**2倍以上**



[1] Adi Shamir, “How to share a secret,” *Communications of the ACM, vol.* 22, no. 11, pp. 612-613, 1979.

従来技術とその問題点

効率性（実用性）と安全性（信頼性）の同時実現が困難

- 共通鍵暗号は計算量が低いが，計算量的安全性を実現
- 鍵暗号を用いた手法は，一般に確定的暗号になる
  （確定的暗号：同じ平文に対して，同じ暗号文を出力）
  - 確率的暗号を実現するには，暗号化の計算量を増加する
- 秘密分散を用いた手法は，確率的な暗号文を生成できる
  - 最小2つの分散値を生成し，安全に送信する手段が必要
  - 送信する情報の量が増加する

新技術の特徴

■ 従来技術の問題点であった，以下を満たす暗号化方式の開発に成功した

① 確率的暗号の実現

② 暗号化処理負荷が小さい

③ 暗号文サイズが小さい

■ 本技術の適用により，暗号化の処理負荷は他の暗号方式と比較して1/10程度（公開鍵暗号に対して）である.

■ 暗号文サイズも最小限（送信情報に対して同サイズ）に抑えられる

■ 暗号化の影響による消費電力も1/10程度まで削減されることが期待される

従来技術との比較

表２　従来技術との比較

	A 提案技術	B 現行研究[2]	C ElGamal	D 楕円暗号	E AES暗号
方法	秘密分散	秘密分散	公開鍵暗号	公開鍵暗号	共通鍵暗号
安全性	◎	◎	○	○	○(◎)
計算量	◎ ※Bと同等	◎ ※計算時間ではCに対して1/10 ※演算回数ではDに対して1/8	△	○	◎
通信量	1倍	5倍	2倍	3倍	1倍(2倍)
消費電力	◎	○	○	○	◎

[2] Y. Kawahara, A. Kamal, M. Fujisawa, Lightweight Information-Sharing System with Access Control in Disaster Management with Security against Dishonest Users, Journal of Signal Processing, vol. 28, no. 4, pp. 161-164, 2024.

想定される用途

■ ドローンによるネットワークを利用した安否情報収集システム

ロ バッテリー容量の小さな情報発信小型端末への適用を想定

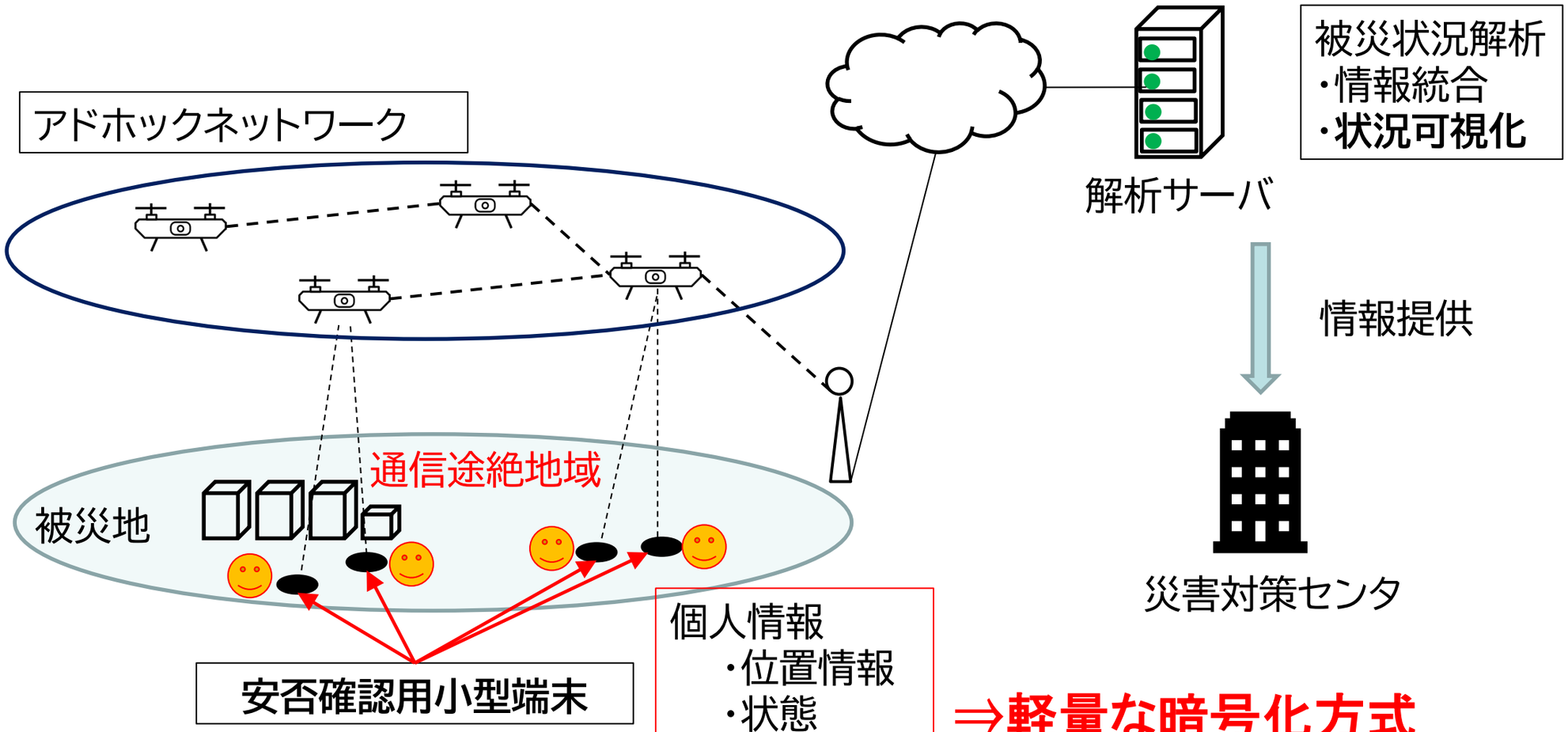
■ また，達成された省電力・暗号化処理の高速化に着目すると，

ロ IoT機器間の軽量・安全な通信

ロ自動車内外の部品間通信にも展開でき，

広く情報処理関連産業への応用が可能であると思われる．

災害時安否確認システム



⇒軽量な暗号化方式

安否確認システムにおける暗号化の必要性

- 無線傍受・ドローンの墜落等による
  個人情報の漏洩
- 安否情報の改ざんによる救助活動の混乱

暗号化による保護の必要性

- 墜落したドローンのメモリを解析 ⇒ ① 確率的暗号
- 小型情報送信デバイス（バッテリ容量小） ⇒ ④ 低消費電力
  - ・暗号化処理の消費電力を抑える ⇒ ② 低処理負荷
  - ・送信電力を抑える ⇒ ③ 暗号文サイズ小

実用化に向けた課題

- 現在，ソフトウェア実装によって暗号化の処理負荷を抑えることが可能であることは実証済み.
- しかし，ハードウェアに実装した際の暗号化における消費電力の評価についての検証が課題である.
- 実用化に向けて，**暗号化ハードウェアを試作して検証**を行い，小型デバイスに組み込んでデバイス**全体での評価**を行う予定である.

社会実装への道筋

時期	取り組む課題や明らかにしたい原理等	社会実装へ取り組みについて
基礎研究	• 暗号化処理の処理負荷の低減について計算機シミュレーションによる検証が完了	
現在	• ハードウェア実装による評価方法の検討（シミュレーションによる代替評価の検討） • 改ざん検知機能の追加	
2年後	• 暗号化処理のLSIチップの試作による消費電力の評価 • LSIチップ利用時におけるハードウェアセキュリティの評価	• ハードウェア実装による評価 • JSTのA-Step事業へ応募し研究資金獲得
3年後	• 安否確認用小型デバイスへの実装による総合的な性能評価、安定性試験の実施	• 評価基礎データの提供 • 試作品サンプル提供が実現
4年後	• 他のIoTデバイスへの展開	

企業への期待

- 「実用化に向けた課題」の解決に向けた共同研究・開発
- ハードウェア実装の技術を持つ，企業との共同研究を希望
  - 本技術を用いて，ハードウェア上の実装実験
  - ハードウェア実装による消費電力の評価と実用化
    HDLの自動生成技術による評価により克服できると考えている.
- 本技術の導入が有効と思われる企業
  - IoTセンサを利用したシステムを開発中の企業
  - 金融など，その他の分野への展開を考えている企業
  - 軽量で安全な暗号機能が必要なサービスを提供する企業

企業への貢献、PRポイント

- 本技術は軽負荷で暗号化処理が可能なため，情報を保護する必要のある様々な場面で企業に貢献できると考えている.
- 本技術の導入にあたり必要な追加実験を行うことで科学的な裏付けを行うことが可能.
- 本格導入にあたっての技術指導等

本技術に関する知的財産権

発明の名称	:	プライバシー保護情報共有技術
出願番号	:	特願2024-149868
出願人	:	東京理科大学
発明者	:	Ahmad A. Aminuddin
		藤沢 匡哉

産学連携の経歴

・2021年　―　有限会社ケー・ピー・ディー社と共同研究実施

・2021年　―　城東地域活性化推進協議会に参画

・2024年　―　本学マルチハザード都市防災研究拠点に参画

お問い合わせ先

東京理科大学
産学連携機構

ＴＥＬ　０３－５２２８－７４４０
e-mail shinsei_kenkyu@admin.tus.ac.jp