通信・情報処理

非力なデバイスで利用可能な軽量非対称暗号方式

Lightweight asymmetric cryptography for devices with poor computational power

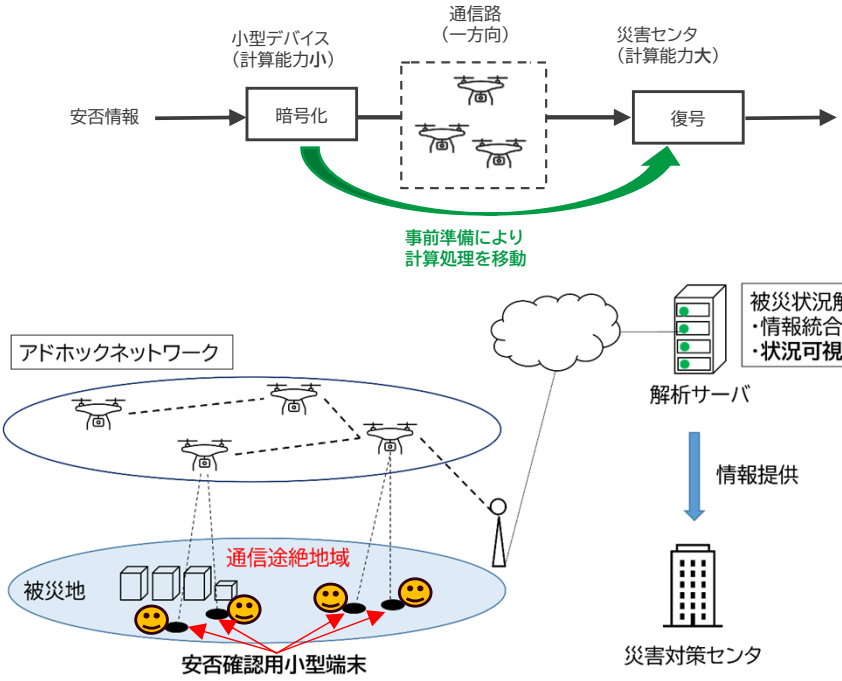
藤沢　匡哉 Masaya FUJISAWA　東京理科大学　工学部　情報工学科　准教授

研究目的

送信側と受信側における暗号処理の負荷を事前処理によって受信側へ移動する（送信側の暗号化処理と受信側の復号処理が非対称となる）ことによって、安全性を保ったままで送信側の暗号化処理の軽量化と送信する暗号文の長さを抑えた暗号方式となります。従来の効率的な暗号方式の暗号化の処理時間に対して、1/10程度の高速化が期待でき、計算能力の低いデバイスへの適応を目指しています。

研究概要

災害時に通信基地局が使えなくなった際に、ドローンによってアドホックネットワークを構築して安否情報を収集するシステムでの利用を考えています。ドローンが落ちたときに情報を盗みとられて解析されても、個人情報が漏れないようにする必要があります。さらに、送信デバイスの計算能力が限られるような状況での利用が想定されるようなIoT機器にも展開ができます。



従来・競合との比較

・従来の暗号方式と比較して、暗号化処理の軽量化に成功
・送信暗号文のサイズを抑えることに成功

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への適用
・IoT機器にも展開ができ、広く情報処理関連産業への応用が可能

実用化に向けた課題

・暗号化における消費電力の評価についての検証が残っています。
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ます。

企業へ期待すること

共同研究等で社会実装の可能性を探りたい。

POINT

・本技術により安全な情報収集が可能
・実装時の容易性も特徴
・広く情報処理関連の産業への応用が可能

今後の展開

2025.12　消費電力の検証を実施
2026.3　システム実装による評価を実施
2026.12　他方面への展開

■関連制度　：A-STEP 産学共同ステージI
■受賞歴　：なし
■試作品　：評価用プログラムはあり
■サンプル　：可能

2025.07

東京理科大学 産学連携機構
〒162-8601 東京都新宿区神楽坂一丁目3番地
TEL:03-5228-7440　E-MAIL:ura@admin.tus.ac.jp