

松浦研究室

暗号と情報セキュリティ

情報・エレクトロニクス系部門



情報理工学系研究科 電子情報学専攻

情報セキュリティ

<http://kmlab.iis.u-tokyo.ac.jp/>

誰もが不安なく情報をやり取りできる社会システム構築への技術的貢献を目標とし、暗号技術、情報セキュリティ、ネットワークプロトコルといった基盤技術、その技術革新、実用時の問題などの研究に取り組んでいます。

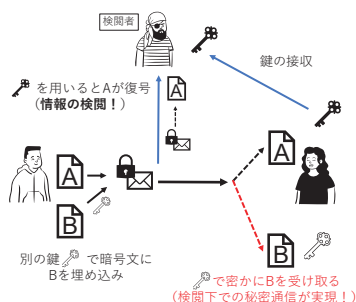
厳しい検閲下でも秘密を守る - アナモルフィック暗号の安全性検証・開発 -

暗号化通信において鍵が強制的に接收されると、機密情報が検閲される恐れがあります。

これを回避するため、**アナモルフィック暗号**が提案されています。

通常の暗号文に別の秘密のメッセージを密かに埋め込み、検閲者に存在を気づかせないようにする技術です。

現在のアナモルフィック暗号の安全性は、「通常の暗号文と区別がつかない」と定義されます。



安全性の検証

現在の安全性が、現実の攻撃を十分に考慮できているかを検証することは、真に安全な暗号技術を実現するために必要不可欠です。

高効率な方式の開発

アナモルフィック暗号を少ない通信量で実現する実用的な方式の開発は、社会実装に重要です。

アナモルフィック暗号の安全性を検証し、さらに安全で効率的なアナモルフィック暗号の設計に向けて研究に取り組んでいます。

$$r^* \stackrel{\$}{\leftarrow} \mathcal{R}$$

$$(c_K^*, K^*) \leftarrow \text{Ecp}(f_{pk_1}; r^*)$$

$$F_K(c_K^*)$$

$$\Pi?$$

$$c[1]c[2] \dots c[\ell] = (C_K, C_D)$$

