平成15年度未踏ソフトウェア創造事業

放送型配信における鍵漏洩抑止スキームの拡張

～一対多の公開鍵型暗号方式～

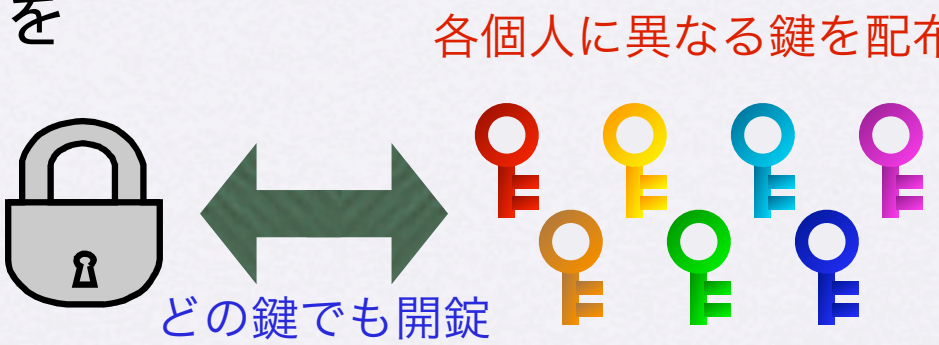
渡辺秀行
光成滋生
高島研也
石田　計

紀信邦PM

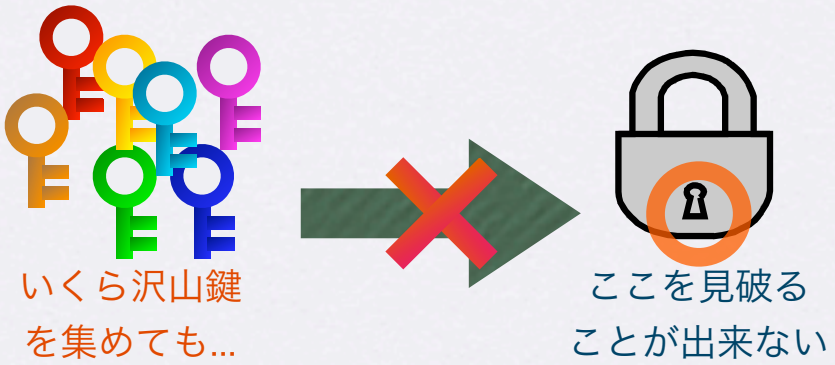
本方式の特長

本方式は、従来の暗号方式とは異なり、以下のような特長を備えています。

- 配信者は一つの暗号化鍵に対応する復号鍵を複数作成できる

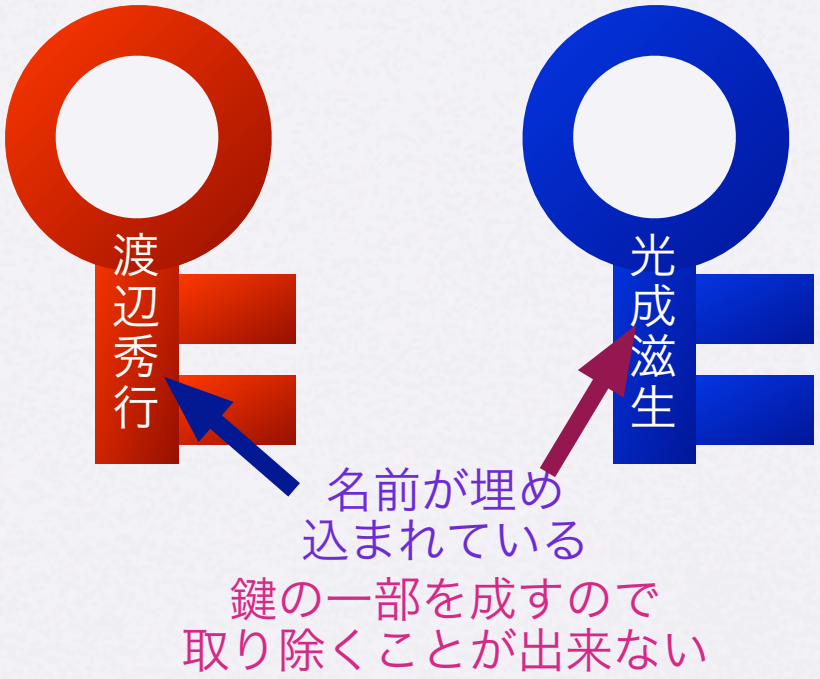


- 受信者は複数の復号鍵から暗号化鍵を見破ることができない
  （ＲＳＡ暗号と同程度）



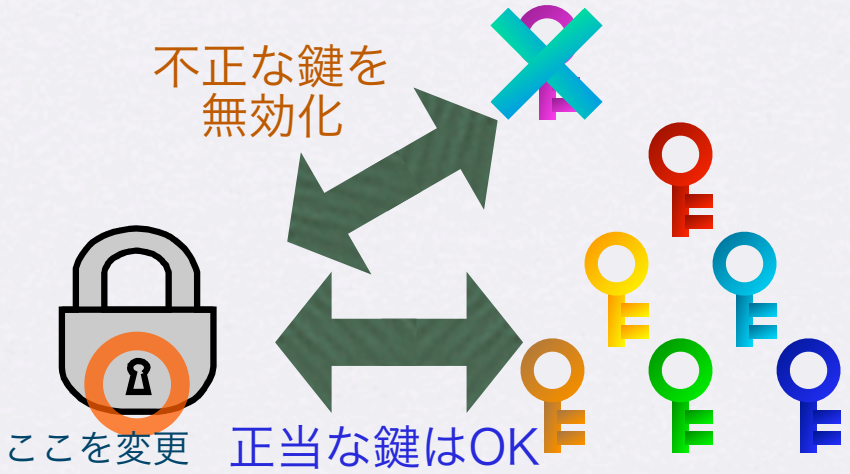
- 配信者は任意の数値（約160ビット）を含む復号鍵を作成できる

※ 復号鍵にユーザ情報を埋め込むことが可能



- 配信者は特定の受信者の鍵を無効化可能（上限あり・鍵サイズは上限に比例）

※ 不正な鍵の無効化



本年度の成果

本年度は、昨年度の成果に基づき、以下のような成果を収めました。

- 加入者排除機能を実装し、特定の受信者の鍵を無効化できるようにした。
- 上位演算部分を抽象化して下位演算部分と分離し、パラメータ依存をなくしてパラメータを隠蔽しやすくした。
- クラスの構造を変更し、メモリの使用方法の効率化を図った。
- パラメータ生成支援プログラムを作成した。
- リコンフィギュアラブルプロセッサDAP/DNA上で多倍長加算を実装し、本実装のハードウェア化の可能性を評価した。