有料配信における海賊版受信機パスワード漏洩抑止スキーム

渡辺秀行、光成滋生、藤井寛、石田計、酒居敬一

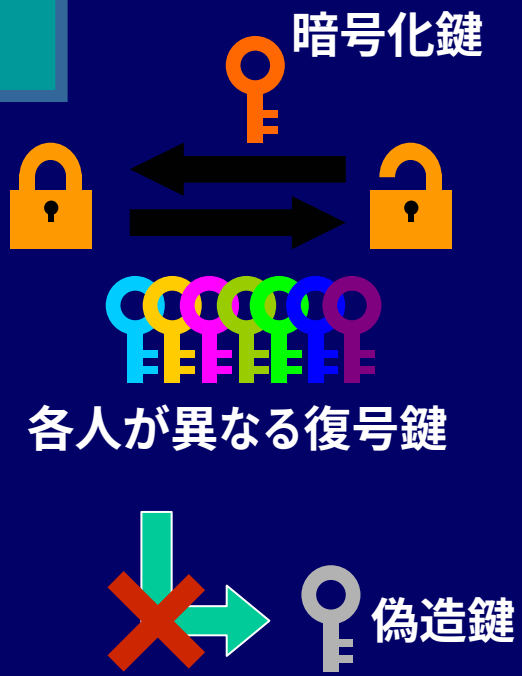
目標

- 放送型配信において不正受信装置の作成を防ぐことを目的とした暗号方式の実装
- 上記実装における各要素技術について問題点を調査･評価し、克服すること
- 上記実装における各機能の高速実装

成果

- 暗号方式の実装を完了
- 問題点の調査の完了、回避方法案の提示(未実装)
- これまで最高の速度を持つとされているライブラリの速度を15%から30%上まわる速度の達成

方式のイメージ



- 暗号化鍵(橙色)は公開
- 復号鍵(様々な色)は受信者の秘密
- 受信者が結託して偽造鍵(灰色)を作るのは不可能
- 従って漏洩した鍵から個人が特定される