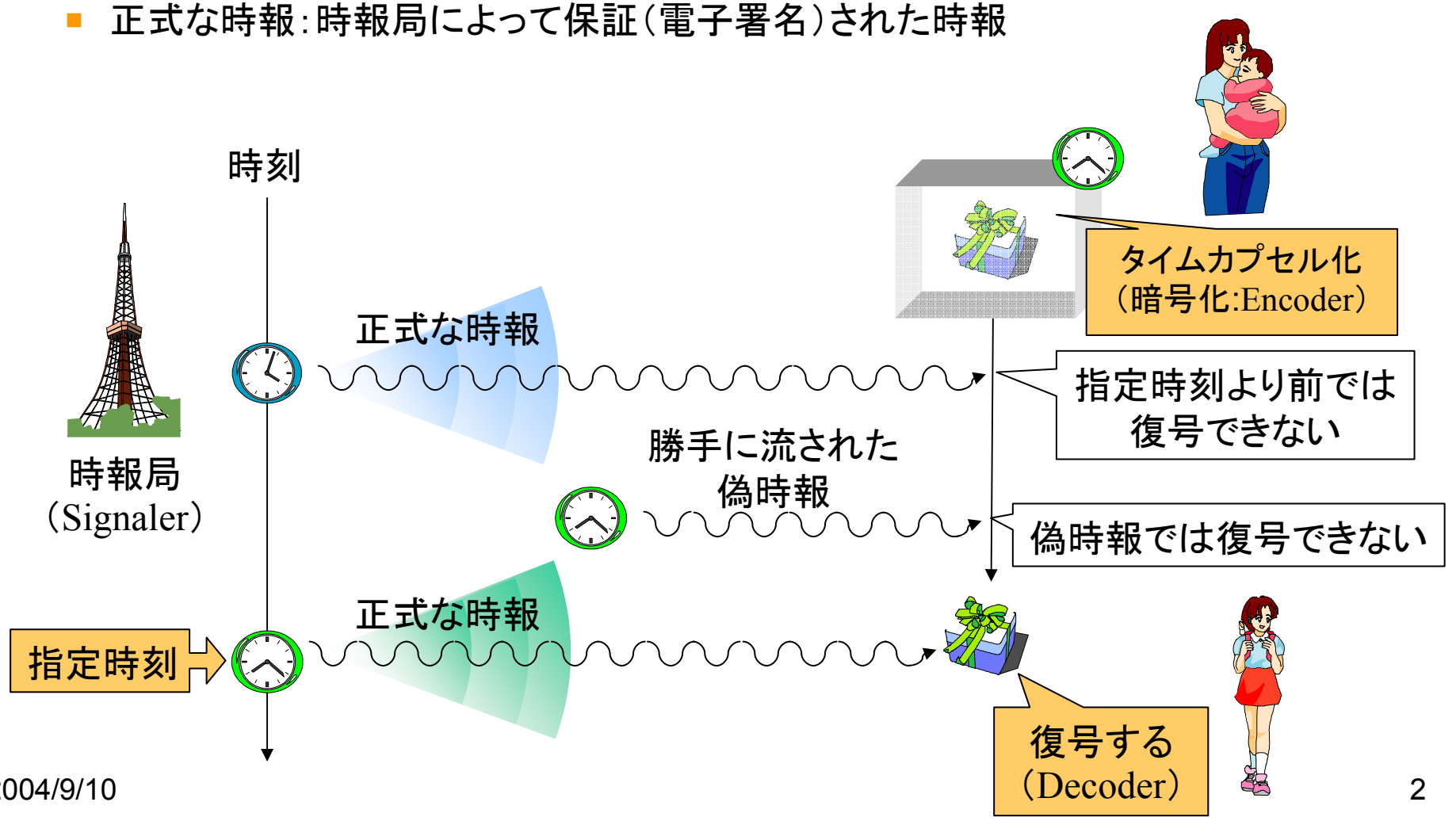
タイムカプセル暗号とその実装

吉田真紀，光成滋生

タイムカプセル暗号

- タイムカプセルは指定時刻の正式な時報を受けて復号される
  - 正式な時報：時報局によって保証（電子署名）された時報



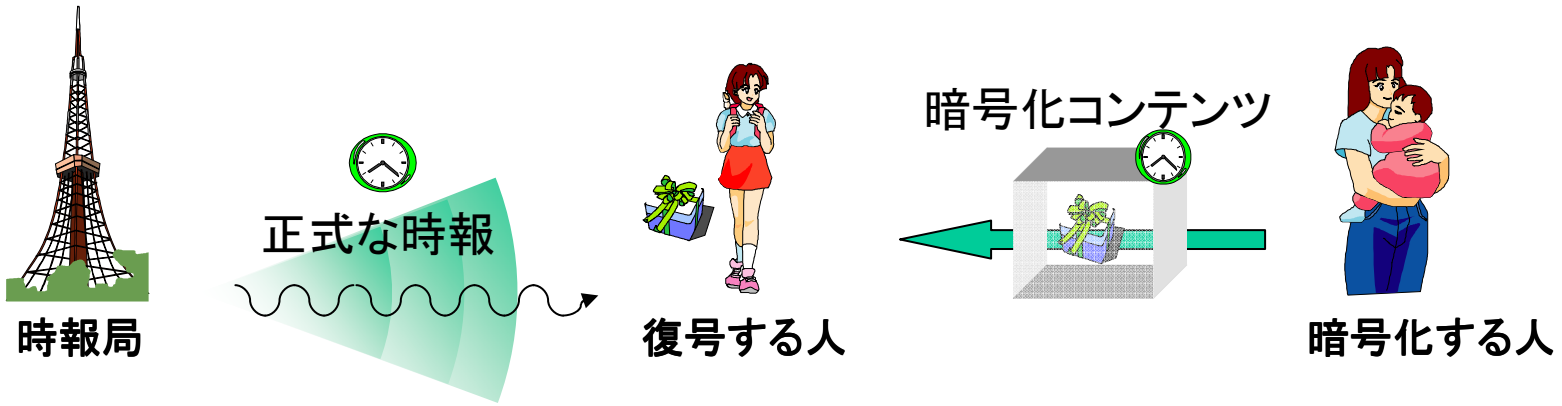
タイムカプセル暗号の特長

- 時報局（Signaler）
  - 電子署名データ確認用の鍵（検証鍵）をあらかじめ公開
  - 時報に電子署名データをつけて放送
- 暗号化する人（Encoder）：複数可
  - 指定時刻を選び、乱数（暗号化鍵）を生成して暗号化
    - 暗号化鍵は誰にも知らせる必要はなく、破棄可能
    - 誰でも自由に指定時刻や暗号化鍵を選び暗号化できる
- 復号する人（Decoder）：複数可
  - 暗号化コンテンツをあらかじめ入手
  - 指定された時刻の正式な時報を受けて復号

署名つき時報を放送する
以外何もする必要がない

暗号化鍵を管理する
必要がない

時報についた
電子署名データだけで
復号できる



通常の暗号を利用した場合との比較

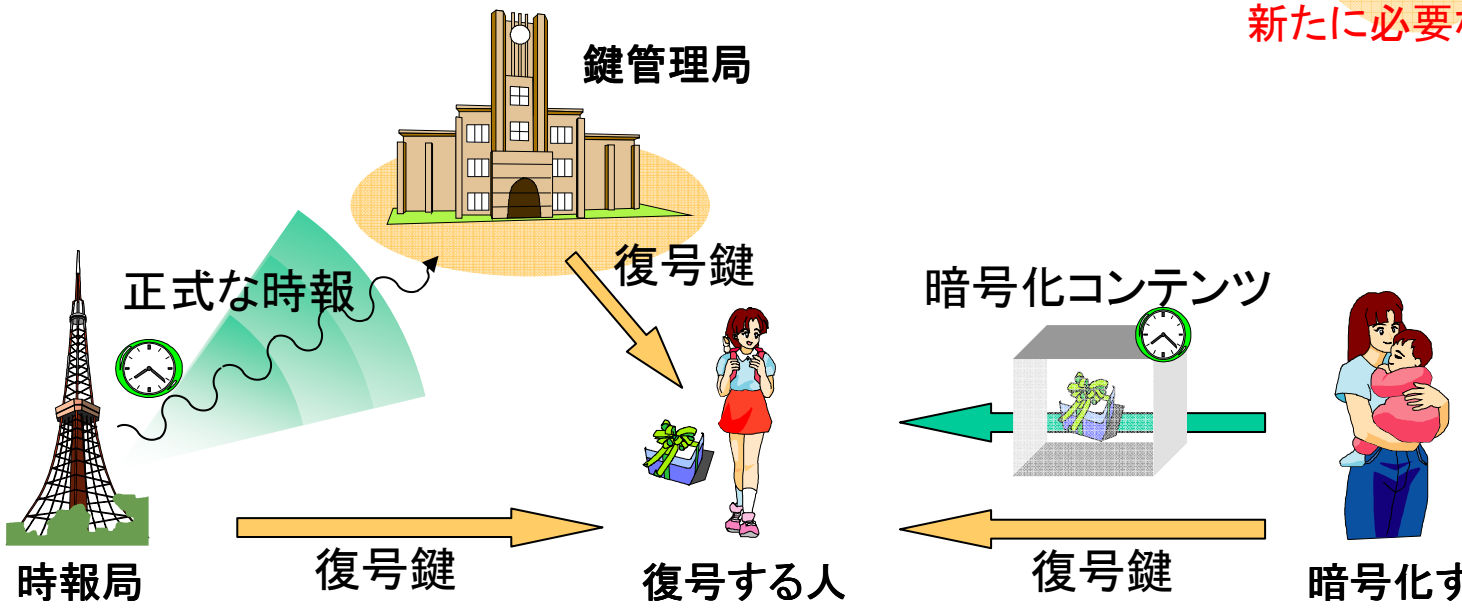
- **復号鍵（暗号化コンテンツ復号のための復号鍵）の管理**が必要
  - 時報局が管理する場合
    - 復号鍵の集め、時刻ごとに時報とともに復号鍵を放送
  - 暗号化した人が管理する場合
    - 指定時刻に復号鍵を送付
  - 新たに鍵管理局を導入する場合
    - 復号鍵を集め、正式な時報を受けて、復号鍵を放送

鍵の収集・保管・放送

鍵の保管・送付

鍵の収集・保管・送付

新たに必要な処理

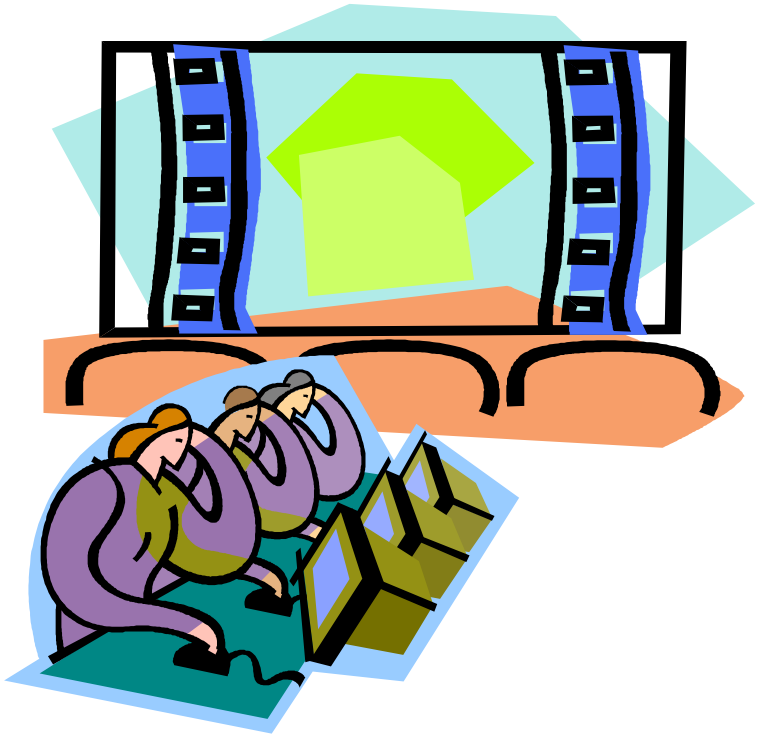


タイムカプセル暗号の性能

- 署名つき時報データ
  - 時刻情報＋約160ビット
- 暗号化コンテンツに付加されるヘッダ情報
  - 指定時刻情報＋約160ビット
- 暗号化鍵のサイズは1024ビット
  - RSA暗号と同じサイズ
- 安全性は楕円離散対数問題（＋α）の困難さに基づく
  - 多くの実用的な暗号と同じ安全性

タイムカプセル暗号の応用先

- 公式発表の日時指定
  - 全プレスや全国民が一斉に情報を入手
- 映画のロードショー日時指定
  - 全国の映画館で一斉に上映開始
- 試験開始の日時指定
  - 全国の会場で一斉に試験開始



- 予めコンテンツをタイムカプセル（暗号）化して配布
- 公開日時まで暗号化鍵を管理しておく必要がない

連絡先と発表予定

- 提案者
  - 吉田真紀（http://www-itl.ics.es.osaka-u.ac.jp/~yoshida/indexV6.html）
    - 大阪大学大学院情報科学研究科マルチメディア工学専攻
- 実装者
  - 光成滋生（http://homepage1.nifty.com/herumi/mtt/tc.html）
    - IPA未踏ソフトウェア事業での成果を利用しています
- 発表予定
  - 電子情報通信学会　情報セキュリティ研究会
    - 開催日：平成16年12月17日（金）
    - 開催地：機械振興会館
    - 発表者：吉田真紀，光成滋生，藤原融