最近の暗号研究

岡本 栄司
筑波大学
システム情報工学研究科

目次

- 情報セキュリティの必要性
- 暗号とは
- いまどきの暗号
  - 安全性証明ーRandom Oracle
  - ハッシュ関数解析ーMD5, SHA-1
  - Pairing暗号

ネットワーク社会

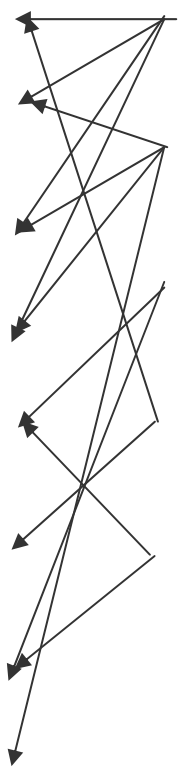
利便性

- 情報リテラシ　メール、Web

- 電子マネー
- ファイル交換
- 電子投票・オークション

リスク

- 情報漏えい、プライバシ侵害
- ウイルス
- スパイウェア、ボット
- フィッシング、ワンクリック
- ID窃盗
- 著作権侵害
- ネット詐欺、脅迫
- DDOS



・メール

・Web

・電子マネー

・ファイル交換

・電子投票/競売

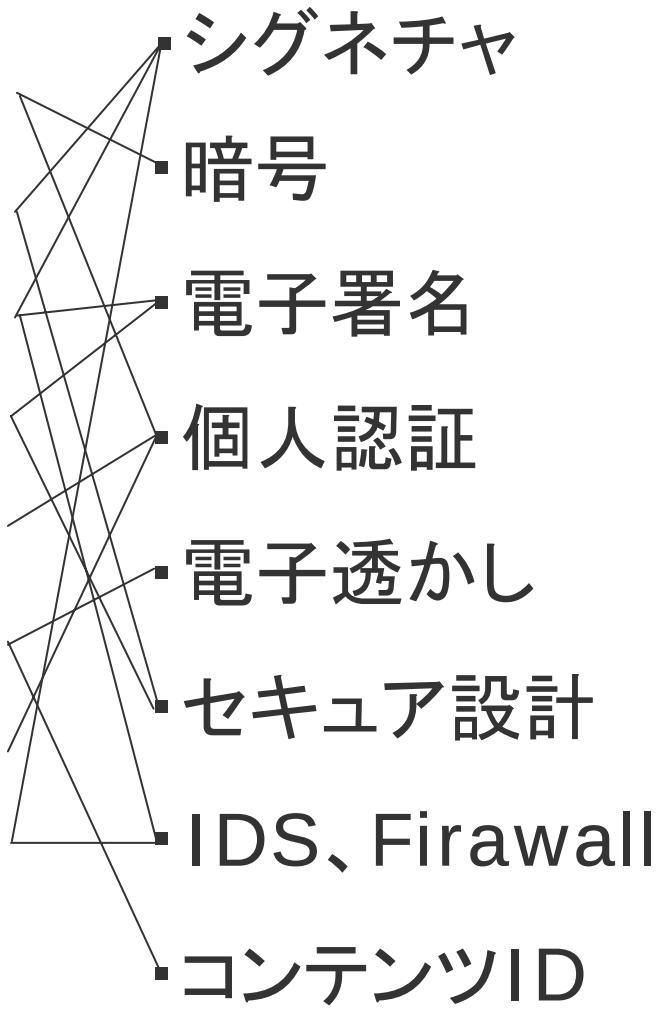
電子署名及び認証業務に関する法律

- 平成12年5月31日法律第102号
  - 郵政省、通産省、法務省

- 電磁的記録に記録された情報について本人による一定の電子署名がなされているときは、真正に成立したものと推定する。
- 認証業務のうち一定の要件を充たすものを特定認証業務と定義し、これを行おうとする者は、主務大臣（三大臣）の認定を受けることができる。
- 利用者が認定認証事業者等に不実の証明をさせる行為について、3年以下の懲役又は200万円以下の罰金に処する。

技術的対策

- 情報漏えい、プライバシ侵害
- ウイルス
- スパイウェア、ボット
- フィッシング、ワンクリック
- ID窃盗
- 著作権侵害
- 詐欺、脅迫
- DDOS



暗　号

暗号アルゴリズム（1）

- 対称暗号系（共通鍵暗号系）
  - ブロック暗号（同期式のみ）
    - DES, LUCIFER, MULTI2, MISTY, Cipherunicorn, AES
  - ストリーム暗号
    - 同期式暗号

      バーナム暗号、入替え暗号
    - 非同期式暗号（自己同期式暗号）

      NFSR

暗号アルゴリズム（２）

- 非対称暗号系（公開鍵暗号系）
  - ブロック暗号（同期式のみ）
    - 冪乗剰余型暗号

      RSA, ElGamal, Rabin, Cramer-Shoup, EPOC
    - ナップザック型暗号

      MH, GS,CR　　（現在、解読法が知られている）
    - その他：McEliece, Obscure表現
  - ストリーム暗号
    - 同期式暗号：BBS
    - 非同期式暗号

AES:Advanced Encryption Standard

- Rijndael : V. Rijmen and J. Daemenの提案
- 2001/11/26公布、2002/5/26施行
- $GF(2^8)$ 上の演算を多用, $\bmod m(x)$ 計算 $m(x) = x^8 + x^4 + x^3 + x + 1$
- 128ビットブロック暗号
- 鍵長 128 → Nk=4 、Nr=10

  192 → Nk=6、Nr=12

  256 → Nk=8、Nr=14

Nk: 鍵word長

Nr: round回数

Word=32bits, state=4*4 Bytes

AESの特徴

- 線形解読、差分解読などの解読に強い
- TDESより高速

  AES

  ソフト(Pentium III, 600MHz): 800 cycles/block、

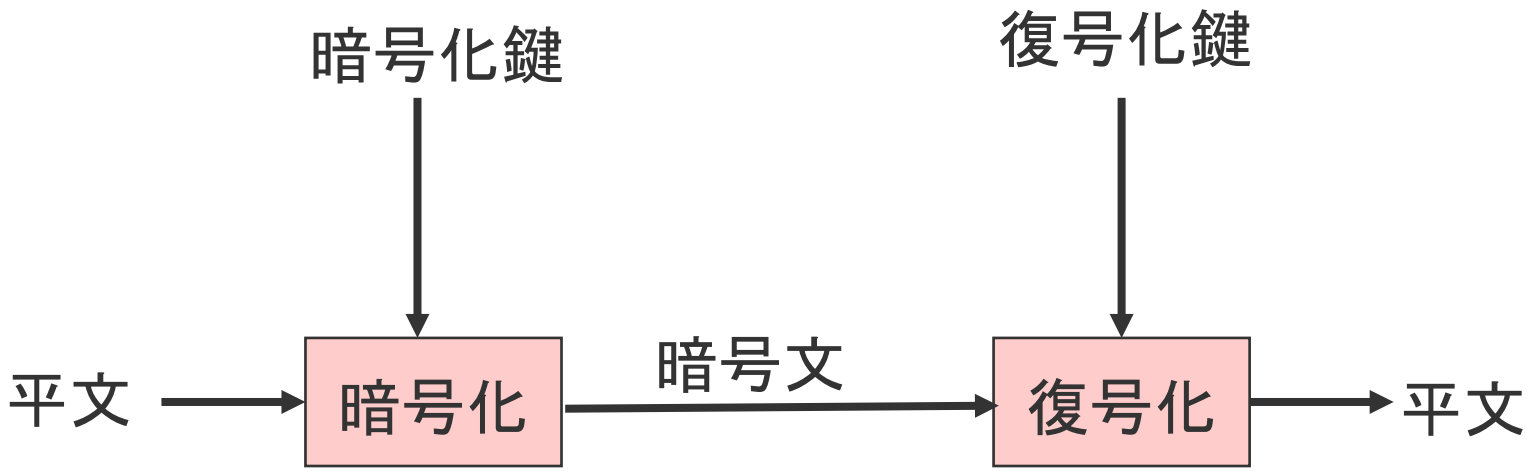
  ハード(NAND換算、0.35μ): 610kGates 、2Gb/s

  TDES

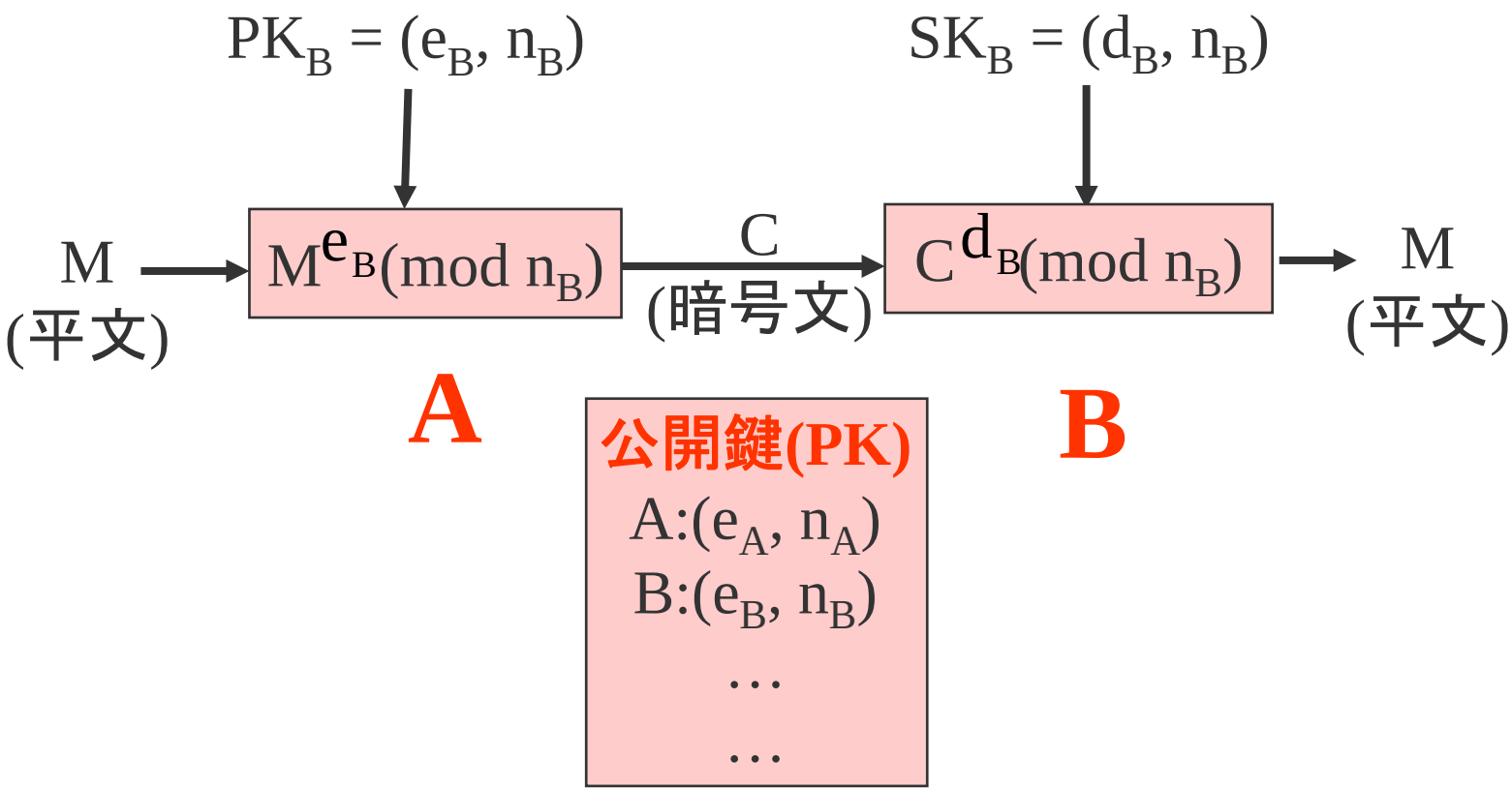
  ソフト: 850 c/b、ソフトウェアサイズ: 44kB

  ハード: 148kG、400Mb/s

公開鍵暗号系



RSA (Rivest, Shamir, Adleman)暗号



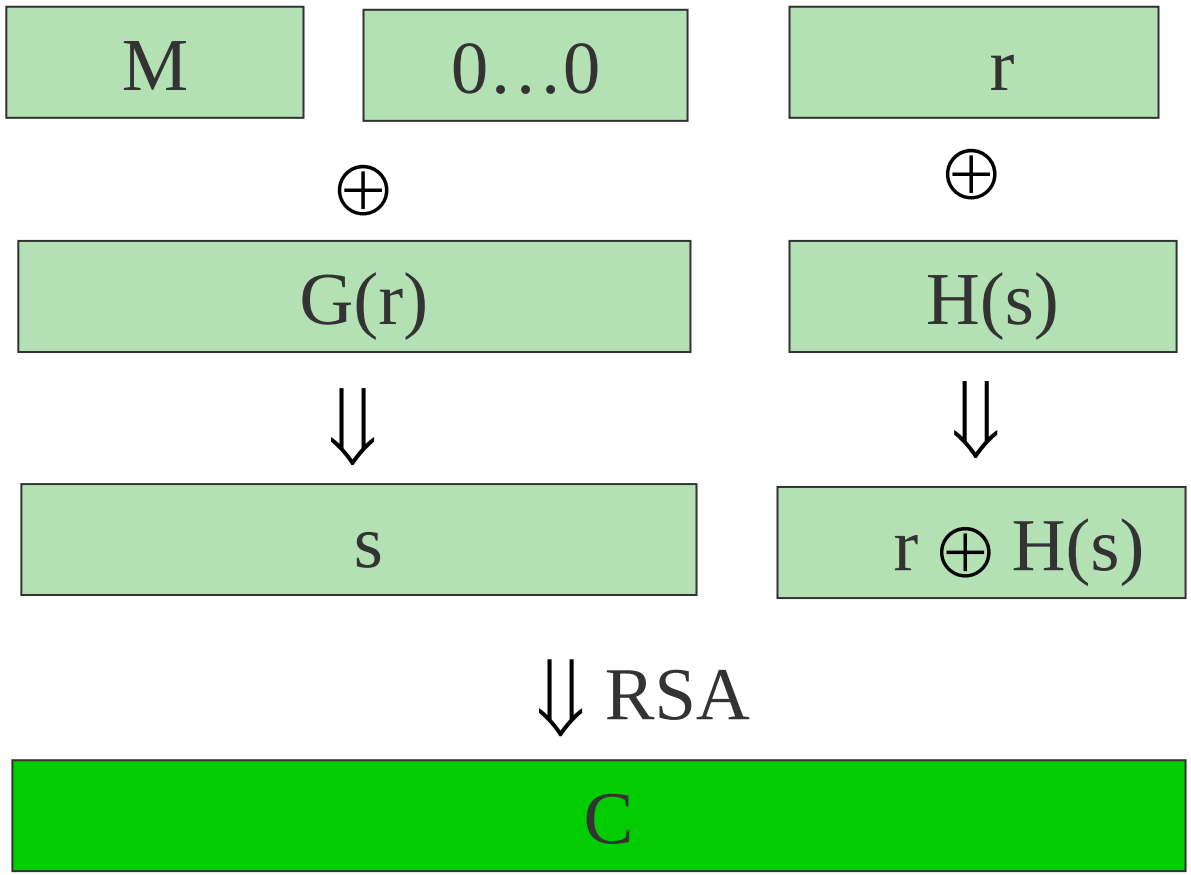
RSA-OAEP

- RSAの欠点
  - ある関係のある二つのメッセージ
  - 小さなメッセージ
  - 固定パターンを含むパディング
- IND-CCA2としてのRSA-OAEP

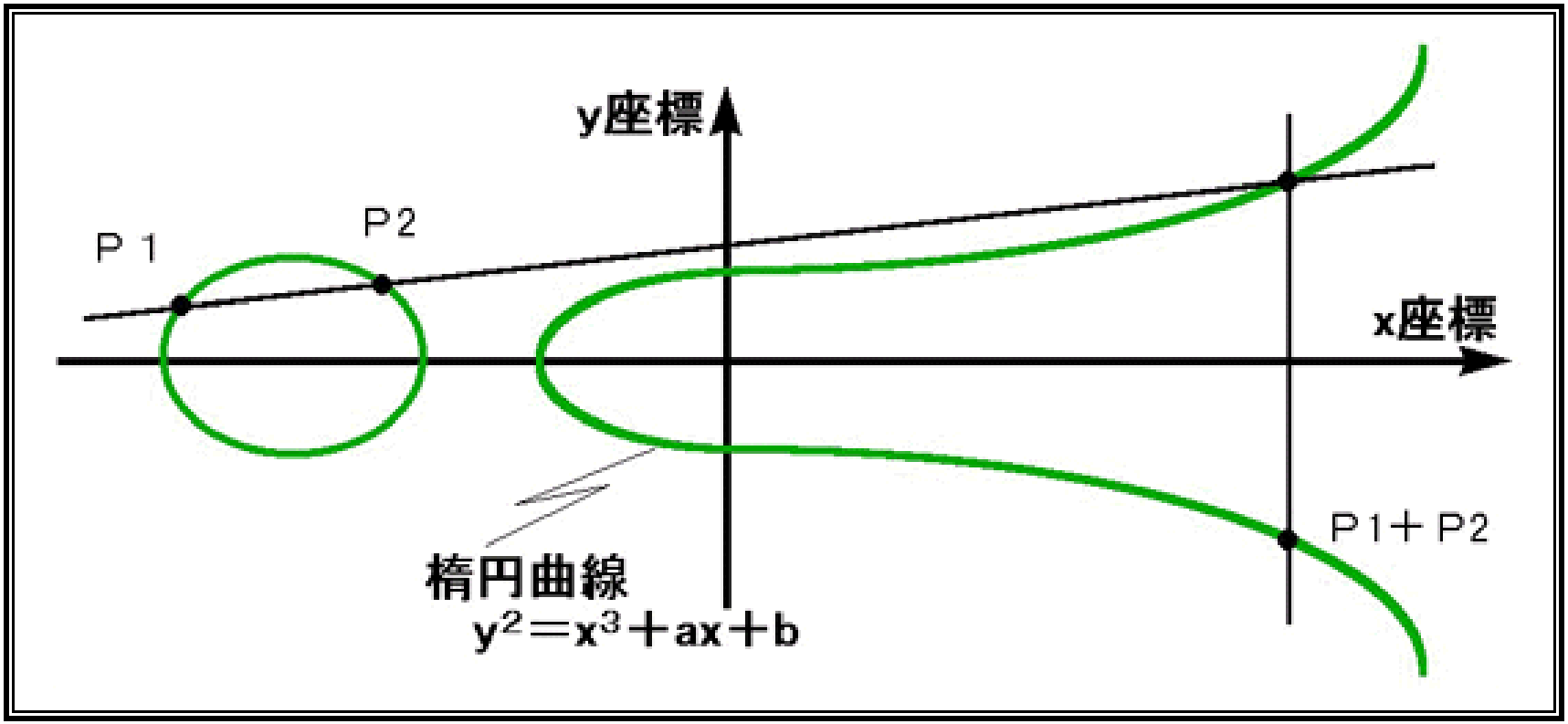
  適応的選択暗号文アタック(CCA2)に対して識別不可能な暗号

RSA-OAEP

Optimal Asymmetric Encryption Padding



楕円曲線



利点

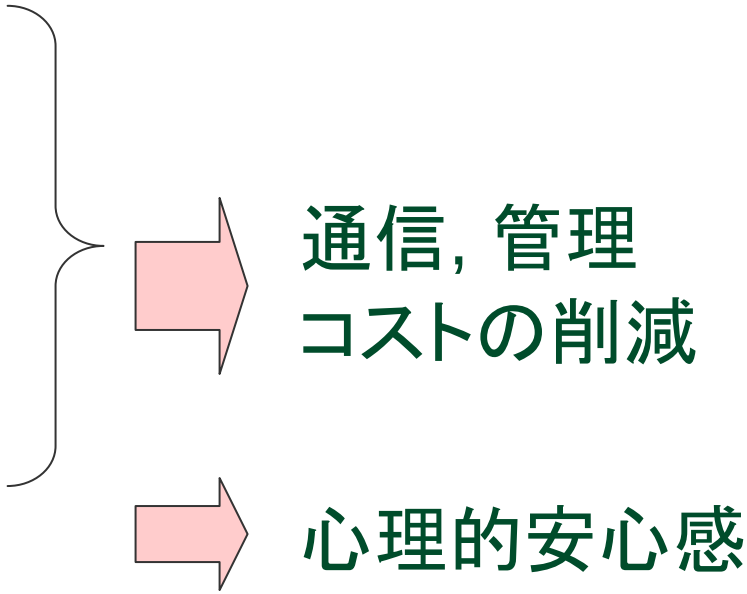
- 離散対数問題 $Y_i = x_i G$ が困難
- ブロック長を小さくできる
- ICカード等に向いている

Pairing Liteプロジェクトの概要

- テーマ名: “Paring Liteの研究開発”
- メンバー:
  - 筑波大学, はこだて未来大学, 情報セキュリティ大学院大学, FDK株式会社
- 競争的資金:
  - 新エネルギー・産業技術総合開発機構 (NEDO)
- 期間:
  - 2005年11月から2007年3月まで

Pairingを用いた暗号の特徴

- 短い署名長と鍵長
  - Pairing: ~160bit
  - 従来アルゴリズム (ex. RSA): ~ 1024bit
- 新しい暗号系
  - ブロードキャスト暗号
    - Pairing: 1-to-n
    - 従来アルゴリズム: 1-to-1
- IDを公開鍵に
  - Pairing: 名前やメールアドレス
  - 従来アルゴリズム: 公開鍵そのもの



こうした特徴を生かして暗号アプリケーションへ適用していく

Pairingとは

定　義

Pairingとは, $P, Q \in E(F_p)$に対して, 以下の双線形性写像eのことである.

$$e(aP,Q) = e(P, Q)^a = e(P,aQ)$$

注) 楕円曲線上の点から構成される元の集合: $E(F_p)$

暗号プロトコルを構成する際に有効な関数のこと

プロジェクトの概要

セキュリティ・プライバシを守る核技術となる楕円曲線上の双線形性写像Pairingを超小型化・超低消費電力化向けに軽量化したPairing Liteチップ(真正乱数搭載)を開発し、それを用いて構成した軽くてスケーラブルなプロトコルをモバイルネットワークに適用することを目指す。

双線形写像 (Pairing) ＋ FPGA ＝ Pairing Lite