楕円曲線とペアリング

吉田 努

白勢研ゼミ 2016/04/25

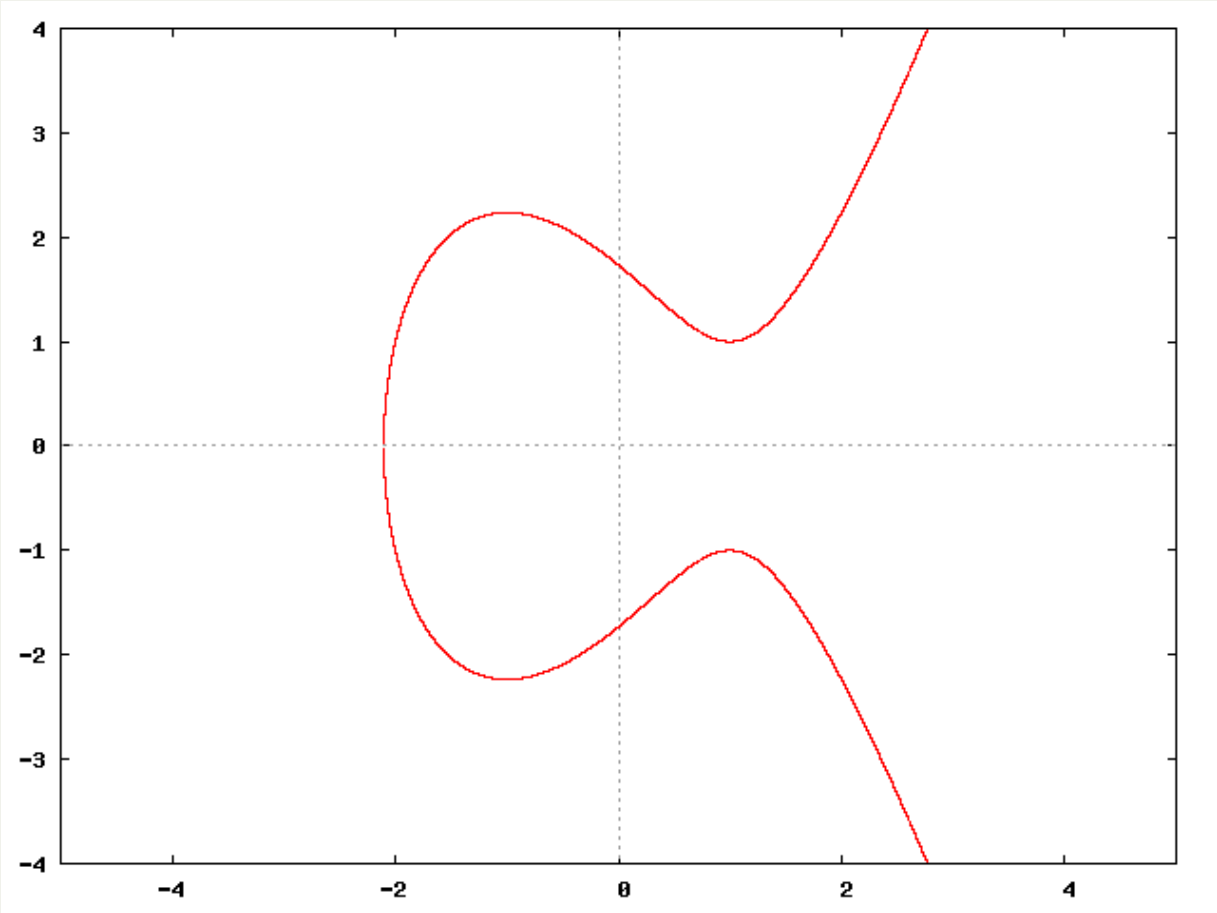
今日の内容

- 楕円曲線
- 公開鍵暗号
- ペアリング

楕円曲線

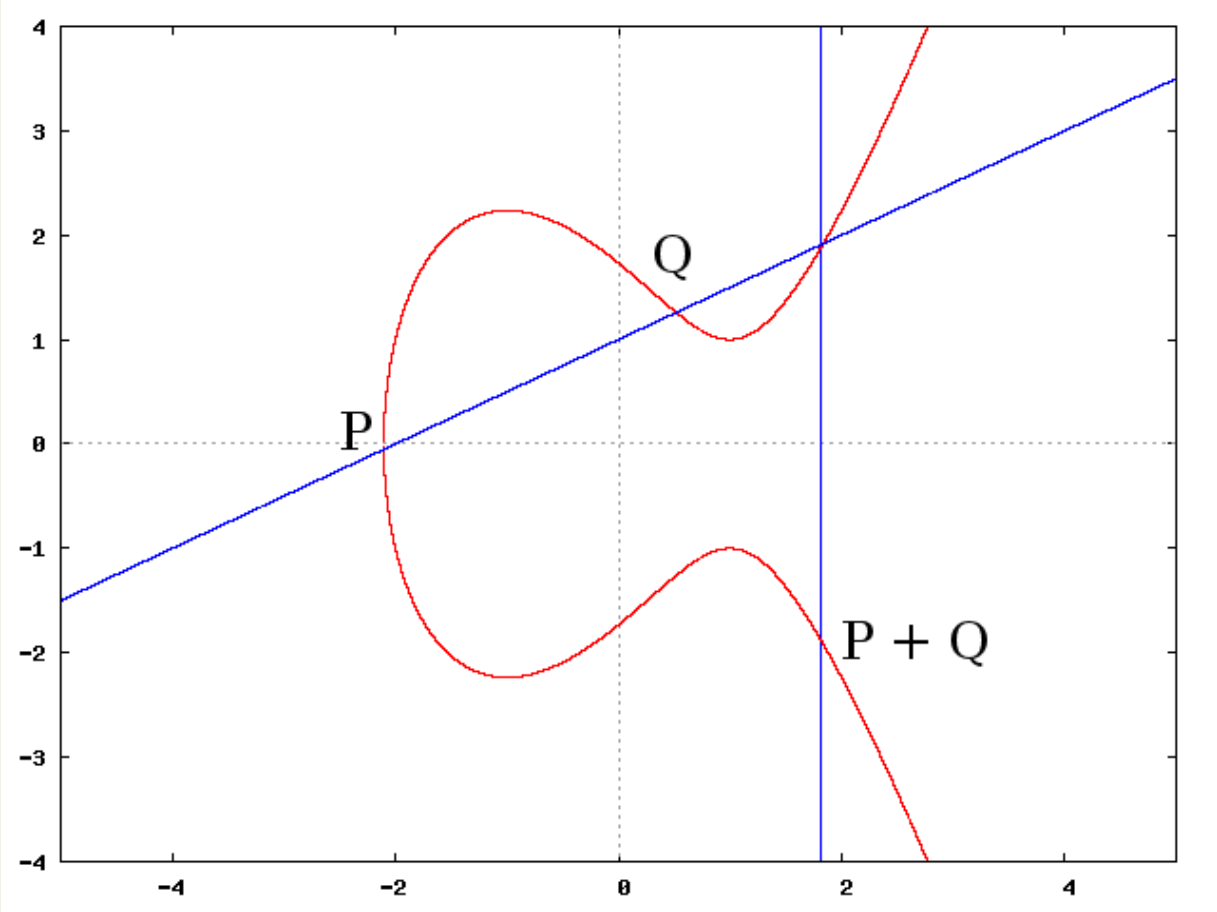
楕円曲線(1/3)

- $y^2 = x^3 + ax + b$
- 無限遠点



楕円曲線(2/3)

- 加算ができる



- P + Qが計算できる

楕円曲線(3/3)

- スカラー倍が計算できる
  - $kP = \underbrace{P + P + \cdots + P}_{k個のP}$
- 加算は群になる
  - 暗号に利用できる

群って何？

1. 単位元が存在する
2. 結合法則が成り立つ
3. 逆元が存在する

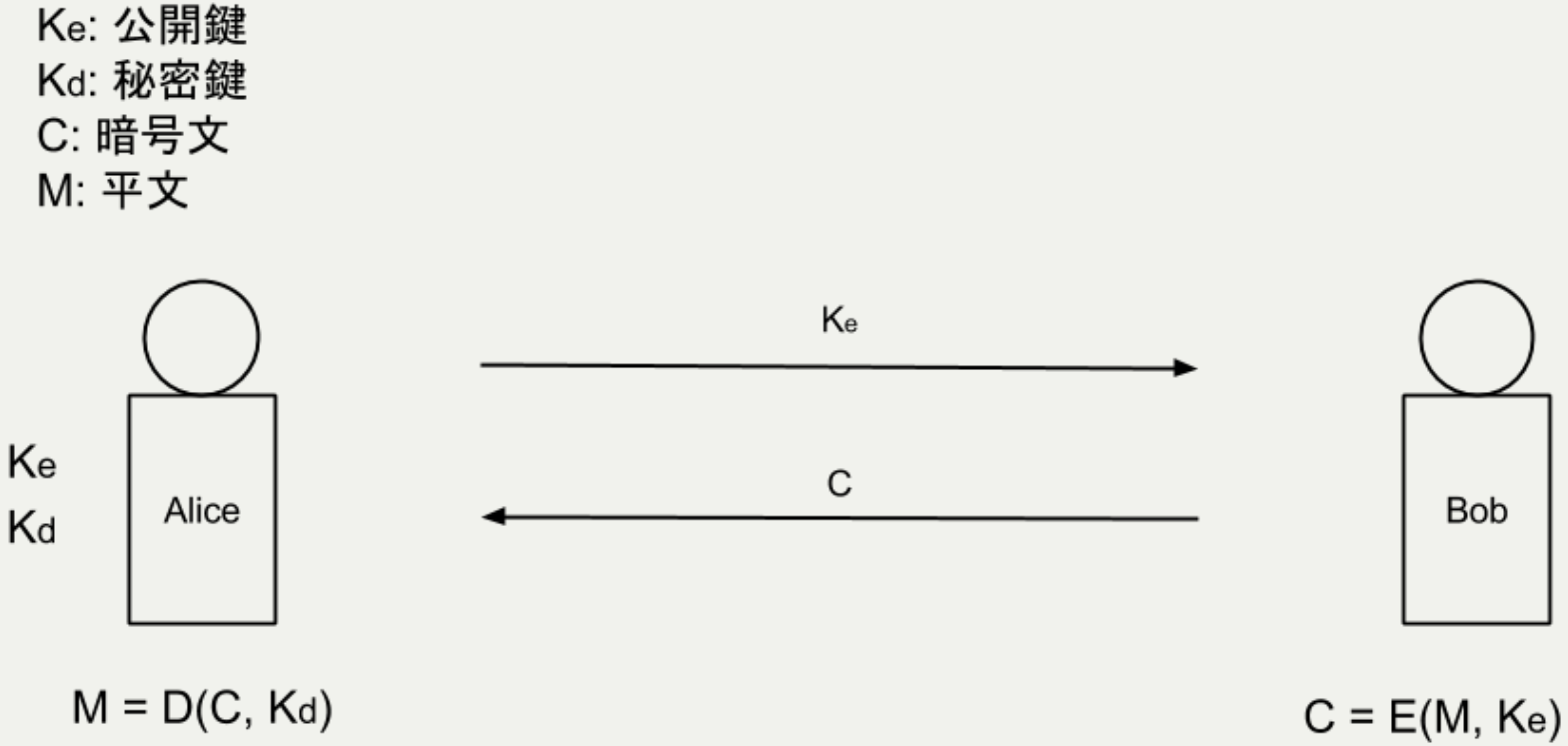
を満たす集合

暗号の話

- 平文: Plain text
- 暗号文: Cipher text
- 暗号化: Encryption
- 復号: Decryption

公開鍵暗号

- 一方向性を利用
- 公開鍵と秘密鍵に分かれている



- 一般的に利用されている
  - SSL/TLSなど

公開鍵暗号

- 離散対数
  - 楕円曲線暗号
  - エルガマル暗号
- 素因数分解
  - RSA

離散対数(1/2)

- $kP = Q$
  - k, Pが与えられたときQを求める
  - 容易
    - 普通のスカラー倍

離散対数(2/2)

- $kP = Q$
  - P, Qが与えられたときkを求める
  - 困難
    - $\frac{Q}{P} = k$とはならない
  - 離散対数問題

ペアリング

- 共通鍵暗号とも公開鍵暗号とも異なる
  - と言いつつ公開鍵暗号っぽい
- 日常的には利用されていない
- 今後普及するかどうか

ペアリング

- 楕円曲線上で定義できる双線形写像
- 入力
  - 楕円曲線上の2点
- 出力
  - 有限体の元

ペアリングの性質

- eをペアリングとする
- 双線形性
  - $e(kP, Q) = e(P, kQ) = e(P, Q)^k$
- 双線形性を上手く利用することで従来とは異なる暗号方式を構成できる

IDベース鍵共有(1/3)

- 鍵生成センターが必要
- 鍵生成センター
  - マスター鍵: s
- ユーザ
  - 秘密鍵: S_{ID}
  - 公開鍵: P_{ID}
  - 秘密鍵を鍵生成センターから受け取る
- IDを楕円曲線上の点に変換する関数$H(X)$
  - $H(ID) = P_{ID}$

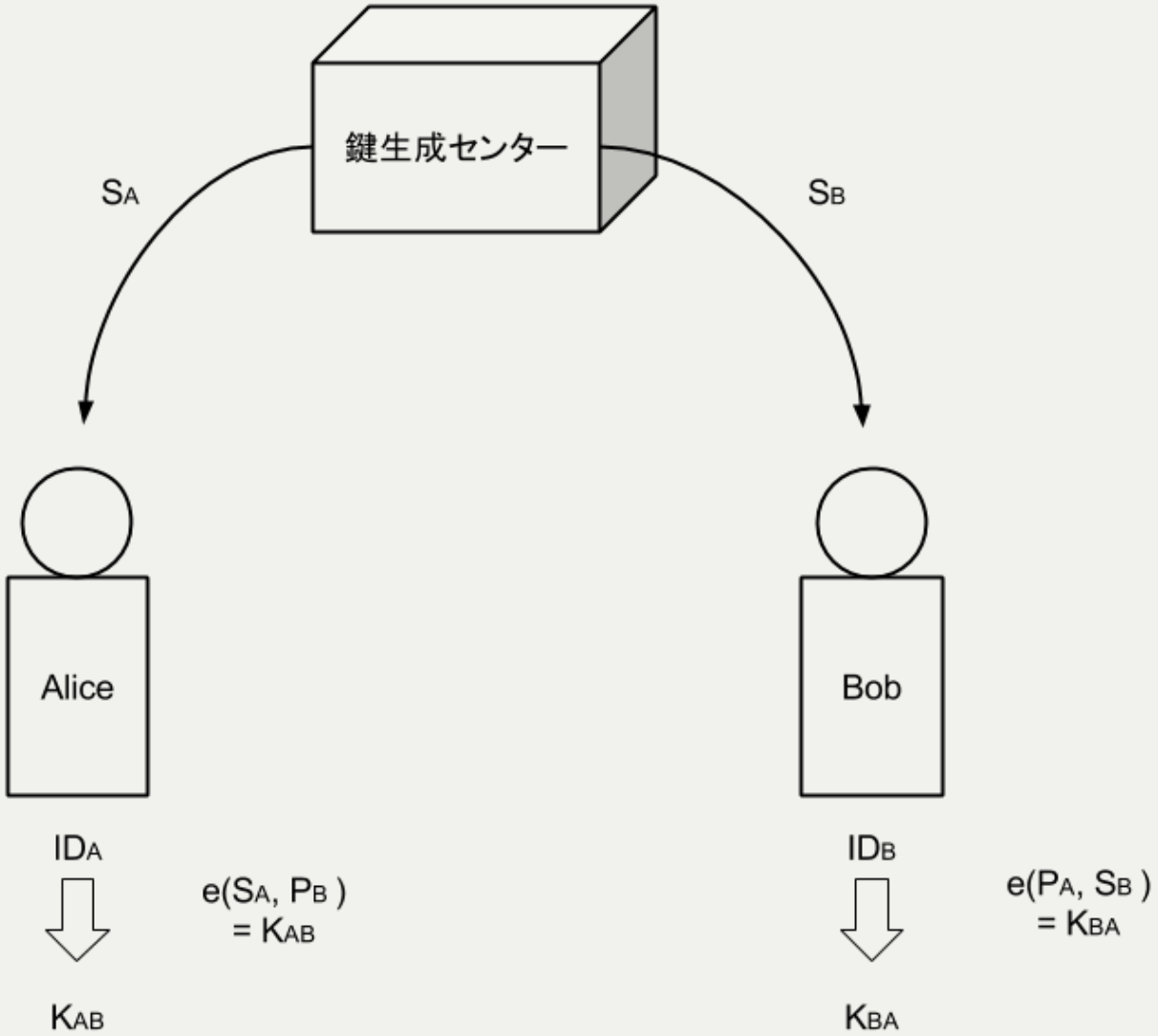
IDベース鍵共有(2/3)

- ユーザ Alice, Bob

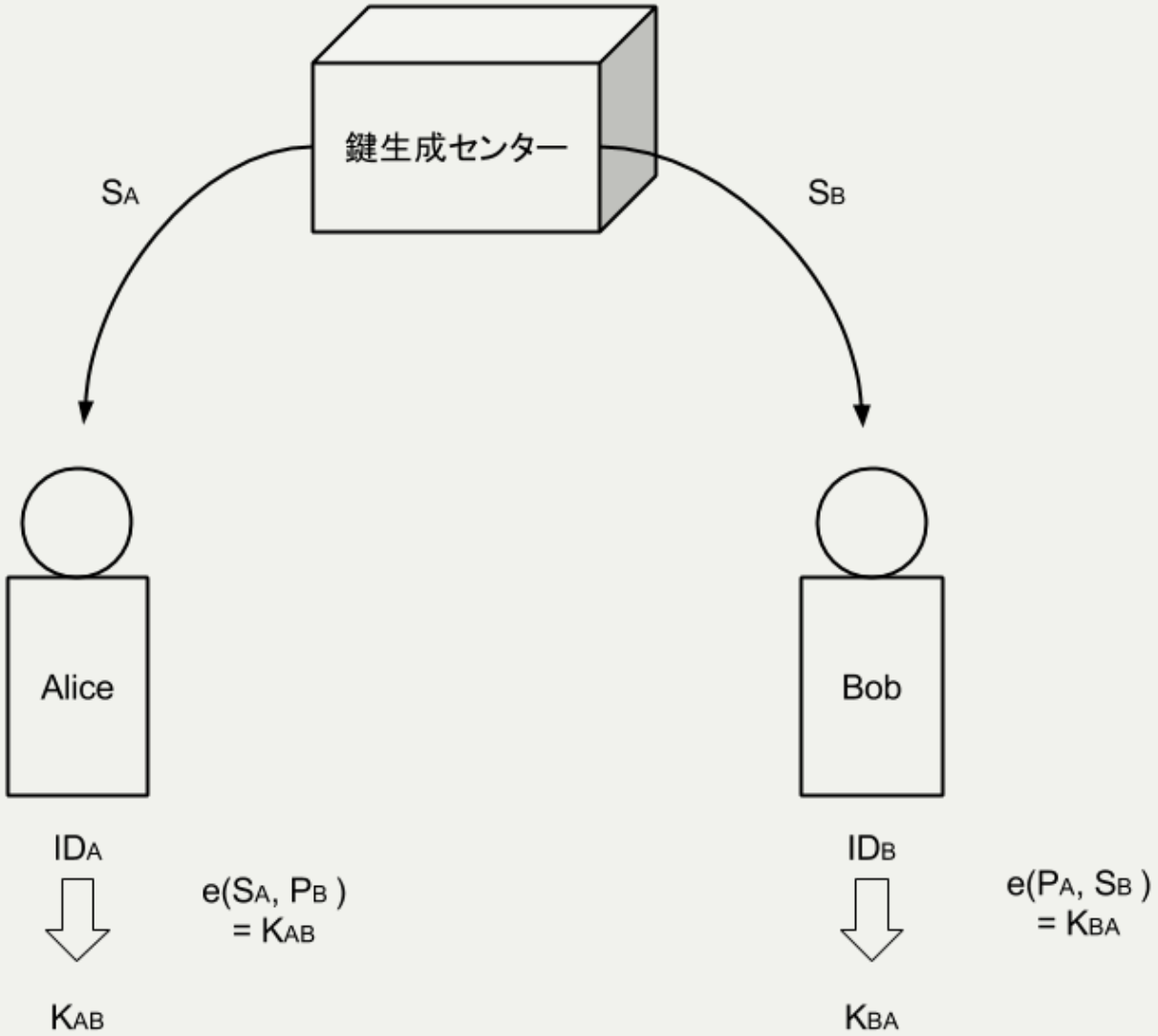
パラメータ	**Alice**	**Bob**
ID情報	ID_A	ID_B
公開鍵	P_A	P_B
秘密鍵	S_A	S_B

- $S_A = sP_A, S_B = sP_B$

IDベース鍵共有(3/3)


鍵生成センター
S_A
S_B
Alice
Bob
ID_A
ID_B
$e(S_A, P_B) = K_{AB}$
$e(P_A, S_B) = K_{BA}$
K_{AB}
K_{BA}

-->


鍵生成センター
S_A
S_B
Alice
Bob
ID_A
ID_B
$e(S_A, P_B) = K_{AB}$
$e(P_A, S_B) = K_{BA}$
K_{AB}
K_{BA}

ペアリングまとめ

- いろいろな応用がきく
  - 属性ベース暗号
  - プロキシ暗号
  - 放送型暗号

  などなど
- 比較的新しい暗号方式

参考文献

- 暗号理論と楕円曲線