Proxy Re-Encryption

代理人再暗号化

以下の二つを解説します

- Proxy Re-Encryptionとは
- 実装内容の理論
- 本来の理論

Proxy Re-Encryptionとは

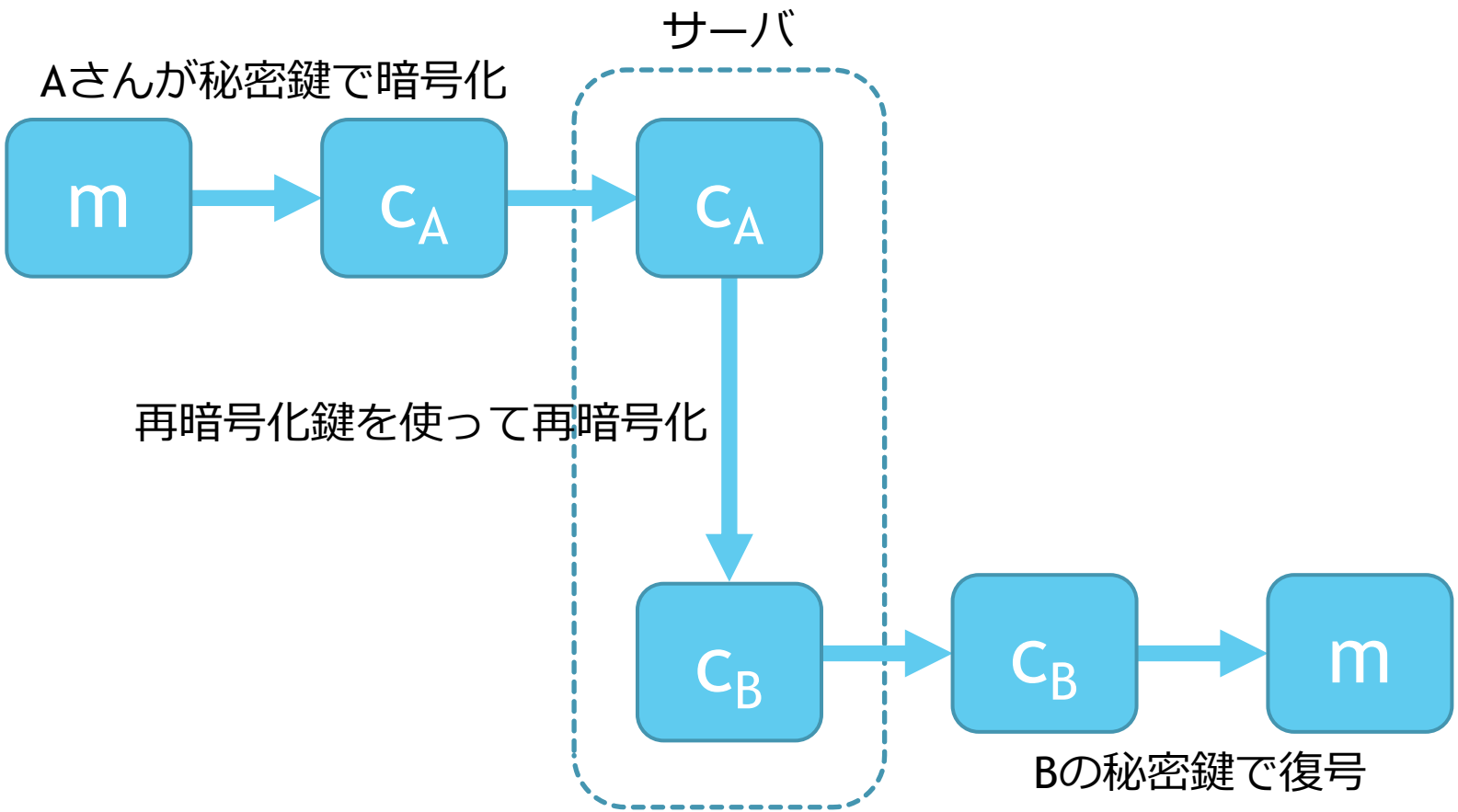
What is Proxy re-encryption?

Proxy Re-Encryptionとは

- プロキシ暗号・代理人再暗号化などと訳される
- 楕円曲線暗号の発展系

- 暗号化したデータを復号することなく特定の第三者が復号できる形に再暗号化できる

再暗号化してデータを共有



実装された理論

実装された理論とは

- 使用するライブラリの都合上，実際の理論とは違う実装となっている．
- また，複数箇所で不都合な実装があるかもしれないがそれは一般学生の限界なので理解してほしい

実装された内容

1. 鍵生成
   - 楕円曲線 E
   - $e: G_1 \times G_2 \rightarrow G_T$を対称ペアリング
   - $g := e(P, Q), P \in G_1, Q \in G_2$
   - P, Q, gを公開する
   - Aは整数aをランダムに選び秘密鍵とし aQを公開鍵とする。Bも似たようにする

実装された内容

- 暗号化($g = e(P, Q)$)
  - $C_a \coloneqq (mg^r, r(aQ))$を暗号文とする
- 通常の復号
  - 暗号文 $C_a \coloneqq (u, V_a)$に対して

$$\frac{u}{e(\frac{1}{a}P, V_a)} = \frac{mg^r}{e(\frac{1}{a}P, raQ)} = \frac{mg^r}{e(P, Q)^r} = \frac{mg^r}{g^r} = m$$

実装された内容

再暗号化鍵

$$r_{A\to B} = \frac{1}{a}bP$$

- 暗号化
  - $C_a := (mg^r, r(aQ))$を暗号文とする
- 再暗号化
  - 暗号文 $C_a := (u, V_a)$に対して

$$e(r_{A\to B}, V_a) = e\left(\frac{1}{a}bP, raQ\right) = e(P,Q)^{rb} = g^{rb}$$

  - 再暗号化文を(u, g^{rb})とする

実装された内容

- 再暗号化
  - $C_a := (mg^r, g^{rb})$を暗号文とする
  - (u, V_b)で届く
- 再暗号化された暗号文の復号
  - $$\frac{u}{V_b^{\frac{1}{b}}} = \frac{mg^r}{(g^{rb})^{\frac{1}{b}}} = \frac{mg^r}{g^r} = m$$

本来の理論

本来の理論

1. 鍵生成
   - 楕円曲線 E
   - E上の点P
   - $e: E \times E \rightarrow G$を対称ペアリング
   - $g := e(P, P) \in G$とし、P, gを公開する
   - Aは整数aをランダムに選び秘密鍵とし aPを公開鍵とする。Bも似たようにする

本来の理論

- 暗号化
  - $C_a := (mg^r, r(aP))$を暗号文とする
- 通常の復号
  - 暗号文 $C_a := (u, V_a)$に対して

$$\frac{u}{e(V_a, \frac{1}{a}P)} = \frac{mg^r}{e(raP, \frac{1}{a}P)} = \frac{mg^r}{e(P,P)^r} = \frac{mg^r}{g^r} = m$$

本来の理論

再暗号化鍵

$$r_{A\to B} = \frac{1}{a}bP$$

- 暗号化
  - $C_a := (mg^r, r(aP))$を暗号文とする
- 再暗号化
  - 暗号文 $C_a := (u, V_a)$に対して

    $$e(V_a, r_{A\to B}) = e\left(raP, \frac{1}{a}bP\right) = e(P,P)^{rb} = g^{rb}$$
  - 再暗号化文を(u, g^{rb})とする

本来の理論

- 再暗号化
  - $C_a := (mg^r, g^{rb})$を暗号文とする
  - (u, V_b)で届く
- 再暗号化された暗号文の復号
  - $\frac{u}{V_b^{\frac{1}{b}}} = \frac{mg^r}{(g^{rb})^{\frac{1}{b}}} = \frac{mg^r}{g^r} = m$