事前課題 C

川原尚己
28G23027

- 秘密の共有の検証

  Alice が Bob は本物かどうかを確認する手順を以下に示す.

  1. Bob が, DH 鍵共有法によって生成した共有鍵を署名して, Alice に送りつける.
  2. Alice は Bob と同じ共有鍵を持っているから, Bob の署名済み共有鍵を検証できる.

  以上のようにして検証が可能である. ただし, 1.で Bob が Alice に署名した鍵を送る際には暗号化された通信路を用いる必要がある. また, 上の手順の Alice と Bob を入れ替えることで Bob が Alice は本物かどうかを確認する.

- 準同型暗号の応用

  $\mathrm{N_v}$を投票者の人数, $\mathrm{N_c}$を候補者の人数, bを投票先を区別するための基数とする. 投票者k番目の候補者に投票するときは, $\mathrm{b^{k-1}}$が平文となる. すべての投票者の投票内容m_iを公開鍵 PK を用い, 暗号化し, 暗号文$\mathrm{c_i}$を得る. ($c_i = Enc(PK, m_i)$) すべての投票者の暗号化した投票内容c_iの総乗を求める. ($\mathrm{T} = \prod_{i=1}^{N_v} c_i \mod \mathrm{n^2}$)最後に復号すると, 集計結果$\mathrm{r_i}$が得られる.

$$\mathrm{result} = \mathrm{Dec(SK, T)} = \mathrm{r_1} b^0 + \cdots + r_{N_c} b^{N_c - 1}$$

- 合議文章

  5 人が順にそれぞれの秘密鍵を用いて署名を行なう. 一人目は平文に, 二人目以降は前の人間の署名結果に署名を加える. 検証の際には, 署名とは逆順にそれぞれの公開鍵を用いて行なう.