応用数学６ 2011 年 1 月 13 日

第 4 回小テスト

講師: 安永憲司

問題 1.

識別不能安全である 1 ビットメッセージ（つまり $\mathcal{M}_n = \{0,1\}$）に対する暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を考える．$\ell(n)$ ビットメッセージに対する暗号方式 $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ を以下のように定義する．

1. $\mathsf{Gen}'(1^n) = \mathsf{Gen}(1^n)$.
2. $\mathsf{Enc}'_{pk}(m_1 m_2 \cdots m_{\ell(n)}) = (\mathsf{Enc}_{pk}(m_1), \mathsf{Enc}_{pk}(m_2), \ldots, \mathsf{Enc}_{pk}(m_{\ell(n)}))$.
   ただし，各 $i \in \{1, \ldots, \ell(n)\}$ について，$m_i \in \{0,1\}$.
3. $\mathsf{Dec}'_{sk}(c_1 c_2 \cdots c_{\ell(n)}) = (\mathsf{Dec}_{sk}(c_1), \mathsf{Dec}_{sk}(c_2), \ldots, \mathsf{Dec}_{sk}(c_{\ell(n)}))$.

このとき，Π' は識別不能安全であることを示せ.

ヒント:

メッセージ $m_0, m_1 \in \{0,1\}^\ell$ に対して，以下の分布 H^i を定義する.

$$H^i = \{(pk, \mathsf{Enc}_{pk}(m_1^0), \ldots, \mathsf{Enc}_{pk}(m_i^0), \mathsf{Enc}_{pk}(m_{i+1}^1), \ldots, \mathsf{Enc}_{pk}(m_\ell^1)) \mid (pk, sk) \leftarrow \mathsf{Gen}(1^n)\}.$$

ただし，$i \in \{0, 1, \ldots, \ell\}$ であり，$m_0 = (m_1^0, m_2^0, \ldots, m_\ell^0), m_1 = (m_1^1, m_2^1, \ldots, m_\ell^1)$ である.

この分布 H^i を利用して，Π' が識別不能安全であることを証明してみよう.

問題 2.

識別不能安全である暗号方式 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を利用して，暗号方式 $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ を以下のように定義する.

1. $\mathsf{Gen}'(1^n) : (pk, sk) \leftarrow \mathsf{Gen}(1^n), r \xleftarrow{R} \{0,1\}^n, pk' = (pk, r), sk' = sk, (pk', sk')$ を出力 .
2. $\mathsf{Enc}'_{pk'}(m) = \begin{cases} (0, \mathsf{Enc}_{pk}(pk')) & m = pk' \text{のとき} \\ (1, \mathsf{Enc}_{pk}(m)) & \text{それ以外} \end{cases}$
3. $\mathsf{Dec}'_{sk'}(b, y) = \begin{cases} pk' & b = 0 \text{ のとき} \\ \mathsf{Dec}_{sk}(y) & \text{それ以外} \end{cases}$

このとき，Π' は，識別不能安全であるが，IND-CPA 安全でないことを示せ.