# Examination of Theoretical Foundation of Cryptography

November 30, 2022

## Grades

Grades will be determined as follows:

- (25%) Homework assignments
  Collaboration is not allowed. You should not submit a problem solution that you cannot explain orally.
- (75%) Reading report (25%)+ Presentation (50%)

## Requirements

- The homework will be graded on *correctness*, *clarity*, and *conciseness*,
- The reading report will be judged by its *quality*, not its *length*. Please keep it succinct.
- All submitted works (homework and reading report) must be typeset in LaTeX and merged in one PDF file. The PDF file should begins with a title page which lists your name, student id, supervisor, then followed by your homework and reading report.
- Please email your work to `202117047@mail.sdu.edu.cn` before 2022.12.28 with subject of the following format: `id-name`

Warning: submission does not meet the above format requirements runs a risk of being degrading!

## Homework

**Exercise 0.1.** Let $f$ be a (randomized) function on the domain of $\Omega$, $X$ and $Y$ are two random variables defined over $\Omega$, prove $\Delta(f(X), f(Y)) \leq \Delta(X, Y)$.

$$
\begin{aligned}
& \Delta(f(X), f(Y)) \\
= & \sum_{z \in Z} \Big| \Pr[f(X) = z] - \Pr[f(Y) = z] \Big| \\
= & \sum_{z \in Z} \Big| \sum_{r \in R} \Pr[R = r](\Pr[X \in S_{r,z}] - \Pr[Y \in S_{r,z}]) \Big| \\
\leq & \sum_{z \in Z} \sum_{r \in R} \Pr[R = r] \Big| \Pr[X \in S_{r,z}] - \Pr[Y \in S_{r,z}] \Big| \\
= & \sum_{r \in R} \Pr[R = r] \sum_{z \in Z} \Big| \Pr[X \in S_{r,z}] - \Pr[Y \in S_{r,z}] \Big| \\
\leq & \sum_{r \in R} \Pr[R = r] \Delta(X, Y) = \Delta(X, Y)
\end{aligned}
$$

**Exercise 0.2.** Let $f : \{0,1\}^* \to \{0,1\}^{\ell(\lambda)}$ be a OWF. Is there a lower bound of $\ell(\lambda)$?

A lower bound of $\ell(\lambda)$ is $\omega(\log \lambda)$. Consider the following attack against one-wayness. Given the challenge $y^*$, $\mathcal{A}$ could simply sample $x \leftarrow X$, then check if $f(x) = y^*$. Let $n = 2^\ell$, its advantage function is:

$$
\begin{aligned}
\mathsf{Adv}_{\mathcal{A}}(\lambda) &= \sum_{i=1}^{n} \Pr[y^* = y_i] \Pr[f(x) = y_i] \\
&= \sum_{i=1}^{n} \Pr[y^* = y_i]^2 = \sum_{i=1}^{n} p_i^2
\end{aligned}
$$

The second equation follows from the fact that the distribution of $f(x)$ and $y^* \leftarrow f(x^*)$ are identical. Next, we bound the above advantage.

The arithmetic mean is defined as

$$
A_{\text{mean}} = \frac{1}{n} \sum_{i=1}^{n} p_i
$$

The quadratic mean is defined as

$$
Q_{\text{mean}} = \sqrt{\frac{1}{n} \sum_{i=1}^{n} p_i^2}
$$

We have

$$
Q_{\text{mean}} \geq A_{\text{mean}} \Rightarrow \sum_{i=1}^{n} p_i^2 \geq \frac{1}{n} \sum_{i=1}^{n} p_i = \frac{1}{n}
$$

Thereby, the lower bound of $\mathcal{A}(\lambda)$ is $1/n = 1/2^\ell$, which achieves when the function is uniform. This means when $f$ is not uniform, the advantage is higher!

To make it negligible, $\ell(\lambda)$ must $\geq \omega(\log \lambda)$.

**Exercise 0.3.** Please build a family of weak PRP, which is not a family of strong PRP.

Let $E$ be a family of weak PRP from $\{0,1\}^n \to \{0,1\}^n$ with key space $\{0,1\}^n$. In the follow, let $x^* = D_k(0^n)$, $y^* = E_k(k)$. Define $E'$ based on $E$ with the following adjustments:

$$E'_k(x) = \begin{cases} E_k(x) & \text{if } x \neq \{k, x^*\} \\ 0^n & \text{if } x = k \\ y^* & \text{if } x = x^* \end{cases}$$

The constant $\{0,1\}^n$ will be part of the public parameter. The choice of $\{0,1\}^n$ is arbitrary, any fixed constant will do. Clearly, $E'$ remains a permutation.

- Actually, $E'$ is a family of weak PRP. To reduce the weak pseudorandomness based on $E$, it suffices to argue that the probability $\mathcal{A}$ querying $x^*$ or $k$ is negligible, since otherwise there exists an adversary can break the weak pseudorandomness $E$ by querying the real-or-random query at these two particular points.
- However, when given access to an inversion oracle $D_k(\cdot)$, $\mathcal{A}$ can obtain $k$ by querying the oracle with $0^n$, then breaks the pseudorandomness entirely.

**Exercise 0.4.** Construct a counterexample between MMI security and the standard IND-CPA security for SKE.

MMI is static in nature. The reason account for MMI is weaker than CPA is that $\mathcal{A}$ is allowed to adaptively select the vulnerable point of encryption system. The idea of separation is exactly built upon this. So, we can craft an ordinary MMI secure SKE to one have a brilliant encryption point, i.e., always encrypts $m^*$ to $m^*$. The information of $m^*$ can be treated as part of $k$, and $\mathsf{Enc}'(k,m)$ is $(\mathsf{Enc}(k,m), m^*)$ when $m \neq m^*$ and is $m^*$ when $m = m^*$. Clearly, the resulting scheme is still MMI, by obviously not IND-CPA secure. This is because after when query to $\mathcal{O}_{\text{enc}}$, the brilliant point $m^*$ is revealed.

**Exercise 0.5.** Show the equivalence between the standard IND-CPA security and the alternative definition.

**Uniform CPA security.** Let $M$ be the message space. PKE is uniform CPA secure if for any PPT $\mathcal{A}$:

$$\mathsf{Adv}_{\mathcal{A}}(\lambda) = \Pr\left[ i = i' : \begin{array}{l} (pk, sk) \leftarrow \mathsf{Gen}(\lambda); \\ M' = \{m_1, \ldots, m_n\} \subseteq M \leftarrow \mathcal{A}, |M'| \geq 2; \\ i \xleftarrow{\text{R}} n; \\ c^* \leftarrow \mathsf{Enc}(pk, m_i); \\ i' \leftarrow \mathcal{A}(pk, M', c^*); \end{array} \right] - \frac{1}{n}$$

is negligible in $\lambda$.

Uniform CPA $\Rightarrow$ IND-CPA: By restricting $|M'| = 2$, the implication is obvious. Let $\mathcal{A}$ be an adversary against IND-CPA security, we can build an adversary $\mathcal{B}$ breaks uniform CPA security. $\mathcal{B}$ selects two distinct messages $m_0, m_1$, submits $M' = \{m_0, m_1\}$, and receives $c^* \leftarrow \mathsf{Enc}(pk, m_\beta)$ in return. $\mathcal{B}$ sends $c^*$ to $\mathcal{A}$ and forwards $\mathcal{A}$'s reply as its solution. Clearly, $\mathsf{Adv}_{\mathcal{B}}(\lambda) = \mathsf{Adv}_{\mathcal{A}}(\lambda)$.

IND-CPA $\Rightarrow$ Uniform CPA: We proceed via a sequence of games.

**Game 0.** Real uniform CPA security game. In the challenge phase, upon receiving $M'$, $\mathcal{CH}$ picks $i \xleftarrow{R} n$, sends $c^* \leftarrow \mathsf{Enc}(pk, m_i)$ to $\mathcal{A}$. Clearly, we have $\mathsf{Adv}_{\mathcal{A}}(\lambda) = |\Pr[S_0] - 1/|M'||$

**Game 1.** Real uniform CPA security game. In the challenge phase, upon receiving $M'$, $\mathcal{CH}$ picks $i \xleftarrow{R} n$, $j \xleftarrow{R} n$, sends $c^* \leftarrow \mathsf{Enc}(pk, m_j)$ to $\mathcal{A}$. In game 1, $i$ is information-theoretically hidden from $\mathcal{A}$, thus we have $\Pr[S_1] = |1/M'|$.

We then prove the following claim: $|\Pr[S_0] - \Pr[S_1]| = \mathsf{negl}(\lambda)$ by assuming the IND-CPA security.

Let $\mathcal{B}$ be an adversary against IND-CPA security, he picks $i, j \xleftarrow{R} n$, sets $m_0 = m_i$ and $m_1 = m_j$, submits $(m_0, m_1)$ to its challenger and receives back $c^*$. $\mathcal{B}$ sends $c^*$ to $\mathcal{A}$. $\mathcal{A}$ outputs a guess $i'$ for $i$. If $i' = i$, $\mathcal{B}$ outputs 0. Else, $\mathcal{B}$ outputs a random guess for $\beta$.

$$\begin{aligned}\mathsf{Adv}_{\mathcal{B}}(\lambda) &= |\Pr[\beta = 0](\Pr[S_0] + (1 - \Pr[S_0])/2) + \Pr[\beta = 1](\Pr[S_1] + (1 - \Pr[S_1])/2) - 1/2| \\ &= \frac{1}{2}\left|\frac{1}{2}(\Pr[S_0] - \Pr[S_1])\right| = \frac{1}{4}|\Pr[S_0] - \Pr[S_1]|\end{aligned}$$

Putting all the above together, we have $\mathsf{Adv}_{\mathcal{A}}(\lambda) = \mathsf{negl}(\lambda)$.

## Reading Report

Please pick your favorite cryptographic paper from the following top conferences (FOCS, STOC, Crypto, Eurocrypt, Asiacrypt, TCC, PKC, ACM CCS, IEEE S&P) in the last 10 years, then write a reading report, which should includes:

- The information of the paper (title, author, conference name)
- The main idea and technique you learn from it
- Your own reflection and thinking

## Presentation

Present your reading report with slides (12 minutes talk and 3 minutes discussions), which should emphasizes

- The novel concept.
- The main technique.
- The key idea.