

# Examination of Theoretical Foundation of Cryptography

December 7, 2021

## 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  $\text{\LaTeX}$  and merged in one PDF file. The PDF file should begin with a title page which lists your name, student id, supervisor, then followed by your homework and reading report.
- Please email your work to `zm_min@mail.sdu.edu.cn` before **2021.12.23** 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  $\Delta(f(X), f(Y)) \leq \Delta(X, Y)$ .

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

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

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

**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  $\mathcal{A}$ :

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

is negligible in  $\lambda$ .

## 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.