

Introduction to Cryptography

CSCI-GA.3210-001

Instructor: Nir Bitansky

Problem Set 3

Due: October 28, 2026 at 11:59 PM

Instructions:

- Turn in your solutions in $\text{\LaTeX}$ and submit a PDF through Gradescope. (You don't have to know latex, can use AI tools like Prism.)
- Solutions will be graded for both correctness and clarity. If you do not know how to solve a question, you may write "I don't know how to do this" to receive 15% credit for that question.
- Discussion with peers is strongly encouraged, but you must write up your solutions on your own and list your discussion partners. Cite any external sources you use.
- AI use is permitted. If you use AI to solve the homework, list the exact model as a collaborator and include your prompts in an appendix. We strongly recommend solving the questions yourself: the final exam will mostly contain variants of homework questions.
- Use the course forum for clarification questions, but do not post solutions there.

1. (22 pts) Prove that inefficiently computable length-doubling PRGs exist unconditionally. That is, give an inefficient deterministic algorithm $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ such that

$$\{G(U_n)\}_{n \in \mathbb{N}} \approx_c \{U_{2n}\}_{n \in \mathbb{N}} .$$

2. (22 pts) Let X be any distribution, and let B be a jointly distributed bit. Show that if an efficient algorithm D distinguishes (X, B) from (X, U_1) with advantage ε , then there exists an efficient algorithm P that, given X , predicts B with probability at least $1/2 + \varepsilon/2$.

3. (28 pts) Consider the distribution

$$(A, As + e),$$

where $A \leftarrow \mathbb{Z}_2^{2n \times n}$ and $s \leftarrow \mathbb{Z}_2^n$ are uniform, and e is sampled from some arbitrary distribution.¹ All operations are over $\mathbb{Z}_2$.

Suppose that there is an efficient deterministic algorithm P such that

$$\Pr[P(A, As + e) = s_1] \geq \frac{1}{2} + \varepsilon.$$

Prove that there is an efficient algorithm B that, given $(A, As + e)$, recovers s with probability at least $\text{poly}(\varepsilon/n)$. The following items will guide you toward this goal.

¹We mentioned in class the case where the coordinates of $e \in \mathbb{Z}_2^{2n}$ are sampled independently, with each coordinate equal to 1 with probability 0.1, corresponding to the LPN problem. This is not relevant to this question.

- (a) (7 pts) Show that for every invertible matrix $M \in \mathbb{Z}_2^{n \times n}$, if A is sampled uniformly from $\mathbb{Z}_2^{2n \times n}$, then AM is also uniformly distributed over $\mathbb{Z}_2^{2n \times n}$.
- (b) (7 pts) Show that, for every distribution $\mathcal{M}$ supported on invertible matrices, with probability at least $\varepsilon/2$ over the choice of (A, s, e) ,

$$\Pr_{M \leftarrow \mathcal{M}} [P(AM^{-1}, As + e) = (Ms)_1] \geq \frac{1}{2} + \frac{\varepsilon}{2},$$

where $(Ms)_1$ denotes the first coordinate of Ms . Call such a triple (A, s, e) good for $\mathcal{M}$.

- (c) (7 pts) Consider the distribution $\mathcal{M}$ obtained by sampling a uniform nonzero vector $r \in \mathbb{Z}_2^n$, using it as the first row of M , and completing it to an invertible matrix in a deterministic canonical way.

Assume that (A, s, e) is good for $\mathcal{M}$. Show how to use P , A , and $As + e$ to construct an oracle $\tilde{L}$ such that

$$\Pr_{r \leftarrow U_n} [\tilde{L}(r) = \langle r, s \rangle] \geq \frac{1}{2} + \frac{\varepsilon}{2}.$$

For the query $r = 0^n$, define $\tilde{L}(r) = 0$.

- (d) (7 pts) Complete the proof by constructing the required algorithm B that recovers s .
4. In class, we've seen the GGM PRF, where both the key s and the input x were of length n . We would like to extend this construction so that for keys $s \in \{0, 1\}^n$, we can apply the function for inputs $x \in \{0, 1\}^*$ of arbitrary length.

- (a) (14 pts) Consider applying the GGM function as is to inputs of arbitrary length. That is, for any $x \in \{0, 1\}^*$, let ℓ be the length of x , let G be a length-doubling PRG, and define

$$F_s(x) := G_{x_\ell}(G_{x_{\ell-1}}(\cdots G_{x_2}(G_{x_1}(s)) \cdots)) .$$

Show that F is not a PRF. (Recall that $G_0(s)$ and $G_1(s)$ denote the first and second n -bit blocks of the output, respectively.)

- (b) (14 pts) Consider the following variant of GGM. Let $G : \{0, 1\}^n \rightarrow \{0, 1\}^{3n}$ be a length-tripling PRG, and let $G_0(s), G_1(s), G_2(s)$ denote its three n -bit output blocks. For any $x \in \{0, 1\}^*$, let ℓ be the length of x and define

$$F_s(x) := G_2(G_{x_\ell}(G_{x_{\ell-1}}(\cdots G_{x_2}(G_{x_1}(s)) \cdots))) .$$

Show that F is a PRF.