CS783: Theoretical Foundations of Cryptography Fall 2024

Assignment 3

September 16, 2024

Instructor: Chethan Kamath

Exercise 1 (MAC and verify oracle)**.** *Recall the definition of EU-CMA security for MAC from Lecture 7 (Definition 2). Now, let's consider a stronger definition, Definition $2'$ where* Tam *is given access (in addition to the* $\mathsf{Tag}(\mathrm{k},\cdot)$ *oracle) to a "verify oracle"* $\mathsf{Ver}(\mathrm{k},\cdot,\cdot)$*, which* Tam *can query on tag and message of her choice. Come up with a MAC that is secure with respect to Definition 2, but not Definition $2'$.*

Exercise 2 (One-way PKE)**.** *Recall the definition of IND-CPA for PKE from Lecture 8. Now consider one-way (OW) CPA , an alternative notion of secrecy for PKEs defined as follows for a PKE* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*

- Eve *is given* pk, *generated as* $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{Gen}(1^n)$.
- *For* $m \leftarrow \mathcal{M}_n$*,* Eve *is given* $c \leftarrow \mathsf{Enc}(\mathrm{pk}, m)$ *as the challenge ciphertext.*
- Eve *outputs* m' *and breaks if* $m' = m$.

A PKE Π is OW-CPA-secure if for all PPT eavesdroppers Eve*, the probability with which* Eve *breaks Π as above is negligible. Now answer the following questions about IND-CPA and OW-CPA.*

1. *Show formally that IND-CPA implies OW-CPA. That is,* any *PKE that is IND-CPA-secure is also OW-CPA-secure.*
2. *What about the opposite direction? Show either that*
   (a) *OW-CPA implies IND-CPA; or*
   (b) *Come up with a counterexample, i.e., a PKE Π that is OW-CPA-secure but* not IND-CPA*-secure.*

Exercise 3 (Amplification via random self-reducibility (RSR))**.** *In Lecture 8 we saw how RSR can be exploited beat the hybrid argument. In this exercise, we exploit RSR of DDH (Lecture 8, Assumption 2) and QR (Lecture 9, Assumption 3) to* amplify *distinguishing advantage.*

1. *Consider the following seemingly stronger variant of DDH, named Assumption $2'$ where we require the distinguishing advantage for every PPT adversaries to be exponentially-close to 0: The DDH assumption holds in $\mathbb{G}$ w.r.to* S *if for all PPT distinguishers* D *(and large enough n)*

$$\left| \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a,b\leftarrow\mathbb{Z}_\ell}}[\mathsf{D}(g^a, g^b, g^{ab}) = 0] - \Pr_{\substack{(\mathbb{G},\ell,g)\leftarrow\mathsf{S}(1^n)\\ a,b,r\leftarrow\mathbb{Z}_\ell}}[\mathsf{D}(g^a, g^b, g^r) = 0] \right| \leq 1/2^n$$

Show that Assumption 2 implies Assumption $2'$. (Hint: invoke the distinguisher for standard DDH multiple times and use Chernoff bound for analysis.)

2. *Define the corresponding Assumption $3'$ for QR, and show that Assumption $3'$ implies Assumption 3.*

Exercise 4 (Gap Diffie-Hellman (DH) Groups). *Recall the definition of DDH and CDH from Lecture 8. A group $\mathbb{G}$ (w.r.to a sampler S) is said to be a* gap DH group *if DDH is easy but CDH is hard in $\mathbb{G}$. Note that DH key exchange is* insecure *in gap DH groups. In the following two groups, CDH is believed to hold. Show that DDH is easy for both groups and hence they constitute gap DH groups.*

1. *$\mathbb{Z}_p^\times$, the multiplicative group modulo prime p. (Hint: Analyse what happens to "squareness" in the real world and random world.)*

2. *A group $\mathbb{G}$ of prime-order p equipped with a* bilinear pairing, *i.e., an efficiently computable function $\mathrm{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ for some "target group" $\mathbb{G}_T$ of order p such that:*

   (a) Bilinear*: for every $g_1, g_2 \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, $\mathrm{e}(g_1^a, g_2^b) = \mathrm{e}(g_1, g_2)^{ab}$.*

   (b) Non-degenerate*: If g is a generator for $\mathbb{G}$ then $\mathrm{e}(g, g)$ is a generator for $\mathbb{G}_T$.*

Exercise 5 (Understanding LWE). *In this exercise, we will try to develop a better understanding of the LWE assumption.*

1. *Recall the definition of DLWE (Assumption 2) from Lecture 10. Now consider the following "worst-case" version of the assumption, which we will denote Assumption $2'$. The (n, m, p, E)-DLWE assumption holds with respect to* worst-case *secrets $\bar{s}$ if for all QPT distinguishers D and* all *$\bar{s} \in \mathbb{Z}_p^n$ the following is negligible*

$$\delta(n) := \left| \Pr_{\substack{\bar{A} \leftarrow \mathbb{Z}_p^{n\times m} \\ \bar{e} \leftarrow \mathrm{E}^m}} [\mathsf{D}(\bar{A}, \bar{s}^\top \bar{A} + \bar{e}^\top) = 0] - \Pr_{\substack{\bar{A} \leftarrow \mathbb{Z}_p^{n\times m} \\ \bar{r} \leftarrow \mathbb{Z}_p^m}} [\mathsf{D}(\bar{A}, \bar{r}^\top) = 0] \right|.$$

   Show that Assumption $2'$ implies Assumption 2. (Hint: exploit linearity)

2. *Consider the* short integer solution *(SIS) problem:*

   - *Input: $\bar{A} \leftarrow \mathbb{Z}_p^{n\times m}$, with $m \geq \lceil n \log(p) \rceil$*
   - *Solution: non-zero vector $\bar{x} \in \{0, \pm 1\}^m$ in $\bar{A}$'s kernel, i.e., $\bar{A}\bar{x} = \bar{0} \bmod p$*

   Now answer the following questions:

   (a) *A solution is guaranteed to exist. Why?*

   (b) *Show that LWE reduces to SIS.*

Exercise 6 (Strong signatures). *As discussed in Lecture 11, a signature scheme Σ is* strongly *EU-CMA-secure if we relax the requirement for forgery in EU-CMA (Definition 2) from "signature on fresh message" to "fresh signature on any message".*

1. *Formally write down the security definition for strong EU-CMA.*

2. *Show that Lamport's signature is* not *strongly one-time EU-CMA-secure. (Hint: you need to come up with the right OWF.)*

3. *How can you make Lamport's signature strongly one-time EU-CMA-secure? Give a formal proof for your construction. (Hint: use a different primitive in place of OWF.)*