MIT 6.5620/6.875/18.425: Cryptography and Cryptanalysis **Due: Oct. 18, 2023**

Problem Set 3

Total Number of Points: 40.

Collaboration Policy: Collaboration is allowed and encouraged in small groups of at most three students. You are free to collaborate in discussing answers, but you must write up solutions on your own and must specify in your submission the names of any collaborators. Do not copy any text from your collaborators; the writeup must be entirely your work. Do not write down solutions on a board and copy them verbatim into LaTeX; again, the writeup must be entirely your own words and your own work and should demonstrate a clear understanding of the solution. Additionally, you may make use of published material, provided that you acknowledge all sources used. Of course, scavenging for solutions from prior years is forbidden.

Problem 1. Authenticated Encryption. (12 points) Let's say Alice and Bob hope to transmit messages to each other in a *private* and *authenticated* manner.

Let $(\mathsf{Gen}_{\mathsf{Enc}}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure symmetric encryption scheme, and let $(\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Mac}, \mathsf{Ver})$ be an EUF-CMA secure message authentication scheme. *You may assume in this problem that* $(\mathsf{Gen}_{\mathsf{Enc}}, \mathsf{Enc}, \mathsf{Dec})$ *has perfect correctness.*

Alice and Bob share the keys $k_1 \leftarrow \mathsf{Gen}_{\mathsf{Enc}}$ and $k_2 \leftarrow \mathsf{Gen}_{\mathsf{MAC}}$, and they want to transmit the message M. Now, they want to transmit the message M. We need to evaluate the security of the suggested protocols and determine whether each of them is IND-CPA secure and/or EUF-CMA secure, or neither. For both aspects of security, prove security or give a counterexample of why the security might not hold.

- **(a)** (4 points) $\mathsf{Enc}_{k_1}(M \| \mathsf{Mac}_{k_2}(M))$
- **(b)** (4 points) $\mathsf{Enc}_{k_1}(M) \| \mathsf{Mac}_{k_2}(M)$
- **(c)** (4 points) $\mathsf{Enc}_{k_1}(M) \| \mathsf{Mac}_{k_2}(\mathsf{Enc}_{k_1}(M))$

Problem 2. Average case to worst case DDH. (12 points) Let $\mathbb{G}$ be a specific cyclic group of prime order q generated by $g \in \mathbb{G}$. Let $n = \texttt{len}(q)$, be the number of bits required to represent q. Assume that we have an efficient algorithm $\mathcal{A}$ that can distinguish a random **DH** triple from a non-**DH** triple with non-negligible advantage. Mathematically, for $\alpha, \beta, \gamma \leftarrow \mathbb{Z}_q, g \leftarrow \mathbb{G}$ sampled uniformly at random, then

$$\left|\mathbf{Pr}[\mathcal{A}(g, g^\alpha, g^\beta, g^\gamma) = 1] - \mathbf{Pr}[\mathcal{A}(g, g^\alpha, g^\beta, g^{\alpha\beta}) = 1]\right| \geq \frac{1}{p(n)}, \quad (1)$$

for some polynomial $p(n)$. Note that this algorithm requires α, β, γ, g to be sampled at random.

(a) (7 points) Given $\mathcal{A}$, construct an efficient algorithm $\mathcal{B}$ that can distinguish **DH** triples for all inputs with a negligible error rate. Mathematically, $\forall \alpha, \beta, \gamma \in \mathbb{Z}_q$ and $\forall g \in \mathbb{G}$ such that $\gamma \neq \alpha\beta$ and g is not the identity,

$$\left|\mathbf{Pr}[\mathcal{B}(g, g^\alpha, g^\beta, g^\gamma) = 1] - \mathbf{Pr}[\mathcal{B}(g, g^\alpha, g^\beta, g^{\alpha\beta}) = 1]\right| \geq 1 - \mu(n), \quad (2)$$

for some negligible function $\mu(n)$.

(b) (2 points) Given $\mathcal{A}$, construct an efficient algorithm $\mathcal{B}'$ that can distinguish, with non-negligible probability, (g, g^α, g^β) from $(g, g^\alpha, g^{\alpha^2})$ for all $\alpha, \beta \in \mathbb{Z}_q$ and generator $g \in \mathbb{G}/\{\mathit{identity}\}$, given $\beta \neq \alpha^2$.

(c) (3 points) Given $\mathcal{B}'$, construct an efficient algorithm that can distinguish (g, g^α, g^β) from $(g, g^\alpha, g^{1/\alpha})$ for all $\alpha, \beta \in \mathbb{Z}_q$ and generator $g \in \mathbb{G}/\{\mathit{identity}\}$, given $\alpha \neq 0, \beta \neq 1/\alpha$. Here, $1/\alpha$ is the multiplicative inverse of α modulo q.

Problem 3. Circular Security. (10 points) In this problem, we consider a security property (of encryption schemes) called circular security: namely, security even when an adversary is given an encryption of the secret key sk.
One variant of circular security for secret key encryption schemes is defined as follows:

Definition 1 (Circularly Secure SKE) *A secret key encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to be circular secure if for all p.p.t. oracle algorithms* $\mathcal{A}^{\mathcal{O}(\cdot)}$*, we have that*

$$\left| \Pr_{sk \leftarrow_R \mathsf{Gen}(1^n)} [\mathcal{A}^{\mathit{Left}_{sk}(\cdot)}(c^*) = 1] - \Pr_{sk \leftarrow_R \mathsf{Gen}(1^n)} [\mathcal{A}^{\mathit{Right}_{sk}(\cdot)}(c^*) = 1] \right| \leq \mathsf{negl}(n), \tag{3}$$

where $c^* \leftarrow \mathsf{Enc}(sk, sk)$, $\mathit{Left}_{sk}(\cdot)$ *is an oracle that on input* (m_L, m_R) *outputs an encryption of* m_L*, and* $\mathit{Right}_{sk}(\cdot)$ *is an oracle that on input* (m_L, m_R) *outputs an encryption of* m_R.

Think about why this is a reasonable definition and how it is similar to the IND-CPA security discussed in lectures.
An analogous definition for public key encryption is as follows.

Definition 2 (Circularly secure PKE) *A public key encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is said to be circularly secure if any p.p.t. algorithm* $\mathcal{A}$ *wins the following game (interacting with a challenger) with probability at most* $\frac{1}{2} + \mathsf{negl}(n)$*:*

(i.) The challenger samples $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$ *and sends* (pk, c^*) *to* $\mathcal{A}$*, where* $c^* \leftarrow \mathsf{Enc}(pk, sk)$ *is a ciphertext where the message is the secret key.*

(ii.) $\mathcal{A}$ *sends two messages* (m_0, m_1) *to the challenger.*

(iii.) The challenger selects $b \leftarrow_R \{0,1\}$ *and sends* $c_b \leftarrow \mathsf{Enc}(pk, m_b)$ *to* $\mathcal{A}$.

(iv.) $\mathcal{A}$ *outputs a bit* $\tilde{b}$*. We say that* $\mathcal{A}$ *wins if* $\tilde{b} = b$.

(a) (6 points) It turns out that not every IND-CPA secure public key encryption scheme is also circularly secure. Construct a public-key encryption scheme which is IND-CPA secure but not circularly secure, relying only on the existence of public-key encryption schemes. Prove that your scheme is IND-CPA secure but not circularly secure.

(b) (4 points) In this part, you will show that a variant of the LWE-based secret key encryption we saw in class does satisfy circular security (under an LWE-like assumption). In particular, we consider a variant of the LWE problem where the secret s is a uniformly random binary string.

Definition 3 (LWE* assumption) *The LWE* assumption with error distribution* χ *states that the following two distributions are computationally indistinguishable:*

$$\{\mathbf{s} \leftarrow_R \{0,1\}^n, \mathbf{A} \leftarrow_R \mathbb{Z}_q^{n\times m}, \mathbf{e} \leftarrow \chi^m : (\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)\} \approx_c \{\mathbf{A} \leftarrow_R \mathbb{Z}_q^{n\times m}, \mathbf{b} \leftarrow_R \mathbb{Z}_q^m : (\mathbf{A}, \mathbf{b}^T)\}. \tag{4}$$

Under the LWE* assumption (with m any polynomial in n, and with error distribution χ), prove that the n bit encryption scheme defined by

$$\mathsf{Enc}(\mathbf{s} \in \{0,1\}^n, \mathbf{m} \in \{0,1\}^m; \mathbf{R} \leftarrow_R \mathbb{Z}_q^{n\times m}, \mathbf{e} \leftarrow \chi^m) = \left(\mathbf{R}, \mathbf{s}^T\mathbf{R} + \mathbf{e}^T + \left\lfloor \frac{q}{2} \right\rfloor \mathbf{m}^T\right) \quad (5)$$

is a circularly secure secret key encryption scheme.

Hint. Show that it is possible to generate an encryption of $\mathbf{s}$ given only an encryption of 0.

Problem 4. Pseudorandom Public Key Encryption (6 points) Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure public-key encryption scheme, $\mathcal{F}_n = \{f_k : \{0,1\}^n \to \{0,1\}^l\}_{k\in\{0,1\}^n}$ be a pseudorandom function (PRF) family, and $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. You may assume that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has perfect correctness. Determine whether the following $(\mathsf{Gen}', \mathsf{Enc}')$ encryption schemes are INDCPA-secure. Either prove the security and construct a decryption algorithm or construct a counterexample that breaks the security.

Assume that the output length of G and $\mathcal{F}$ has the appropriate length for Enc' to be well-defined.

(a) (2 points) $\mathsf{Gen}'(1^n) = \mathsf{Gen}(1^n)$ and $\mathsf{Enc}'(pk, m; r) = \mathsf{Enc}(pk, m; G(r))$.

(b) (2 points) $\mathsf{Gen}'(1^n) = \mathsf{Gen}(1^n)$ and $\mathsf{Enc}'(pk, m; s) = \mathsf{Enc}(pk, m; f_s(m))$.

(c) (2 points) $\mathsf{Gen}'(1^n; \rho||s) = (pk\|s, sk)$, where $\mathsf{Gen}(1^n; \rho) = (pk, sk)$, and $\mathsf{Enc}'(pk\|s, m) = \mathsf{Enc}(pk, m; f_s(m))$.