Signal – Homework

Please answer the following questions. **We don't expect formal proofs: rather, just a high-level argument from intuition.** Please submit your answers as a **PDF** to Gradescope. Collaboration is allowed and encouraged, but you must write up your own answers and acknowledge your collaborators in your submission.

Due Date: *Wednesday, February 12th.*

Review of Security Definitions

We first briefly review the various security definitions covered in class.

- **Chosen Plaintext Attack (CPA)** security for an *encryption scheme*: An encryption scheme is CPA-secure if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$ who can query for encryptions of arbitrary messages, $\mathcal{A}$ cannot distinguish between an encryption of m_0 and an encryption of m_1. All the messages and m_0, m_1 are chosen by $\mathcal{A}$.

- **Chosen Ciphertext Attack (CCA)** security for an *encryption scheme*: An encryption scheme is CCA-secure if for any PPT adversary $\mathcal{A}$ who can query for encryptions of arbitrary messages as well as decryptions of arbitrary ciphertexts, $\mathcal{A}$ cannot distinguish between an encryption of m_0 and an encryption of m_1. All the messages, ciphertexts, and m_0, m_1 are chosen by $\mathcal{A}$, with the only restriction that the queried ciphertexts cannot be the challenge ciphertext.

- **Unforgeability** for an *encryption scheme*: An encryption scheme is unforgeable if for any PPT adversary $\mathcal{A}$ who can query for encryptions of arbitrary messages, $\mathcal{A}$ cannot generate a new valid ciphertext c that decrypts to a message m where m has never been queried by $\mathcal{A}$ before.

- **Chosen Message Attack (CMA)** security for a *message authentication code (MAC)* or *digital signature scheme*: a MAC (resp. digital signature) scheme is CMA-secure if for any PPT adversary $\mathcal{A}$ who can query for tags (resp. signatures) of arbitrary messages, $\mathcal{A}$ cannot generate a new valid message-tag (resp. message-signature) pair (m, t) where m has never been queried by $\mathcal{A}$ before.

- **Strong CMA** security for a *message authentication code (MAC)* or *digital signature scheme*: a MAC (resp. digital signature) scheme is CMA-secure if for any PPT adversary $\mathcal{A}$ who can query for tags (resp. signatures) of arbitrary messages,

$\mathcal{A}$ cannot generate a new valid message-tag (resp. message-signature) pair (m, t) where the pair (m, t) has never appeared in $\mathcal{A}$'s queries before.

1 Computational Security

Recall the distinction between perfect (information-theoretic) security and computational security that we discussed in class.

(1) In your own words, explain what is computational security and why we introduced this notion.

(2) When we say a cryptosystem sets the computational security parameter as $\lambda = 128$ (or achieves 128-bit security), what does it mean?

2 Cryptographic Schemes

(1) Why isn't the plain RSA encryption scheme CPA-secure?

(2) Why is the ElGamal encryption scheme CPA-secure?

(3) Why isn't the plain RSA signature scheme CMA-secure? Why does adding a cryptographic hash function make it CMA-secure?

3 Authenticated Encryption

Given a CPA-secure symmetric-key encryption scheme $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and a strongly CMA-secure MAC scheme $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Mac}_2, \mathsf{Vrfy}_2)$, we try to construct an authenticated encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

(1) Describe the three constructions: Encrypt-and-MAC, Mac-then-Encrypt, and Encrypt-then-MAC.

(2) Why isn't Encrypt-and-MAC necessarily CPA-secure?

(3) Why isn't Mac-then-Encrypt necessarily CCA-secure?

(4) (Extra Credit) Why is Encrypt-then-MAC both CCA-secure and unforgeable?

4 Potential Attacks

In this question, we exploit potential attacks on the Signal project.

(1) **Man-in-the-Middle (MitM) Attack.** Our protocol ensures that two parties can establish shared secret keys, but it does *not* ensure that they know exactly who they are talking to. Indeed, an adversary could pretend to be who they are talking to. Describe a man-in-the-middle attack that compromises the security.

(2) **Replay Attack.** Our protocol is *not* entirely secure against replay attacks. In particular, once a secure channel is established, the same encrypted messages could be sent multiple times (before the parties switch to a new key). For instance, consider an application that upon receiving a suitable message, will send a dollar to charity. Describe a replay attack that exploits this system, and propose a mechanism for protecting against this attack.