CSE 208: Advanced Cryptography (Fall 2023)

Problem Set 2

Lecturer: Daniele Micciancio **Due:** *Tue October 17, 2023*

This homework assignment explores security properties of homomorphic encryption schemes that go beyond the basic notion of IND-CPA security. Informally, a homomorphic encryption scheme is *function-private* if it hides not only the encrypted messages, but also the homomorphic computations performed on them. A scheme is *sanitizable* if it is possible to re-randomize ciphertexts, to produce a distribution that depends only on the encrypted message. In this homework assignment, we will use the following formal definitions.

Definition 1 (Sanitization) *Let* $\mathbf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a public key encryption scheme. We say that* **PKE** *is* sanitizable *if there is an efficient (probabilistic polynomial time) algorithm* San *mapping ciphertexts to ciphertexts, such that for any pair of keys* $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(\kappa)$*,*

- *for any ciphertext* c*, if* $\mathsf{Dec}(\mathsf{sk}, c) \neq \perp$*, then* $\mathsf{Dec}(\mathsf{sk}, \mathsf{San}(\mathsf{pk}, c)) = \mathsf{Dec}(\mathsf{sk}, c)$
- *for any ciphertexts* c, c'*, if* $\mathsf{Dec}(\mathsf{sk}, c) = \mathsf{Dec}(\mathsf{sk}, c') \neq \perp$*, then* $\mathsf{San}(c) \approx \mathsf{San}(c')$*, i.e., these distributions are statistically close.*[1]

Definition 2 (Function Privacy) *A public key homomorphic encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ *satisfies* (t, ϵ) function privacy *if any (probabilistic, stateful) adversary* $\mathcal{A}$ *running in time at most* t*, has advantage at most* ϵ *in the following decision game* $\Im_b^{fp}$*:*

1. *Choose* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(\kappa)$
2. *Run* $(m_0, m_1, f_0, f_1) \leftarrow \mathcal{A}(\mathsf{pk})$*,*
3. *Check that* $m_0, m_1 \in \mathcal{M}$ *and* $f_0, f_1 \colon \mathcal{M} \to \mathcal{M}$ *are valid messages and functions supported by the encryption scheme,*[2] *and* $f_0(m_0) = f_1(m_1)$*. If not, abort the game.*
4. *Compute* $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$ *and* $c' \leftarrow \mathsf{Eval}(\mathsf{pk}, f_b, c)$*,*

[1] One may relax the definition by requiring these distributions to be only computationally indistinguishable, which is arguably enough in most applications. We require statistical closeness for simplicity, and because known sanitization techniques typically achieve this stronger definition of security. In fact, for the purpose of this homework assignment, you may assume perfect security, i.e., interpret $X \approx X'$ as meaning that the probability distributions are *identical*.

[2] For notational simplicity, we focus on unary functions, but everything is easily extended to functions $f \colon \mathcal{M}^w \to \mathcal{M}$ with an arbitrary number of inputs.

5. *Run* $b' \leftarrow \mathcal{A}(c, c')$ *and output* b'.

There are several variants of the above definitions of sanitizability and function privacy. You are encouraged to explore alternative definitions on your own, and check how different definitional choices affect the following homework problems.

1 Sanitizability implies Function Privacy

Show that any sanitizable homomorphic encryption scheme can be made Function Private. More specifically, assume $\mathbf{FHE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ is sanitizable, with sanitization algorithm San, IND-CPA secure, and it satisfies the homomorphic property

$$\mathsf{Dec}(\mathsf{sk}, \mathsf{Eval}(\mathsf{pk}, f, \mathsf{Enc}(\mathsf{pk}, m))) = f(m)$$

for all keys $(\mathsf{sk}, pk) \leftarrow \mathsf{Gen}(\kappa)$, messages $m \in \mathcal{M}$ and functions $f \in \mathcal{F}$. Use $\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{San}$ to define a (possibly different) homomorphic encryption scheme $\mathbf{FHE}'$ (with the same message space $\mathcal{M}$ and functions $\mathcal{F}$), and prove that $\mathbf{FHE}'$ is still $\mathcal{F}$-homomorphic, IND-CPA secure, and also function private.

2 Sanitizability implies Full Composability

Show that any encryption scheme that is sanitizable and homomorphic on sanitized ciphertext, can be transformed into a (possibly different) scheme that is fully composable. More specifically, assume $\mathbf{FHE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ is sanitizable, with sanitization algorithm San, IND-CPA secure, and it satisfies the homomorphic correctness property

$$\mathsf{Dec}(\mathsf{sk}, \mathsf{Eval}(\mathsf{pk}, f, c)) = f(m)$$

for all ciphertexts $c = \mathsf{San}(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, m))$, message $m \in \mathcal{M}$, and function $f \in \mathcal{F}$.[3] Use $\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{San}$ to define a (possibly different) $\mathbf{FHE}'$ scheme, and prove that $\mathbf{FHE}'$ is still valid, IND-CPA secure, and fully composable, with the same message space $\mathcal{M}$ and functions $\mathcal{F}$.

[3] As usual, for notational simplicity, we assumed $\mathcal{F}$ is a set of unary functions. You can adapt the problem to functions with an arbitrary number of inputs.