Week 3

Nadav Kohen

July 9, 2025

This week has a little less content volume than last week, so I want to encourage you to also review and become more comfortable with the Week 2 document and its exercises as part of this week's assignment.

Now that we have a little bit of experience working with security definitions using attack games and probabilities, our goal this week is to make all of the details rigorous to pave the way for the study of the security of Schnorr digital signatures, which we will continue next week.

The primary missing piece in our formalism from last week is the definition of the notion that a probability is "negligible." Recall that this notion was central to all of our security definitions, which were all the result of requiring all advantage values to be negligible.

Reading 1. *Read about negligible functions and probabilities in:*
Mike Rosulek - The Joy of Cryptography - pages 67-71.

In Reading 1, we encountered the following two equivalent definitions of what it means for a function, f, to be negligible:

- For all polynomials, p, $\lim_{\lambda\to\infty} p(\lambda)\cdot f(\lambda) = 0$.
- For all natural numbers, c, $\lim_{\lambda\to\infty} \lambda^c \cdot f(\lambda) = 0$.

The following are three additional equivalent definitions:

- For all polynomials, p, here exists a natural number, N, such that for all $\lambda > N$, $|f(\lambda)| \leq \frac{1}{|p(\lambda)|}$.
- For all polynomials, p, here exists a natural number, N, such that for all $\lambda > N$, $\frac{1}{|f(\lambda)|} \geq |p(\lambda)|$.
- For all natural numbers, c, here exists a natural number, N, such that for all $\lambda > N$, $\frac{1}{|f(\lambda)|} \geq |\lambda^c|$.

All three of these statements are more-or-less equivalent to the statement that f grows smaller faster than the reciprocal of any polynomial, or equivalently that the reciprocal of f grows larger faster than any polynomial. From this perspective, I hope that it is clear that the first two definitions from the reading are also capturing this idea. With this intuition in mind,

Exercise 1. *Prove that a function, f satisfying any one of the above properties satisfies all of the above properties.*

You may now use any of these definitions interchangeably as it suits you.

Exercise 2. *The final page of Reading 1 has exercises demonstrating properties of negligible functions. Complete Exercises 4.2, 4.3(a), 4.3(b), 4.4 and 4.5.*

Exercise 3. *Now that we have some more comfort with the formal definition of negligible, double-check, for rigor, your solutions to Exercises 2 and 8 from last week.*

One last note on our formal model for proving cryptographic security is that the adversary is not allowed to be an arbitrary program, but rather we will require it to be a Probabalistic Polynomial Time (PPT) program. In addition to allowing our adversaries to have access to randomness (hence, probabalistic) this also means that the number of steps in any execution of $\mathcal{A}$ must be bounded by some polynomial, $p(\lambda)$. This assumption is not only sensical and

practical, but it is also necessary for our definition of negligible to work because it ensures that our adversary cannot turn a negligible success probability into a non-negligible one by brute force (for example, the adversary may not sample a non-negligible proportion of all possible private keys).

Let us now begin our study of Schnorr signatures, beginning with the definition of security of a signature scheme: (keep in mind that an "oracle" in cryptography is simply a program that all other programs have access to as an interface that takes an input and returns an output, but no party has access to any information about the source code of this program beyond the specification; also note that a PPT adversary can make at most a polynomial-bounded number of queries to any oracle)

Reading 2. *Read about the definition of Existentially UnForgable under Chosen Message Attack (EUF-CMA) in:*
Jonathan Katz and Yehuda Lindell - Introduction to Modern Cryptography - pages 463-468.

Note that when Kats and Lindell refer to n, they are talking about the security parameter, which we have been calling λ. To have some practice with this definition,

Exercise 4. *Let (G, S, V) be a secure signature scheme with the message space $\{0,1\}^\lambda$. Let $\hat{G}$ be a new key generation function that simply calls G twice and returns a pair of secret keys, (sk_0, sk_1), and the corresponding pair of public keys, (pk_0, pk_1). Which of the following signature schemes, $(\hat{G}, \hat{S}, \hat{V})$, are secure? Show an attack or prove security (by reduction).*

(a) Prove that "Sign halves" is ***not*** *secure:*

$$\hat{S}((sk_0, sk_1), (m_L, m_R)) = (S(sk_0, m_L), S(sk_1, m_R)),$$

$$\hat{V}((pk_0, pk_1), (m_L, m_R), (\sigma_0, \sigma_1)) = V(pk_0, m_L, \sigma_0) \wedge V(pk_1, m_R, \sigma_1).$$

(b) Show that "Sign with randomness" is ***not*** *secure:*

$$\hat{S}(sk_0, m) = [\textit{choose random } r \in \{0,1\}^\lambda; \textit{output } (r, S(sk_0, m \oplus r), S(sk_0, r))],$$

$$\hat{V}(pk_0, m, (r, \sigma_0, \sigma_1)) = V(pk_0, m \oplus r, \sigma_0) \wedge V(pk_0, r, \sigma_1).$$

(c) Prove that "Accept one valid" is secure:

$$\hat{S}((sk_0, sk_1), m) = (S(sk_0, m), S(sk_1, m)),$$

$$\hat{V}((pk_0, pk_1), m, (\sigma_0, \sigma_1)) = V(pk_0, m, \sigma_0) \vee V(pk_1, m, \sigma_1).$$

(Hint: Consider using that $Pr[\sigma_0 \text{ or } \sigma_1 \text{ is valid}] \leq Pr[\sigma_0 \text{ valid}] + Pr[\sigma_1 \text{ valid}]$ *from Exercise 4 of last week).*

Now we are almost ready to see the Fiat-Shamir Transform (next week), which turns secure identification protocols into secure digitial signature schemes. We will use the Fiat-Shamir Transform to prove the security of the Schnorr signature soon. The only ingredient missing is the Random Oracle Model (ROM), which is how we model our hash functions to make proofs more practical:

Reading 3. *Read about the Random Oracle Model in:*
Jonathan Katz and Yehuda Lindell - Introduction to Modern Cryptography - pages 187-191.

One strange but important feature of the ROM discussed in the section "Definitions and Proofs in the ROM" is that during a reduction, adversaries $\mathcal{A}$ must "report" all of their oracle queries to the adversary $\mathcal{A}'$ that is using $\mathcal{A}$ as a subroutine, and additionally $\mathcal{A}'$ may adaptively control the response that $\mathcal{A}$ gets to these queries so long as $\mathcal{A}$ cannot distinguish what they receive from a regular random oracle. This kind of reporting feature is also key to other models we will discuss in the future.

Next week, we will use the Random Oracle Model (ROM) to construct the Fiat-Shamir transform, and then we will dive straight into proving that the Schnorr digital signature is secure!