Cryptographic Secret Sharing

Girls Talk Math

Introduction

In this problem set, you will learn about ...

One last note about reading mathematical texts: it is very normal when reading math to read a passage or even a single sentence several times before understanding it properly. Also, never trust the author! Check every claim and calculation (time permitting). Take your time and never give up. Let's talk math!

Contents

1 Probability and Randomness

1.1 Introduction

1.2 Randomness in Cryptography

(NG: Define *information-theoretic security*. Define what a security parameter is (λ).)

1.3 Sharing Secrets

Secret sharing is a way to "split" a secret value (call it s) into pieces. When we distribute those pieces among a large set of people, and some subset (or maybe the whole set) can recover the secret only if they pool their information (their shares).

(NG: Define the privacy property and the cryptographic privacy game? The goal can be to have a (bonus) exercise in which they write a real cryptographic proof of privacy of a secret sharing scheme (likely the XOR scheme).)

2 A simple secret sharing

2.1 Binary Arithmetic

The exclusive-OR (XOR) operation is denoted by the symbol $\oplus$ and defined by the following truth table:

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

(NG: explain binary representations of numbers and binary arithmetic.)

2.2 Sharing Secrets using XOR

$\underline{\mathsf{Share}(s)}$
$s_1 \leftarrow\!\!\$\ \{1, \ldots, 2^\lambda\}$
$\mathsf{return}\ (s_1, s \oplus s_2)$

$\underline{\mathsf{Reconstruct}(s_1, s_2)}$
$\mathsf{return}\ s_1 \oplus s_2$

2.2.1 Proving Security*

(NG: Optional section. Introduce the privacy game, have them act as the adversary and try to beat the privacy and get some intuition about why it's hard, then work through a simple proof.)

3 Shamir's Secret Sharing

3.1 Polynomials

(NG: y-intercept, zeroes)

3.1.1 Uniqueness

(NG: How many points uniquely define a polynomial)

3.1.2 Lagrange Interpolation

Exercise 3.1 (NG: Practice some manual Lagrange interpolation. Pick a polynomial, evaluate it at 3 points, then use those 3 points in Lagrance Interpolation and recover the polynomial.)

3.2 Sharing Secrets Using Polynomials

Shamir secret sharing is a $(t+1)$-out-of-n secret sharing protocol, for some numbers t and n. This means that we split the secret s into n values and distribute them to n people. Then, at least $t+1$ of those people must work together to recover s.

(NG: Don't introduce finite fields but maybe make a note that this should be done over finite fields.)

(NG: Use the Jupyter Notebook to play around with this.)