Homework 7

Due: Nov 10, 2023

CS 1510: Intro. to Cryptography and Computer Security

1 Group Properties

Let $(\mathbb{G}, \cdot)$ be a group. Prove the following:

a. There is a unique identity in $\mathbb{G}$.

b. Every element $g \in \mathbb{G}$ has a unique inverse.

c. Prove that the RSA group, or $\mathbb{Z}_n^* = \{a \in \{1, 2, ..., N-1\} \mid \texttt{gcd}(a, N) = 1\}$, is an abelian group under multiplication modulo N.

2 CRHF from the Discrete Logarithm Assumption

Let $\mathcal{G}$ be a polynomial-time algorithm that, on input 1^n, outputs a (description of) cyclic group $\mathbb{G}$, its order q (which is prime), and a generator g. Define a fixed-length hash function (Gen, H) as follows:

- Gen: On input 1^n, run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$ and then select uniform random $h_1, \ldots, h_t \xleftarrow{\$} \mathbb{G}$. Output $s := \langle \mathbb{G}, q, g, (h_1, \ldots, h_t) \rangle$ as the key.
- H: Given a key $s = \langle \mathbb{G}, q, g, (h_1, \ldots, h_t) \rangle$ and input $(x_0, x_1, \ldots, x_t)$ with $x_i \in \mathbb{Z}_q$, output $H_s(x_0, x_1, \ldots, x_t) := g^{x_0} \cdot \prod_{i=1}^{t} h_i^{x_i}$.

Prove that if the discrete logarithm problem is hard relative to $\mathcal{G}$, then for any t, this construction is a fixed-length collision-resistant hash function.

3 CPA-Secure PKE

Consider the following public-key encryption scheme. The public key is $(\mathbb{G}, q, g, h)$ and the secret key is x, generated exactly as in the El Gamal encryption scheme. To encrypt a bit $m \in \{0, 1\}$ (the messages space is $\mathcal{M} = \{0, 1\}$):

- If $m = 0$, then choose a uniform $y \xleftarrow{\$} \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := h^y$. The ciphertext is $c = \langle c_1, c_2 \rangle$.

- If $m = 1$, then choose independent uniform $y, z \xleftarrow{\$} \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := g^z$. The ciphertext is $c = \langle c_1, c_2 \rangle$.

a. Show how to decrypt a ciphertext c given the secret key x.

b. Prove that this encryption scheme is CPA-secure if DDH is hard relative to $\mathcal{G}$.

4 Fair Coin Tossing Using PKE

Consider the following protocol for two parties Alice and Bob to flip a fair coin:

1. A trusted party Charlie publishes his public key pk for a public-key encryption scheme.
2. Alice chooses a uniform random bit $b_A \xleftarrow{\$} \{0,1\}$, encrypts it using pk, and announces the ciphertext c_A to Bob and Charlie.
3. Bob acts symmetrically and announces a ciphertext c_B.
4. Finally, Charlie decrypts both c_A and c_B and publishes the results b_A and b_B, and the parties XOR the results to obtain the value of the coin, namely $b := b_A \oplus b_B$.

a. Argue that even if Alice is dishonest (but Bob is honest), the final value of the coin is uniformly distributed.

b. Assume the parties use El Gamal encryption (where the bit b is encoded as the group element g^b before being encrypted – note that efficient decryption is still possible). Show how a dishonest Bob can bias the coin to any value he likes.

5 Attacking the RSA Trapdoor Permutation

We saw in class how RSA is a candidate trapdoor permutation with the following algorithms:

- **Key generation**: $\mathsf{KeyGen}(1^k)$ picks two k-bit primes p and q. Let $N = pq$. Find e that is co-prime $\varphi(N) = (p-1)(q-1)$, where φ is Euler's totient function. Let d be such that $ed \equiv 1 \mod \varphi(N)$. Output $pk = (N, e)$ and $sk = d$.
- **Evalution**: $\mathsf{Eval}(pk, x)$ checks if $x \in \mathbb{Z}_N^\star$, and if so, outputs $x^e \mod N$. Otherwise, it fails.
- **Inversion**: $\mathsf{Invert}(pk, sk, y)$ checks if $y \in \mathbb{Z}_N^\star$, and if so, outputs $y^d \mod N$. Otherwise, it fails.

We will denote the TDP instantiated by $(N, e) \leftarrow \mathsf{KeyGen}(1^k)$ as $f_{N,e}$. Evaluating the TDP is $f_{N,e}(x) = \mathsf{Eval}((N, e), x) = x^e \mod N$. We will now see how this TDP is vulnerable to certain types of attacks.

a. We say that a function f is *malleable* if given the value of $f(x)$, you can compute the value of $f(g(x))$ for some function g of your choice, without knowing x. Prove that $f_{N,e}$ is malleable. In particular, show that given the value of $f_{N,e}(x)$, it is possible to compute the value of $f_{N,e}(g(x))$, where $g(x) = c \cdot x$ for a constant c and unknown x. Assume that $g(x) \in \mathbb{Z}_N^*$ so that $f_{N,e}(g(x))$ does not fail.

b. Propose another function $g(x)$ such that $f_{N,e}$ is malleable with respect to g. Explain why.

6 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. You will be permitted to use this one-page resource (along with the other weeks' resources) on the midterm and final.

Changes to this document prior to the exams are permitted, but for each change, you will be asked to state what you changed and why. For example, if you dropped something and replaced it with something else, justify why the thing you dropped wasn't as important as the thing you inserted, why you think it might be more useful for the exam, etc.

Please note that the purpose of this question is to help you organize and synthesize the material for your own future use. It will be graded based on completion—we will not be checking it for correctness.