VE475 project presentation: Random Oracle Model

Project Group 12

July 20, 2021

Idea of Random Oracle Model

Basic Definition

Two kinds of definitions:

- An oracle that responds to every unique query with a random response chosen uniformly from its output domain.
- A mathematical function chosen uniformly at random and mapping each possible query to a random response from its output domain

Idea of Random Oracle Model

Basic Definition

Two kinds of definitions:

- An oracle that responds to every unique query with a random response chosen uniformly from its output domain.
- A mathematical function chosen uniformly at random and mapping each possible query to a random response from its output domain

Basic Information

- First used for rigorous cipher proof in a 1993 publication by Mihir Bellare and Phillip Rogaway(1993)
- Used to prove the system security

Basic Property

The ideal random oracle model follows the three basic property:

Properties

- Consistency
- Calculability in polynomial time complexity
- Uniform Distribution

Motivating Scenario

Considering the following scenario:

Scenario

- Alice wants to publish a puzzle in the magazine.
- Alice attaches a string c so that the readers can solve the puzzle to verify that they have the right solution.
- Alice hopes the string c won't give away partial information about the solution x to readers who have not solved the puzzle themselves.

Solution

Thus, what is the ideal solution for Alice?

Solution

Thus, what is the ideal solution for Alice?

Solution

- Alice designs a random oracle R, where $c = R(x)$.
- It is easy to verify that $c = R(x)$.
- However, as long as the correct x is not found, $R(x)$, as a completely random string, gives no information about x.

The Definition of Three Levels of Protection

There is one situation in cryptography that the application of cryptography is required to prevent everyone including the user from understanding the crypt and thus breaking it. This case raises the definition of three levels of protection.

Signature schemes

- Authentication schemes: A can prove to B that he is A, but someone else cannot prove to B that he is A.
- Identification schemes: A can prove to B that he is A, but B cannot prove to someone else that he is A.
- Signature schemes: A can prove to B that he is A, but B cannot prove even to himself that he is A.

Practical Application

The process of the verification of the unforgeable ID cards is as follows:

Process

- Generate a random hash function
- The secure code is generated by inputting the personal information of the card owner to the random hash function.
- During the authentication, the verifier only receives the personal information string from the prover to generate a sequence for authentication and generate the output by the random hash function.

Difficulty of finding the pseudo-random-behavior function/algorithm

The Random Oracle can be mainly replaced by two kinds of functions: single hash function and hash function ensemble.

Analysis for single hash function

- The computability feature requires the time to perform the function to be within the range of a polynomial time complexity.
- It will be hard to generate the outputs which do not leak any partial information by using a single function to perform in the polynomial time complexity.

Analysis for hash function ensemble

Analysis for hash function ensemble

- Still, the computability feature requires the time to perform the function to be within the range of a polynomial time complexity.
- Since the behavior of hash function is always determined once we constructed the system, if we constantly input the inputs with some relativities, the correlation between their output will still be tractable.