Random Oracle Model summary

donderdag 19 januari 2023 21:39

Attack goals

Full break (FB)	A can compute secret key
Universal forgery (UU)	A can forge a signature for any message
Selective forgery (SU)	A can forge a signature for a message chosen before the start of the attack
Existential forgery (EU)	A can forge a signature for an arbitrary message for which the signature was not obtained from an oracle during the attack

Attack models

Key-only attack (KOA)	A only gets the public key
Random message attack (RMA)	A gets the public key & signatures on a set of random messages
Adaptively chosen message attack (CMA)	A learns the public key and is allowed to adaptively ask for the signatures on messages of its choice

Note: *'adaptively'* means that the attacker can make their choice based on the target; that is, they may choose what oracle queries they make after obtaining the target.

Attacks on RSA-based schemes

- In textbook RSA, encrypting a random string σ produces a message M for which σ is a valid signature.
- Similarly, due to homomorphic properties, the product of two signatures is a valid signature on the product of the messages.
- In a blinding attack, the true message to be signed is hidden by multiplying the message to be signed by r^e, for some random r. This r contributes a factor $r^{ed} = r \bmod n$ to the signature, which can then be divided out.
- A scheme in which the hash of a message is signed is vulnerable to index calculus attacks.

Random oracle model

In the ***standard model***, it is assumed that a building block has a property P, which is then used in a reduction. In an ***idealized model***, it is assumed that a building block behaves perfectly; the building block is replaced by an oracle in a reduction.
The random oracle model replaces hash functions with a random oracle, which always returns a uniform random (but consistent) result. It can be implemented in theory by *'lazy sampling'*: returning the result if it stored, and returning a randomly sampled value (which is then stored) if the result is not yet stored. The random oracle model is a heuristic model.

RSA-FDH

RSA Full Domain Hash (RSA-FDH) is a signature scheme where the hash function maps to the entire domain of the RSA group. This ensures the space of possible hashes is sufficiently large to prevent index calculus attacks.