Sponge: Anonymous Communication without Onion Encryption

May 17, 2016

1 Notation

- Let λ be the security parameter.
- Let H be a cryptographic hash function with output size λ.
- Let F_k be a PRF with key k and output size λ.
- Let Cr, R, and P be a consumer, router, and producer, respectively.
- Let $I(N, s)$, $P(N, s)$, and $C(N)$ be an interest, push interest, and content object, respectively with the name N and nonce s.

2 Main Goal

The desired security goal is that for a given name N, the probability for any probabilistic polynomial time adversary to distinguish the transformed version of N – $T(N)$ – from a random string is negligible (in something). This implies that the distribution $(T(N), T(N))$ for a fixed N is computationally indistinguishable from the tuple $(T(N), r)$ for the same N and random r. Here, we assume that $T(N)$ is a probabilistic algorithm.

Assume that a node had some data structure with two procedures: insert and lookup. We do not specify how they are implemented. Let k be the number of unique elements in this data structure at any given point in time. We will prove that their respective runtimes must be $O(1)$ and $O(k)$, respectively.

Theorem 1. *Let D be a data structure as defined above. Its* insert *operation runs in $\Omega(k)$ time.*

Proof. TODO □

Theorem 2. *Let D be a data structure as defined above. Its* lookup *operation runs in $\Theta(k)$ time.*

Proof. TODO □