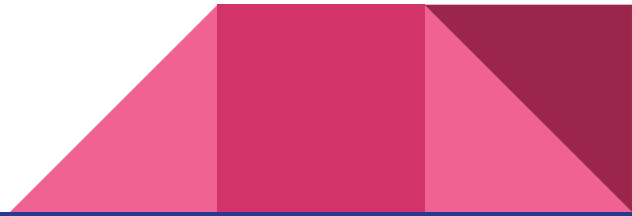
Leftover Hash Lemma (LHL) (without the proof)

Saral Uttamani

Background

- The leftover hash lemma is a lemma in cryptography first stated by Russell Impagliazzo, Leonid Levin, and Michael Luby in 1989.
- For cryptographic, we need ideal randomness, but those are not practical. We often deal with imperfect randomness.
- For most use cases, we must have a min-entropy to deal with this imperfect randomness.



Important Definitions

- Entropy is Randomness. Min-Entropy is defined as
  - For a source n: $Pr[X=x] \leq 2^{-n}$, for all x
- H is universal family of hash functions if for every x,y

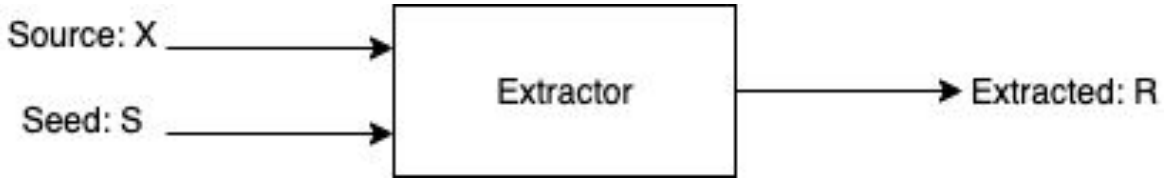
$$x, y \epsilon \{0,1\}^n$$
$$h \epsilon H \text{ where } h : \{0,1\}^n \rightarrow \{0,1\}^m$$
$$\text{then } \mathbb{P}_{h \epsilon H}[h(x) = h(y)] \leq 2^{-m}$$

Random Extractors

A function when applied to a weakly random source, with a uniform random seed, generates a highly random output that appears independent from the source and uniformly distributed.

Input: a weak X and a uniform random seed S.

Output: extracted key R = Ext(X,S)



Leftover Hash Lemma

Universal Hash functions are good extractors.

More formally,

Let X be a random variable with universe U and $H_\infty(X) \geq k$.
Fix $\epsilon > 0$.Let H be a universal hash family of size 2^n with output length $v = k - 2log(1/\epsilon)$.

We define: $Ext(x,h) = h(x)$.

Then Ext is a strong $(k, \epsilon/2)$extractor with seed length n and output length v

Parameter explanation

- k is the lower bound on the entropy of the source.
- Output length = v
- Entropy Loss = L
- Error (epsilon) is the measure of statistical distance from uniform.
- Seed length = n

Optimising parameters

We need to minimise the Entropy Loss

$$L = 2log(1/\epsilon) - O(1).$$

We need to decrease the seed length.

$$n = log|X| + 2log(1/\epsilon) + O(1).$$

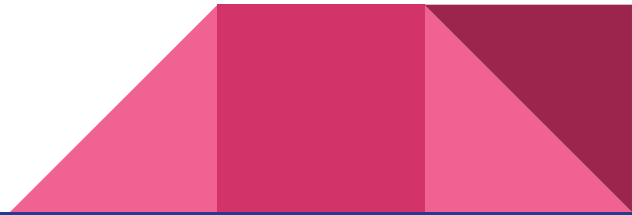
Cryptographic Context and Application

Suppose Alice and Bob share a secret w and want a secret key, but w is not uniform.

For example w could be a password or the result of a Diffie-Hellman key exchange.

They can send a public seed and use an extractor to obtain an almost uniform secret key.

We only require that no single password is too likely. So we can deal with bad distributions.



Brief Proof (for reference)

The proof is comprised of three parts:

1. First we bound the collision probability of the extractor.
2. Then we use this to bound the L2-distance between the extractor’s output and true randomness.
3. Finally, we convert the L2-distance into statistical distance.

References

Leftover hash lemma Wiki

Randomness extractor Wiki

R. Impagliazzo, L. A. Levin, and M. Luby Pseudo-random generation from one-way functions. In Proceedings of the twenty-first annual ACM symposium on Theory of computing (STOC ’89) pages 12-24, 1989.

Extractors and the Leftover Hash Lemma - Scribe by Thomas Steinke, David Wilson