Key Derivation Without Entropy Waste

Yevgeniy Dodis
NYU

9/25/2013 at 11:00 am
CoRE 431

Abstract

We revisit the classical question of converting an imperfect source X of min-entropy k into a usable m-bit cryptographic key for some underlying application P. If P has security delta (against some class of attackers) with a uniformly random m-bit key, we seek to design a key derivation function (KDF) h that allows us to use R=h(X) as the key for P and results in comparable security delta' close to delta. Seeded randomness extractors provide a generic way to solve this problem provided that k > m + 2*log(1/delta), and this lower bound on k (called "RT-bound") is known to be tight in general. Unfortunately, in many situation the "waste" of 2*log(1/delta) bits of entropy is significant, motivating the question of designing KDFs with less waste for important special classes of sources X or applications P.I will discuss several positive and negative results in this regard.

The most surprising of them will be a positive result for all unpredictability applications P, yielding a provably secure KDF with entropy "waste" only loglog(1/delta) - an expenential improvement over the RT-bound.

Organizer(s): Swastik Kopparty and Shubhangi Saraf