Alternating Extraction

supervisor: Krzysztof Pietrzak, pietrzak@cwi.nl

Alternating Extraction. A strong extractor is a function Ext with the property that $[K, \mathsf{Ext}(K, X)]$ is close to uniformly random if K is uniformly random and X has sufficiently high min-entropy. (X has min-entropy k, denoted $H_\infty(X) = k$, if $\Pr[X = x] \leq 2^{-k}$ for every x).
Alternating extraction [2] is a process by which one generates keys $K_1, K_2, \ldots$ by alternatingly extracting from two random variables A, B as

$$K_i = \mathsf{Ext}(K_{i-1}, C) \quad \text{where } C = A \text{ if } i \text{ is odd and } C = B \text{ otherwise.}$$

One can prove that no interactive protocol between two parties holding A and B respectively exists which (for any i) computes K_i unless either the parties exchange i messages or the communication complexity (i.e., the total length of messages exchanged) is very large (such that one party can send almost its entire input to the other).

Goals of the Project. Alternating extraction has some interesting applications in cryptography, most notably [1] described below, and there are many open problems. The goal of this project is to first read and understand [1, 2] – and possibly a few more papers – and then investigate some of the open problems in this area.

On [1]. Consider two parties, we'll call them Alice and Bob, who share a string W, and who can communicate over a public channel like the Internet. "Public" means that we assume that an adversary, we'll call here Eve, has complete control over the channel: she can read and replace any messages as she likes.
If the string is W is uniformly random, and Eve has no information about it, Alice and Bob can use standard cryptographic tools (i.e., encryption and authentication schemes) to turn the public channel into a secure one, where all Eve can do is to block communication, but she will never learn anything about the messages send by Alice or Bob (this is called privacy), nor can she convince Alice that a message is from Bob, unless he really did send it, and vice versa (this is called authenticity).
In many settings, the string W shared between Alice and Bob is not uniformly random, but only has some min-entropy: W has min-entropy k, denoted $H_\infty(W) = k$, if for every possible w, $\Pr[W = w] \leq 2^{-k}$. This is e.g. the case if W is a human memorable password, biometric data, or if W has been subject to some attack. Turning a public channel efficiently into a secure one using only such a weak shared secret W has been a long standing open problem, and has recently been solved [1].

Required Background. Background in information theory and combinatorics is helpful.

References

[1] Yevgeniy Dodis and Daniel Wichs. One-round authenticated key agreement from weak secrets. Cryptology ePrint Archive, Report 2008/503, 2008. http://eprint.iacr.org/.

[2] Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *FOCS*, pages 227–237, 2007.