Cryptology ePrint Archive: Report 2013/105

Lossy Chains and Fractional Secret Sharing

Yuval Ishai and Eyal Kushilevitz and Omer Strulovich

Abstract: Motivated by the goal of controlling the amount of work required to access a shared resource or to solve a cryptographic puzzle, we introduce and study the related notions of {\em lossy chains} and {\em fractional secret sharing}.

Fractional secret sharing generalizes traditional secret sharing by allowing a fine-grained control over the amount of uncertainty about the secret. More concretely, a fractional secret sharing scheme realizes a fractional access structure $f:2^{[n]}\to [m]$ by guaranteeing that from the point of view of each set $T\subseteq [n]$ of parties, the secret is {\em uniformly} distributed over a set of $f(T)$ potential secrets. We show that every (monotone) fractional access structure can be realized. For {\em symmetric} structures, in which $f(T)$ depends only on the size of T, we give an efficient construction with share size $poly(n,\log m)$.

Our construction of fractional secret sharing schemes is based on the new notion of {\em lossy chains} which may be of independent interest. A lossy chain is a Markov chain $(X_0,\ldots,X_n)$ which starts with a random secret X_0 and gradually loses information about it at a rate which is specified by a {\em loss function} g. Concretely, in every step t, the distribution of X_0 conditioned on the value of X_t should always be uniformly distributed over a set of size $g(t)$. We show how to construct such lossy chains efficiently for any possible loss function g, and prove that our construction achieves an optimal asymptotic information rate.

Category / Keywords: foundations / Secret sharing, Markov chains

Publication Info: The 30th Symposium on Theoretical Aspects of Computer Science (STACS 2013)

Date: received 24 Feb 2013

Contact author: yuvali at cs technion ac il