Cryptology ePrint Archive: Report 2013/201

Non-malleable Codes from Additive Combinatorics

Divesh Aggarwal and Yevgeniy Dodis and Shachar Lovett

Abstract: Non-malleable codes provide a useful and meaningful security guarantee in situations where traditional error-correction (and even error-detection) is impossible; for example, when the attacker can completely overwrite the encoded message. Informally, a code is non-malleable if the message contained in a modified codeword is either the original message, or a completely unrelated value. Although such codes do not exist if the family of "tampering functions" \cF is completely unrestricted, they are known to exist for many broad tampering families \cF. One such natural family is the family of tampering functions in the so called {\em split-state} model. Here the message m is encoded into two shares L and R, and the attacker is allowed to arbitrarily tamper with L and R {\em individually}. The split-state tampering arises in many realistic applications, such as the design of non-malleable secret sharing schemes, motivating the question of designing efficient non-malleable codes in this model.

Prior to this work, non-malleable codes in the split-state model received considerable attention in the literature, but were either (1) constructed in the random oracle model [DPW10], or (2) relied on advanced cryptographic assumptions (such as non-interactive zero-knowledge proofs and leakage-resilient encryption) [LL12], or (3) could only encode 1-bit messages [DKO13]. As our main result, we build the first efficient, multi-bit, information-theoretically-secure non-malleable code in the split-state model.

The heart of our construction uses the following new property of the inner-product function <L,R> over the vector space F^n (for any finite field F and large enough dimension n): if L and R are uniformly random over F^n, and $f,g: F^n \rightarrow \F^n are two arbitrary functions on L and R, the joint distribution (<L,R>,<f(L),g(R)>) is ``close" to the convex combination of "affine distributions" {(U,c U+d)| c,d \in F}, where U is uniformly random in F. In turn, the proof of this surprising property of the inner product function critically relies on some results from additive combinatorics, including the so called {\em Quasi-polynomial Freiman-Ruzsa Theorem} (which was recently established by Sanders [San12] as a step towards resolving the Polynomial Freiman-Ruzsa conjecture [Gre05]).

Category / Keywords: applications / Non malleable codes, Combinatorics

Date: received 8 Apr 2013

Contact author: divesha at cs nyu edu