Non Malleable-Codes

January 18, 2010

Perquisites. Some background in coding theory is helpful.

Error-Correction/Detection Codes. A (probabilistic) encoding scheme (or simply code) is a pair of functions $\mathsf{Enc} : \{0,1\}^m \times \{0,1\}^r \to \{0,1\}^n, \mathsf{Dec} : \{0,1\}^n \to \{0,1\}^m$.

Important examples of codes are *error-correcting* and *error-detecting* codes. A code is error-correcting (for distance d) if for any codeword $C = \mathsf{Enc}(M, R)$ and any function $f : \{0,1\}^n \to \{0,1\}^n$ where the Hamming distance[1] of C an $f(C)$ is at most d we have

$$\mathsf{Dec}(f(\mathsf{Enc}(M, R))) = M \ .$$

That is, the decoding recovers the encoded message even if up to d positions in the codeword were flipped.

Non-Malleability. In some settings a weaker security guarantee than correction (or detection) is sufficient. One example is the context of securing cryptosystems against so called "tampering attacks" [1], where it is sufficient to require that the tampered codeword $C' = f(C)$ (for some $C = \mathsf{Enc}(M, R)$) either decodes to the original message, $\mathsf{Dec}(C') = M$, or the decoded message $M' = \mathsf{Dec}(C')$ is independent of the original message M.

This property, called *non-malleability*, is weaker than error-detection, as a consequence, one can construct codes which are non-malleable against classes of tampering functions for which error-detection (and thus also correction) is trivially impossible. A simple example are the constant functions $f_x(C) = x$, a more interesting example are functions where the the ith bit of the tampered codeword $f(C)$ can be any function of the ith bit in the original codeword C.

Goal. In this project the student should first read and understand the definitions and technical results of [1]. In a second phase, the student can either try to extend some of the results from [1]. E.g. coming up with constructions with better rate or for broader classes of tampering functions. Another option is to do read and report on more related literature.

Supervision. Krzysztof Pietrzak

References

[1] S. Dziembowski, K. Pietrzak, D. Wichs Non-Malleable Codes In *ICS*, 2010.

[1] The Hamming distance of two strings is the number of positions in which they differ.