Cryptology ePrint Archive: Report 2013/160

Interactive Coding, Revisited

Kai-Min Chung and Rafael Pass and Sidharth Telang

Abstract: How can we encode a communication protocol between two parties to become resilient to adversarial errors on the communication channel? This question dates back to the seminal works of Shannon and Hamming from the 1940's, initiating the study of error-correcting codes (ECC). But, even if we encode each message in the communication protocol with a ``good'' ECC, the error rate of the encoded protocol becomes poor (namely $O(1/m)$ where m is the number of communication rounds). Towards addressing this issue, Schulman (FOCS'92, STOC'93) introduced the notion of \emph {interactive coding}.

We argue that whereas the method of separately encoding each message with an ECC ensures that the encoded protocol carries the same amount of information as the original protocol, this may no longer be the case if using interactive coding. In particular, the encoded protocol may completely leak a player's private input, even if it would remain secret in the original protocol. Towards addressing this problem, we introduce the notion of \emph{knowledge-preserving interactive coding}, where the interactive coding protocol is required to preserve the ``knowledge'' transmitted in the original protocol. Our main results are as follows.

\begin{itemize} \item The method of separately applying ECCs to each message is essentially optimal: No knowledge-preserving interactive coding scheme can have an error rate of $1/m$, where m is the number of rounds in the original protocol.

\item If restricting to computationally-bounded (polynomial-time) adversaries, then assuming the existence of one-way functions (resp. subexponentially-hard one-way functions), for every $\epsilon>0$, there exists a knowledge-preserving interactive coding schemes with constant error rate and information rate $n^{-\epsilon}$ (resp. $1/\polylog(n)$) where n is the security parameter; additionally to achieve an error of even $1/m$ requires the existence of one-way functions.

\item Finally, even if we restrict to computationally-bounded adversaries, knowledge-preserving interactive coding schemes with constant error rate can have an information rate of at most $o(1/\log n)$. This results applies even to \emph{non-constructive} interactive coding schemes. \end{itemize}

Category / Keywords: foundations / interactive coding, knowledge preserving, simulation paradigm, error correcting codes,

Date: received 17 Mar 2013

Contact author: chung at cs cornell edu