Cryptology ePrint Archive: Report 2013/194

On the (Im)Possibility of Tamper-Resilient Cryptography: Using Fourier Analysis in Computer Viruses

Per Austrin and Kai-Min Chung and Mohammad Mahmoody and Rafael Pass and Karn Seth

Abstract: We initiate a study of the security of cryptographic primitives in the presence of efficient tampering attacks to the randomness of honest parties. More precisely, we consider p-tampering attackers that may \emph{efficiently} tamper with each bit of the honest parties' random tape with probability p but have to do so in an ``online" fashion. Our main result is a strong negative result: We show that any secure encryption scheme, bit commitment scheme, or zero-knowledge protocol can be ``broken" with probability p by a p-tampering attacker. The core of this result is a new Fourier analytic technique for biasing the output of bounded-value functions, which may be of independent interest.

We also show that this result cannot be extended to primitives such as signature schemes and identification protocols: assuming the existence of one-way functions, such primitives can be made resilient to (1/\poly(n))-tampering attacks where n is the security parameter.

Category / Keywords: foundations / Tampering, Randomness, Fourier Analysis, Encryption.

Date: received 3 Apr 2013, last revised 9 Apr 2013

Contact author: austrin at kth se, chung@cs cornell edu, mahmoody@gmail com, rafael@cs cornell edu, karn@cs cornell edu