Cryptology ePrint Archive: Report 2011/226

The Advanced Encryption Standard, Candidate Pseudorandom Functions, and Natural Proofs

Eric Miles and Emanuele Viola

Abstract: We put forth several simple candidate pseudorandom functions $f_k : \zo^n \to \zo$ with security (a.k.a.~hardness) 2^n that are inspired by the AES block-cipher by Daemen and Rijmen (2000). The functions are computable more efficiently, and use a shorter key (a.k.a.~seed) than previous constructions. In particular, we have candidates computable by \begin{enumerate}[(1)] \item circuits of size $n\, \poly \lg n$ (thus using a seed of length $|k| \le n\, \poly \lg n$); \item $\tcz$ circuits of size $n^{1+\e}$, for any $\e > 0$, using a seed of length $|k| = O(n)$; \item for each fixed seed k of length $|k| = O(n^2)$, a single-tape Turing machine with $O(n^2)$ states running in time $O(n^2)$. \end{enumerate} Candidates (1) and (3) are natural asymptotic generalizations of AES with a specific setting of parameters; (2) deviates somewhat from AES, by relaxing a certain state permutation in AES to have larger range. We argue that the hardness of the candidates relies on similar considerations as those available for AES.

Assuming our candidates are secure, their improved efficiency brings the ``Natural Proofs Barrier'' by Razborov and Rudich (JCSS '97) closer to the frontier of circuit lower bounds. For example, the fact that standard pseudorandom function candidates could not be computed as efficiently as the one in (2) had given rise to a plan for $\tcz$ circuit lower bounds (Allender and Kouck{\'y}; J.~ACM 2010).

We also study the (asymptotic generalization of the) AES S-box. We exhibit a simple attack for the multi-bit output, while we show that outputting one, Goldreich-Levin bit results in a small-bias generator.

Category / Keywords: foundations / Advanced encryption standard (AES), circuit, exponential hardness, lower bound, natural proofs, pseudorandom function (PRF), TC^0, Turing machine

Publication Info: ECCC - TR11-076

Date: received 8 May 2011

Contact author: enmiles at ccs neu edu

Available formats: PDF | BibTeX Citation

Version: 20110512:034448 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]