

Meeting: 998, Houston, Texas, SS 17A, Special Session on Coding Theory and Cryptography

998-68-428

Phillip Rogaway* (rogaway@cs.ucdavis.edu), Department of Computer Science, Kemper Hall, University of California, Davis, CA 95616 USA. *Efficient Instantiations of Tweakable Blockciphers*. Preliminary report.

We describe highly efficient constructions, XE and XEX, that turn a blockcipher $E: \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ into a tweakable blockcipher $\tilde{E}: \mathcal{K} \times \mathcal{T} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ having tweak space $\mathcal{T} = \{0, 1\}^n \times \mathbb{I}$ where \mathbb{I} is a set of tuples of integers such as $\mathbb{I} = [1..2^{n/2}] \times [0..10]$. When tweak T is obtained from tweak S by incrementing one of its numerical components, the cost to compute $\tilde{E}_K^T(M)$ having already computed some $\tilde{E}_K^S(M')$ is one blockcipher call plus a small and constant number of elementary machine operations. Our constructions work by associating to the i^{th} coordinate of \mathbb{I} a “small” element $\alpha_i \in \mathbb{F}_{2^n}^*$ and multiplying by α_i when one increments that component of the tweak. We illustrate the use of this approach by refining the authenticated-encryption scheme OCB and the message authentication code PMAC, yielding variants of these algorithms, OCB1 and PMAC1, that are simpler and faster than the original schemes, and yet have simpler proofs. Our results bolster the thesis of Liskov, Rivest, and Wagner (CRYPTO '02) that a desirable approach for designing modes of operation is to start from a tweakable blockcipher. We elaborate on their idea, suggesting the kind of tweak space, usage-discipline, and blockcipher-based instantiations that give rise to simple and efficient modes of operation of a conventional blockciphers. (Received March 08, 2004)