

On block ciphers and permutations in hashing

Joan DAEMEN¹ Gilles VAN ASSCHE¹

¹STMicroelectronics

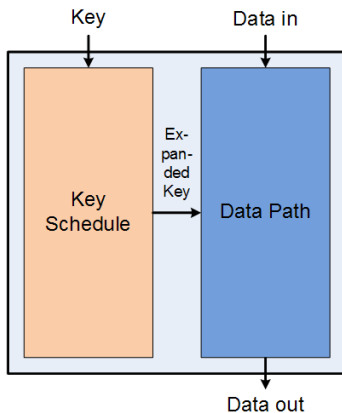
15 January 2008 — Dagstuhl Cryptography Seminar

Block cipher vs. Permutation

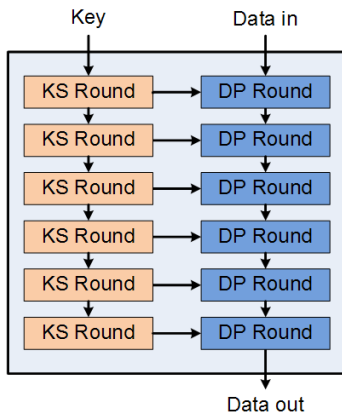
	Block cipher	Permutation
Dimensions	Block length n Key length m	Width $r + c$
Message block	m bits	r bits
Indiff. bound	$N^2/2^{n+1}$	$N^2/2^{c+1}$
Assumes	Ideal cipher	random permutation

- $n = c$ for same *indifferentiability* strength
- $m = r$ for same message blocksize

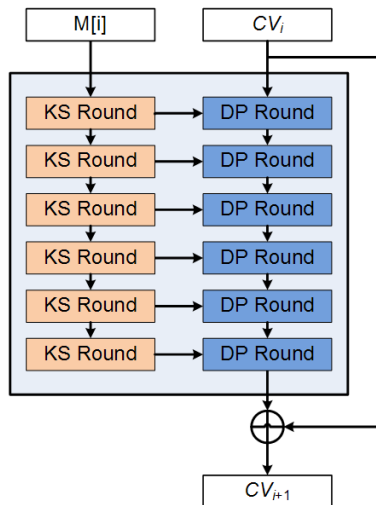
Block cipher



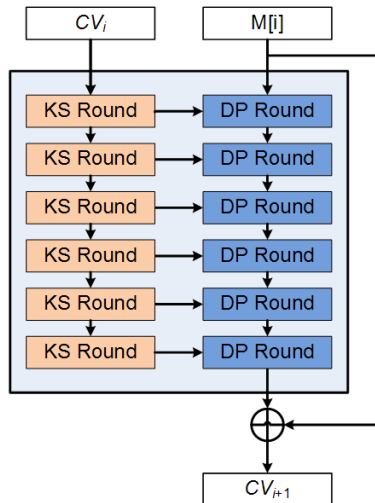
The internals



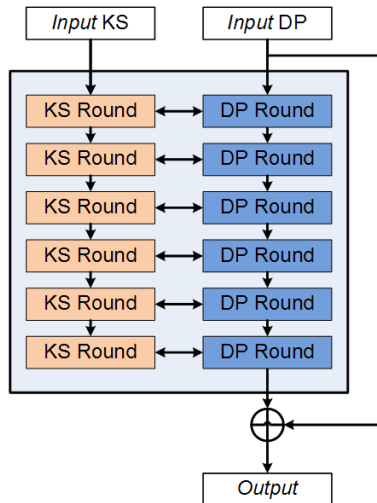
Davies-Meyer mode compression function



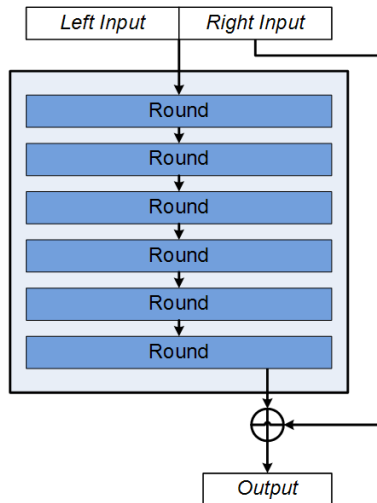
Matyas-Meyer-Oseas mode compression function



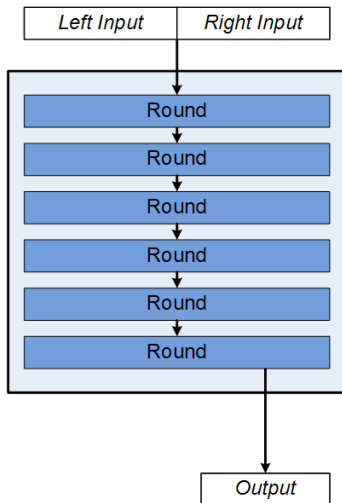
Removing restrictions not required in hashing



Simplifying the view



No more need for the feedforward ...



Just use the full output!

