On Noekeon, no!

Joan Daemen*, Gilles Van Assche*, Michael Peeters* and Vincent Rijmen**

*Proton World, Brussels
**CRYPTOMAThIC, Leuven





On related-key attacks

- What does it take?
 - to attack a key K, many ciphertext-plaintext pairs must be obtained for K and another key K*
- Relation between K and K* depends on key schedule mode. For a chosen value A
 - Direct mode: protocol should allow K* = A ⊕ K
 - Indirect mode: K * = Noekeon⁻¹(A ⊕ Noekeon(K))
- Conditions for the attacks to be mountable:
 - Direct mode: lousy key management
 - Indirect mode: Trojan Horse





On the wide trail strategy

- The relevant property:
 - minimum number of active S-boxes per round
 - in differential and linear trails
- Still, documentation can be clarified
 - theta was chosen first
 - combination of rotations of Pi1 and S-box was chosen to optimize relevant property
 - This process eliminated all "weak" S-boxes
- Let's call it a variant of the wide trail strategy ;-)
 - The trails are wide, aren't they?
 - 20 active S-boxes per 4 rounds!





Noekeon:

- is ultra compact and fast in hardware,
- runs fast even in DPA-resistant implementations,
- has very low RAM usage in software,
- takes very small amount of code,
- is very efficient on a wide range of platforms,
- so simple that it can be memorized by an average person!



