Cryptology ePrint Archive: Report 2011/140

Some Instant- and Practical-Time Related-Key Attacks on KTANTAN32/48/64

Martin Ågren

Abstract: The hardware-attractive block cipher family KTANTAN was studied by Bogdanov and Rechberger who identified flaws in the key schedule and gave a meet-in-the-middle attack. We revisit their result before investigating how to exploit the weakest key bits. We then develop several related-key attacks, e.g., one on KTANTAN32 which finds 28 key bits in time equivalent to $2^{3.0}$ calls to the full KTANTAN32 encryption. The main result is a related-key attack requiring $2^{28.44}$ time (half a minute on a current CPU) to recover the full 80-bit key. For KTANTAN48, we find three key bits in the time of one encryption, and give several other attacks, including full key recovery. For KTANTAN64, the attacks are only slightly more expensive, requiring $2^{10.71}$ time to find 38 key bits, and $2^{32.28}$ for the entire key. For all attacks, the requirements on related-key material are modest as in the forward and backward directions, we only need to flip a single key bit. All attacks succeed with probability one. Our attacks directly contradict the designers' claims. We discuss why this is, and what can be learnt from this.

Category / Keywords: secret-key cryptography / cryptanalysis, related key, block cipher, key schedule, lightweight cipher, key-recovery

Date: received 21 Mar 2011, last revised 30 Sep 2011

Contact author: martin agren at eit lth se