Cryptology ePrint Archive: Report 2011/201

Improved Meet-in-the-Middle Cryptanalysis of KTANTAN

Lei Wei and Christian Rechberger and Jian Guo and Hongjun Wu and Huaxiong Wang and San Ling

Abstract: We revisit meet-in-the-middle attacks on block ciphers and recent developments in meet-in-the-middle preimage attacks on hash functions. Despite the presence of a secret key in the block cipher case, we identify techniques that can also be mounted on block ciphers, thus allowing us to improve the cryptanalysis of the block cipher KTANTAN family. The first and major contribution is that we spot errors in previous cryptanalysis, secondly we improve upon the corrected results. Especially, the technique indirect-partial-matching can be used to increase the number of matched bits significantly, as exemplified by our attacks. To the best of our knowledge, this is the first time that a splice-and-cut meet-in-the-middle attack is applied to block ciphers. When the splitting point is close to the start or the end of the cipher, the attack remains to be at very low data complexity. The secret key of the full cipher can be recovered faster than exhaustive search for all three block sizes in the KTANTAN family. The attack on KTANTAN32 works with a time complexity $2^{72.9}$ in terms of full round encryptions. The attack has a time complexity of $2^{73.8}$ and $2^{74.4}$ on KTANTAN48 and KTANTAN64, respectively. Moreover, all the three attacks work with 4 chosen ciphertexts only. These results compare favourably with the factor 2 speed-up over brute force obtained in earlier work 4 , and hence these attacks are the best cryptanalysis results so far.

Category / Keywords: secret-key cryptography / block cipher, hash function, meet-in-the-middle attack, KTANTAN, indirect-partial-matching, splice-and-cut

Date: received 20 Apr 2011, last revised 27 Apr 2011

Contact author: WL at pmail ntu edu sg

Available formats: PDF | BibTeX Citation

Version: 20110427:081645 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]