Improved Meet-in-the-Middle cryptanalysis of KTANTAN (poster)

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

2011

Wei, L., Rechberger, C., Guo, J., Wu, H., Wang, H. & Ling, S. (2011). Improved Meet-in-the-Middle Cryptanalysis of KTANTAN (Poster). Lecture Notes in Computer Science, 6812, pp.433-438.

https://hdl.handle.net/10356/99904

https://doi.org/10.1007/978-3-642-22497-3_31

Improved Meet-in-the-Middle Cryptanalysis of KTANTAN (Poster)*

Lei Wei[1], Christian Rechberger[2], Jian Guo[3], Hongjun Wu[1], Huaxiong Wang[1], and San Ling[1]

[1] Nanyang Technological University, Singapore
{weil0005,wuhj,hxwang,lingsan}@ntu.edu.sg
[2] Katholieke Universiteit Leuven, ESAT/COSIC and IBBT, Belgium
christian.rechberger@groestl.info
[3] Institute for Infocomm Research, A*STAR, Singapore.
ntu.guo@gmail.com

Abstract. This paper presents ongoing work towards extensions of meet-in-the-middle (MITM) attacks on block ciphers. Exploring developments in MITM attacks in hash analysis such as: (i) the *splice-and-cut* technique; (ii) the *indirect-partial-matching* technique. Our first contribution is that we show corrections to previous cryptanalysis and point out that the key schedule is more vulnerable to MITM attacks than previously reported. Secondly we further improve the time complexities of previous attacks with (i) and (ii), now the 80-bit secret key of the full rounds KTANTAN-$\{32, 48, 64\}$ can be recovered at time complexity of $2^{72.9}$, $2^{73.8}$ and $2^{74.4}$ respectively, each requiring 4 chosen-plaintexts.

1 Introduction

We study the KTANTAN family [3] on resistance to MITM attacks. In the attack due to Bogdanov and Rechberger [2], the key schedule was reported to be weak and the key of full KTANTAN-32 can be recovered slightly faster than brute force. In this paper, we first point out that the previous analysis was not correct (as it was found based on a wrong key schedule), the actual key schedule is even weaker than reported. Based on the corrections, we further examine how developements on MITM preimage attacks in hash analysis can improve the attack. Indeed, with *splice-and-cut* and *indirect-partial-matching*, we find chosen-plaintext key recovery attacks with improved time complexities, faster than brute force by $2^{7.1}$, $2^{6.2}$ and $2^{5.6}$ for block size 32, 48 and 64.

The paper is organized as follows: techniques in MITM attacks are discussed in Section 2, the previous attack versus our experiment results are discussed in Section 3, our improve attacks to KTANTAN family with hash analysis techniques are shown in Section 4 and we conclude in Section 5.

2 Developments in MITM Attacks

MITM attacks were originally developed from cryptanalysis of block ciphers. In 2008, Sasaki and Aoki noticed that the MITM attacks could be applied to hash functions, to find (second) preimages faster than brute-force [4]. The attacks and further developments have successfully broken the one-wayness of many designs. We briefly introduce the techniques relevant to our attacks with Fig. 1.

* Full version at http://www1.spms.ntu.edu.sg/~weil0005/mitm2.pdf

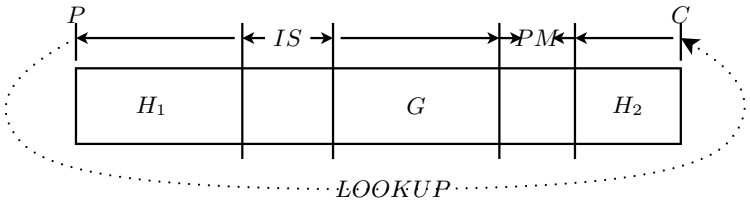

Fig. 1. A general setup for MITM attacks

In a Davies-Meyer construction from a block cipher E keyed by message m, the feedforward $\oplus h$ is used to compute h' as $E_m(h) \oplus h$. To *splice-and-cut*, $E(h)$ is written as three sub-ciphers as $E(h) = H_2 \circ G \circ H_1(h)$ (without IS and PM). Let $h_{inter} = H_1(h)$, we have $H_2^{-1}(H_1^{-1}(h_{inter}) \oplus h') = G(h_{inter})$. The output of E is computed as $h \oplus h'$, this is the *splice* that connects the input and output of E. The attack starts at position h_{inter} and *cut* E into $G(\cdot)$ and $H_2^{-1}(H_1^{-1}(\cdot) \oplus h')$. For a block cipher attack, a lookup table $LOOKUP$ is used as a *virtual* feedforward. For *initial-structure* (IS), neighbouring key bits around h_{inter} may be swapped for more neutral key bits. Let $K_c := K_1 \cap K_2$, we compute $M := G_{K_1}(h_{inter})$ and $M' := H_{K_2}^{-1}(h_{inter})$. A *partial-matching* (PM) of m bits of M and M' is sufficient for filtering wrong keys at a ratio of 2^{-m}. After this the PM portion is repeated to filter more wrong keys, and it does not dominate the overall complexity if $(|K_1| + |K_2| - 2|K_c| - m) + \log_2(\alpha) < \max(|K_1| - |K_c|, |K_2| - |K_c|)$, where α is the percentage of PM steps. *Indirect-partial-matching* (IPM) extends PM for more steps. PM usually starts when key bits in $K_2 \setminus K_c$ appear after the end of G (otherwise, one can extend G for more steps). Similarly for the other side, *i.e.,* key bits in $K_1 \setminus K_c$ appear just before H_2. IPM aims to find, from the PM steps, state bits that can be computed by both $G_{K_1} + \phi_{K_2}$ and $H_{K_2} + \mu_{K_1}$ from h_{inter}, such that the matching can be checked between $G_{K_1} - \mu_{K_1}$ and $H_{K_2} - \phi_{K_2}$ instead. ϕ and μ are linear in their key materials.

3 Meet-in-the-Middle Cryptanalysis of KTANTAN

The KTANTAN family of block ciphers, with block sizes of 32, 48 and 64, was proposed at CHES'09 [3]. They accept 80-bit key and share a key schedule for 254 rounds.

3.1 The Previous Meet-in-the-Middle Attack

The attacks reported in [2] work with a few known plaintexts at around the *unicity distance*. The attack to full KTANTAN32 works in 2^{79} encryptions. Although arguably marginal, it is the first key-recovery attack to the full 254 rounds faster than brute force. For block size b of 48 and 64, the attack manages to break 251 and 248 rounds respectively [4].

The attack cuts the R-round KTANTAN-b cipher (b for block size) into three parts for some $\alpha, \beta < R$. Let $K := k_{79}k_{78} \ldots k_1k_0$ be the key and $A := \{k_0, k_1, \ldots, k_{78}, k_{79}\}$. Let x_i be the state after round i, for $0 \leq i \leq 254$. Let $\varphi_{i,j}$ be the transformation from round i to round j (inclusive), key bits in $A_1 :=$

[4] The authors later updated in `http://eprint.iacr.org/2010/532.pdf` and [1]

$\{k_{15}, k_{79}\}$ are neutral to $H := \varphi_{254-\beta+1,254}$ (the backward phase) and $A_2 := \{k_5, k_{37}, k_{69}\}$ neutral to $G := \varphi_{1,\alpha}$ (the forward phase). Let $A_0 := A \setminus (A_1 \bigcup A_2)$. The attack to KTANTAN32 proceeds with a text pair (P, C), for each guess of key bits in A_0, compute 3-bit of x_{128} for independent guesses of A_1 and A_2, from respectively $M := G(P) = \varphi_{1,105}(P)$ and $M' := H^{-1}(C) = \varphi^{-1}_{137,254}(C)$. For a key guess that passes this 3-bit filter, try current and additional pairs of (P, C) one by one. For $\lceil 80/b \rceil$ pairs tested, the correct key can be recovered with probability close to 1. The claimed complexity is at around $2^{|A_0|}(2^{|A_1|} + 2^{|A_2|}) + 2^{80-3} = 2^{79}$ encryptions. A more accurate calculation showes that it works at a time complexity of $2^{|A_0|}(2^{|A_1|} \cdot \alpha/R + 2^{|A_2|} \cdot \beta/R + 2^{|A_1|+|A_2|-m}(R-\alpha-\beta)/R) \doteq 2^{77.6}$.

3.2 New Experimental Observations on the Attack

We reimplement the family of KTANTAN from its design paper [3] and examine the key schedule according to the attack in [2], different sets of neutral key bits are found and it suggests that the key schedule is much weaker than reported. Under this observation, the MITM approach brings non-marginal attacks for the full ciphers of the entire family. The previous results and our attacks (*) are summarized in Table 1.

Table 1. The B-R attack and our results

b	R	α	β	A_1	A_2	m	Time	Data	
32	254	105	118	15, 79	5, 37, 69	3	$2^{79.0}$	3 KP	[2]
48	251	107	112	11, 15, 75, 79	5, 69	1	$2^{79.7}$	2 KP	[2]
64	248	107	112	9, 73	5, 69	2	$2^{79.58}$	2 KP	[2]
32	254	111	122	3, 20, 41, 47, 63, 74	32, 39, 44, 61, 66, 75	12	$2^{73.88}$	3 KP	*
32	254	110	122	3, 20, 41, 47, 63, 74	27, 32, 39, 44, 59, 61, 66, 75	4	$2^{73.88}$	3 KP	*
32	254	109	122	3, 20, 41, 47, 63, 74	13, 27, 32, 39, 44, 59, 61, 66, 75	3	$2^{74.33}$	3 KP	*
48	254	123	122	3, 20, 41, 47, 63, 74	32, 44, 61, 66, 75	37	$2^{74.53}$	2 KP	*
48	254	111	121	3, 20, 41, 47, 63, 74	32, 39, 44, 61, 66, 75	4	$2^{73.97}$	2 KP	*
64	254	123	122	3, 20, 41, 47, 63, 74	32, 44, 61, 66, 75	44	$2^{74.53}$	2 KP	*

3.3 Low Complexity Implementation of the Attack

In the cases that the secret keys are not derived with full 80-bit entropy, the attack may become a real threat when the time is 2^6 to 2^7 times less due to the attack of this paper. For example, it is not hard to eavesdrop a small amount of ciphertext corresponding to known protocol headers and it is feasible to launch an attack. We implement a low complexity version of an attack to KTANTAN32 in Table 1. We assume 40 bits of A_0 are known by the attacker, the attack has $\alpha = 111, \beta = 122, A_1 = \{3, 20, 41, 47, 63, 74\}, A_2 = \{32, 39, 44, 61, 66, 75\}$ and 12 bits match. The attack successfully recovers the 40-bits in 5 hours 34 seconds on a Quad-core HP xw4600 workstation at 2.40GHz. With 40 bits known, the estimated complexity 2^{74} is reduced to 2^{34}. The experiment confirms roughly a reduction of 2^6 as encrypting 2^{26} plaintexts takes 45 seconds. As a comparison, recovering 40 bits by exhaustive search would take roughly half a month if using the same workstation.

4 More General MITM Attacks on KTANTAN Family

The effeciency of the attacks discussed in Section 3 depends crucially on the number of neutral key bits in the forward phase and backward phases. Hence a natural question is, can we improve the attack by finding more neutral key bits or more bits for matching? We show how *splice-and-cut* and *indirect-partial-matching* address this question.

4.1 The Observations and Search

In round r the computations for $f_{r,a}$ and $f_{r,b}$ are repeated 1, 2 or 3 times for 3 respective block sizes. For each evaluation[5] of $f_a(L_1)$ or $f_b(L_2)$, a single round key bit is mixed XOR-linearly into the LSB of L_1 or L_2, hence affecting the lowest 1 to 3 bits considering the shift(s). In the round that follows, only a few bits of the state get involved in the nonlinear part in computing $f_{r,a}$ and $f_{r,b}$. We observe that the round key bits remain linear in the state bits for some rounds, hence expecting more bits to be matched by IPM.

Let x_i be the state after round i for $1 \leq i \leq 254$ then x_{254} is the ciphertext and denote the plaintext x_0. For φ_{b_0,b_1} as the backward phase and φ_{f_0,f_1} as forward, the rounds between (exclusive) b_0 and f_0 are used for the *initial structure*. We search exhaustively for all feasible combinations of (f_0, f_1, b_0, b_1) and compute the complexities. IS is applicable and we set $f_0 - b_0 - 1$ to up to 20. The search shows that IS is not contributing to a better attack, hence $f_0 = b_0 + 1$. We list the best attacks in Table 2. The IPM checks between two fully determined states $M := x_{f_1}$ (after round f_1) and $M' := x_{b_1-1}$ (before round b_1).

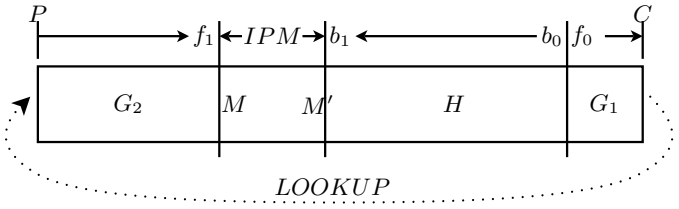

Fig. 2. Illustration of MITM attack with splice-and-cut and IPM

4.2 The Attack with Splice-and-Cut and Indirect-Partial-Matching

First we construct the table $LOOKUP$ to *splice* two ends of cipher. Select a random value for x_{b_0} and compute $C := G_1(x_{b_0})$ for all 4 possible outputs of $G_1 := \varphi_{f_0,254}$. Add the chosen-ciphertext pair (C, P) to the table. Let A_1 be the key bits neutral to $H^{-1} := \varphi^{-1}_{b_1,b_0}$ and A_2 for $G := G_2 \circ LOOKUP \circ G_1 = \varphi_{1,f_1} \circ LOOKUP \circ \varphi_{f_0,254}$.

The attack goes as follows: for each guess of A_0 we try parallel guesses for A_1 and A_2, computing $M := G(x_{b_0})$ and $M' := H^{-1}(x_{b_0})$. m-bit *partial matching signature* s can be computed from both M and M', it is used as a filter of ratio 2^{-m} and the matching is done in a table. A survival key is then tested on whether $M' = \varphi_{f_1+1,b_1-1}(M)$ for K, and on other pairs of (P, C). The right key is the one that survices all $\lceil 80/b \rceil$ pairs.

[5] Notations follow from [3].

The m-bit partial matching signature is computed from the matching position, as Section 2 on IPM. The signature includes state bits independent or linearly dependent with the active (non-neutral) key bits in the IPM phase. The technique significantly improves the number of bits that can be matched, the matching can be extended for more rounds to have more neutral bits. For KTANTAN32, the matching position is at x_{115}. Denote x_{115} as x and let $x[i]$ be the i-th bit of x, for $0 \leq i \leq 31$. For the forward part of IPM, the following key bits are linear in the corresponding state bits, k_{27} in $x[0]$, k_{13} in $x[1]$, k_{39} in $x[3]$, k_{59} in $x[4]$ and k_{39} in $x[22]$. For the backward part, we have k_{74} in $x[26]$, k_{74} in $x[21]$, k_{74} in $x[3]$ and k_{20} in $x[2]$. Hence the matching signature is $(x[26] - k_{74}, x[22] - k_{39}, x[21] - k_{74}, x[7], x[6], x[5], x[4] - k_{59}, x[3] - k_{39} - k_{74}, x[2] - k_{20}, x[1] - k_{13}, x[0] - k_{27})$ which can be computed from both sides without knowing the value for the active key bits from that side.

Table 2. MITM attack with splice-and-cut and indirect-partial-matching

b	R	b_1	b_0	f_0	f_1	A_1	A_2	m	Time	Data
32	254	148	253	254	109	$13, 27, 32, 39, 44, 59, 61, 66, 75$	$3, 20, 41, 47, 63, 74$	11	$2^{72.93}$	4 CC
48	254	150	253	254	111	$32, 39, 44, 61, 66, 75$	$3, 20, 41, 47, 63, 74$	15	$2^{73.77}$	4 CC
64	254	151	253	254	112	$32, 44, 61, 66, 75$	$3, 20, 41, 47, 63, 74$	54	$2^{74.38}$	4 CC

5 Conclusions

We have shown corrected results for the KTANTAN key schedule for MITM attacks, and have confirmed the attack with an experiment. Moreover, we have shown some techniques from hash function MITM preimage attacks effective for improving the results on KTANTAN. In particular, *splice-and-cut* gives more neutral bits and *indirect-partial-matching* improves over *partial-matching* with much better matching. It is open to examine if better enhancements can be discovered for MITM attacks and dedicated techniques to be found for particular ciphers.

Acknowledgments This work was supported in part by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

References

1. A. Bogdanov and C. Rechberger. A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN. In *Selected Areas in Cryptography*, pages 229–240, 2010.
2. A. Bogdanov and C. Rechberger. Generalized Meet-in-the-Middle Attacks: Cryptanalysis of the Lightweight Block Cipher KTANTAN. 2010. In preproceedings of SAC, `http://homes.esat.kuleuven.be/~abogdano/talks/ktantan_sac10.pdf`.
3. C. D. Cannière, O. Dunkelman, and M. Knezevic. KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers. In C. Clavier and K. Gaj, editors, *CHES*, volume 5747 of *LNCS*, pages 272–288. Springer, 2009.
4. Y. Sasaki and K. Aoki. Preimage Attacks on 3, 4, and 5-Pass HAVAL. In J. Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *LNCS*, pages 253–271. Springer, 2008.