Improved Meet-in-the-Middle Cryptanalysis of KTANTAN

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

[1]Nanyang Technological University, Singapore

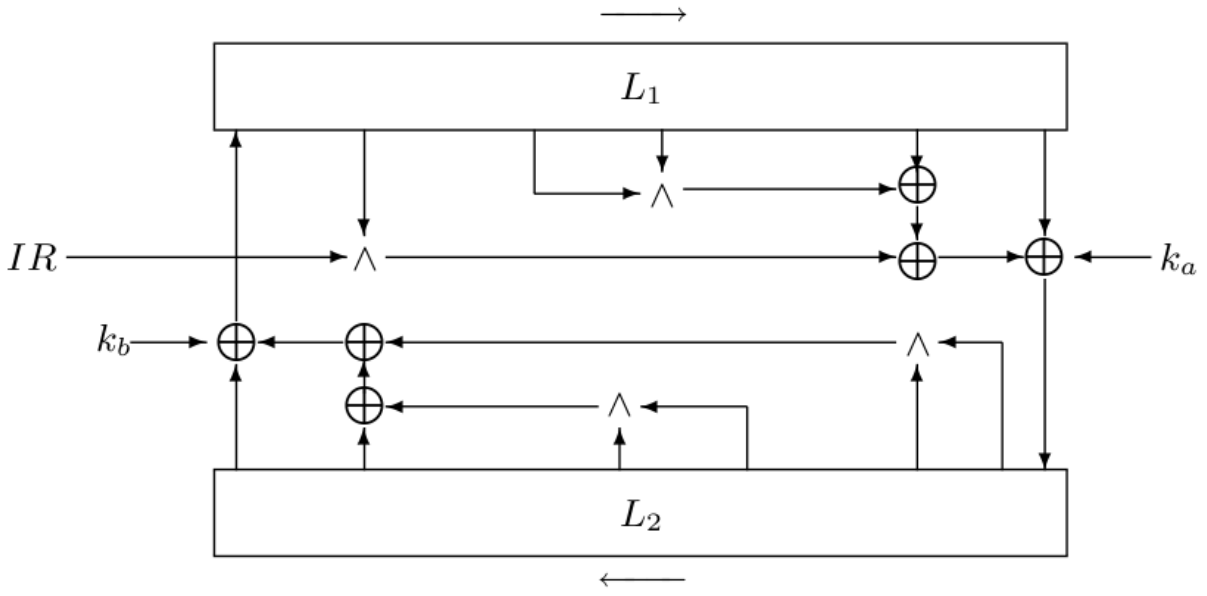
[2]ENS Paris and Chaire France Telecom

[3]Institute for Infocomm Research, A*STAR, Singapore

ACISP 2011, 12 Jul 2011

The KATAN/KTANTAN Family of Block Ciphers

- by Chrstophe de Canniere, Orr Dunkelman, and Miroslav Knezevic in CHES 2009
- three block sizes: 32, 48, 64, sharing 80-bit key with 254 rounds
- KATAN and KTANTAN differ in key schedule only



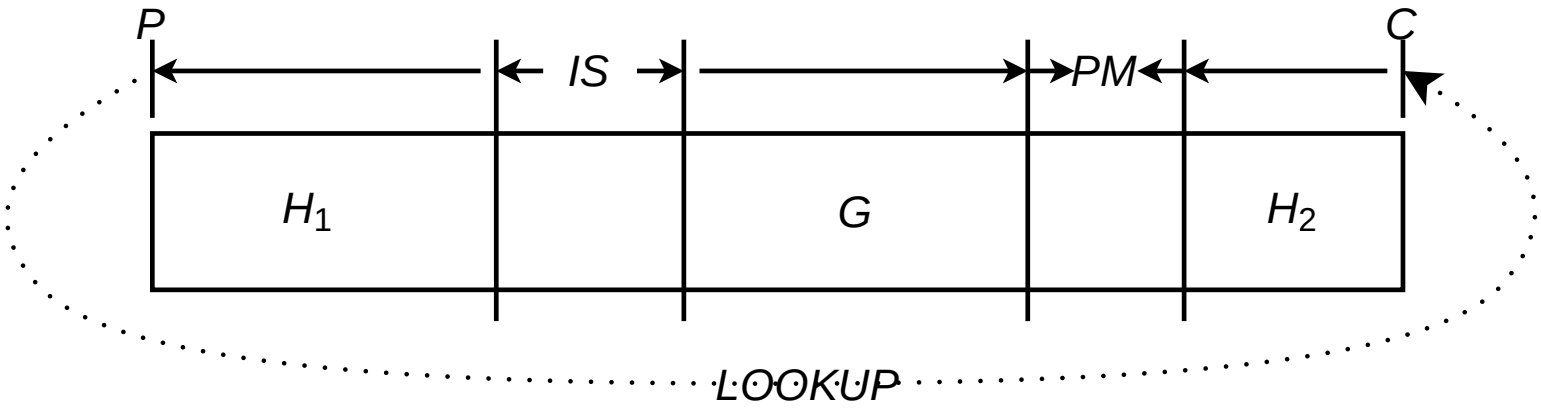
Performance of the KATAN/KTANTAN Family

Cipher	Throughpout (Kbps @ 100 KHz)	Size (GE)
KATAN32	12.5	802
KATAN48	18.8	927
KATAN64	8.4	1027
KATAN64	25.0	1054
KATANTAN32	12.5	**462**
KATANTAN48	18.8	588
KATANTAN64	25.0	688

v.s. PRINTCipher-48 (block size 48) with 402 GE, and PRINTCipher-96 (block size 96) with 726 GE

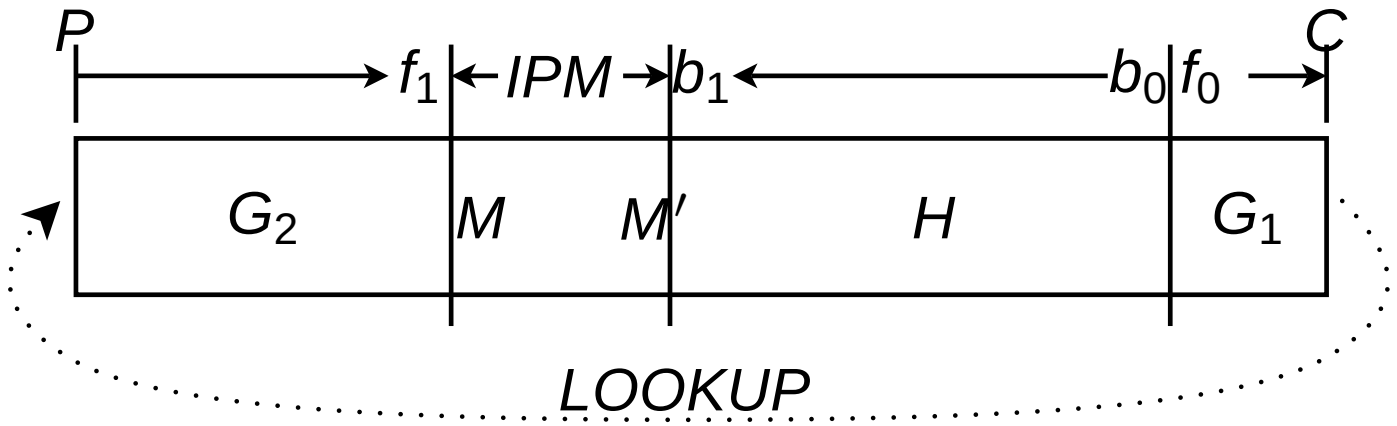
MITM Attacks: Developments in Hash Analysis

- Originally developed from cryptanalysis of block ciphers [DH77, CE85].
- From 2008, more techniques are developed in finding (second) preimages in hash functions: HAVAL [SA08], MD5 [SA09], reduced SHA-0,1 [AS09], SHA-2 [AGMSW09] and Tiger [GLRW10].
- New techniques in particular *splice-and-cut*, *initial-structure* (IS) and *indirect-partial-matching* (IPM) are relevant to the attacks on KTANTAN.
- Application to block ciphers



MITM Attacks against KTANTAN

- Application to all block sizes of the KTANTAN family.
- *splice-and-cut* and *indirect-partial-matching*.



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