Attacking KLEIN

J.-Ph. Aumasson, María Naya-Plasencia,
Markku-Juhani O. Saarinen

Presented at INDOCRYPT 2011 (December)

KLEIN: RFIDSec 2011 (June)

rfid-cusp.org/rfidsec/program.php

10:10–10:35 AM Coffee and Tea Break

Technical Session 1: On-Tag Cryptography
(Session chair: Farinaz Koushanfar)

KLEIN: A New Family of Lightweight Block Ciphers
Authors: Zheng Gong, Svetla Nikova and Yee Wei Law
Affiliations: School of Computer Science, South China Normal University, China and Faculty of EWI, University of Twente, The Netherlands and Department of EEE, The University of Melbourne, Australia

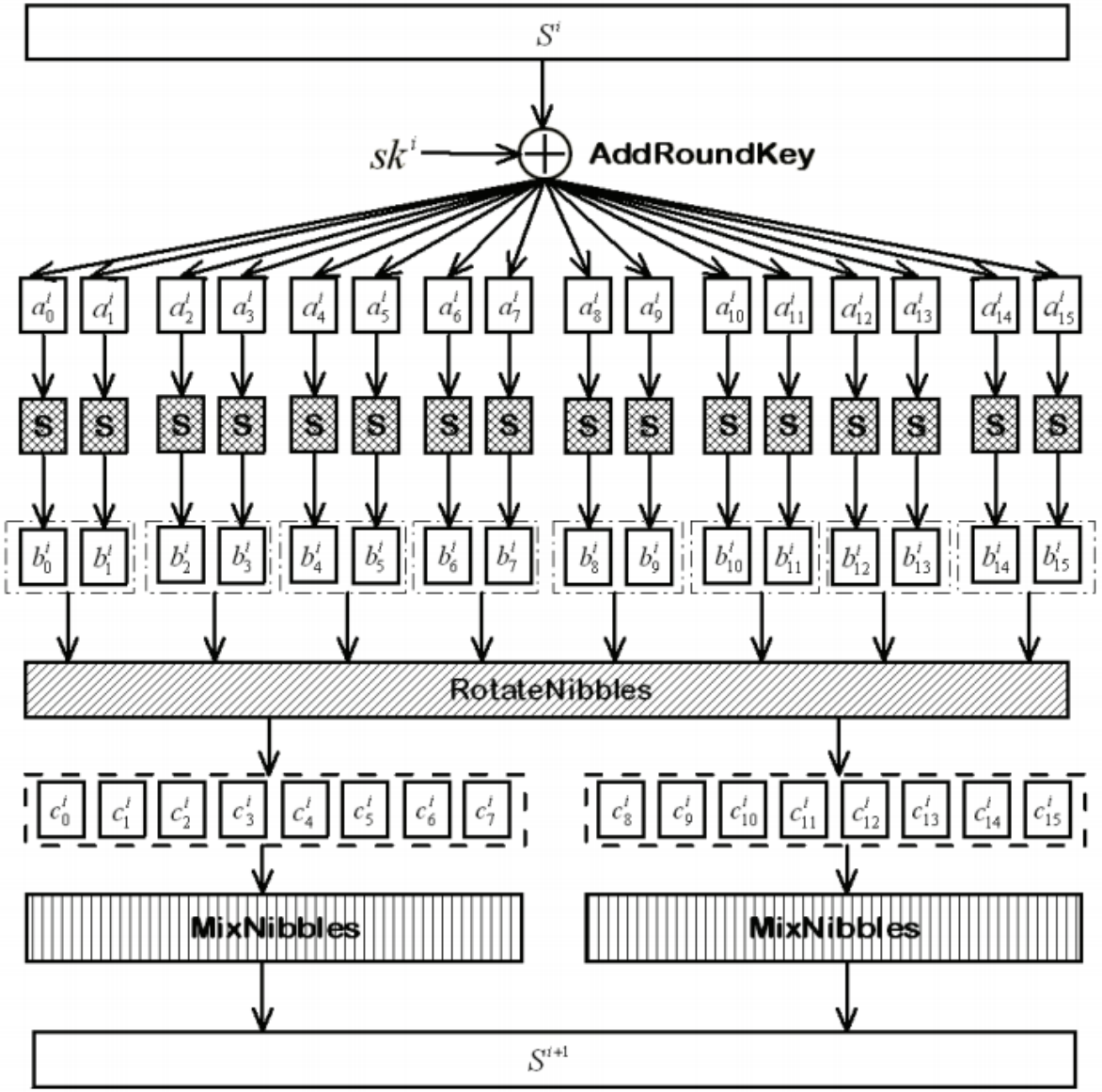
Low-RAM on small MCUs

~2000 GE on 180 nm ASIC

Reasonable speed

Simple and elegant design

=> How secure is it?


S^i
sk^i
AddRoundKey
a_0^i a_1^i a_2^i a_3^i a_4^i a_5^i a_6^i a_7^i a_8^i a_9^i a_{10}^i a_{11}^i a_{12}^i a_{13}^i a_{14}^i a_{15}^i
S
b_0^i b_1^i b_2^i b_3^i b_4^i b_5^i b_6^i b_7^i b_8^i b_9^i b_{10}^i b_{11}^i b_{12}^i b_{13}^i b_{14}^i b_{15}^i
RotateNibbles
c_0^i c_1^i c_2^i c_3^i c_4^i c_5^i c_6^i c_7^i
c_8^i c_9^i c_{10}^i c_{11}^i c_{12}^i c_{13}^i c_{14}^i c_{15}^i
MixNibbles
MixNibbles
S^{i+1}

64-bit block

64-bit key -> 12 rounds

80-bit key -> 16 rounds

96-bit key -> 20 rounds

Interaction between:

Nibble-oriented S-box

Byte-oriented MixColumn

Observation 1

X \in {1,2,…,7} [i.e. nibble with null MSB]

MixColumn(m) $\oplus$ MixColumn(m $\oplus$ 0000000X)

= 0Y0Y0Y0Y

Where Y is a wildcard for nibbles \in {1,2,…,F}

Observation 2

X **wildcard** for nibbles \in {1,2,…,7}

MixColumn(m) $\oplus$ MixColumn(m $\oplus$ 0X0X0X0X)

= 0Y0Y0Y0Y

Where Y is a wildcard for nibbles \in {0,1,…,F}

Observation 3

X **wildcard** for nibbles \in {8,9,…,F}

MixColumn(m) $\oplus$ MixColumn(m $\oplus$ 0X0X0X0X)

= 0Y0Y0Y0Y

Where Y is a wildcard for nibbles \in {0,1,…,F}

Observation 4

X \in {1,2,…,F}

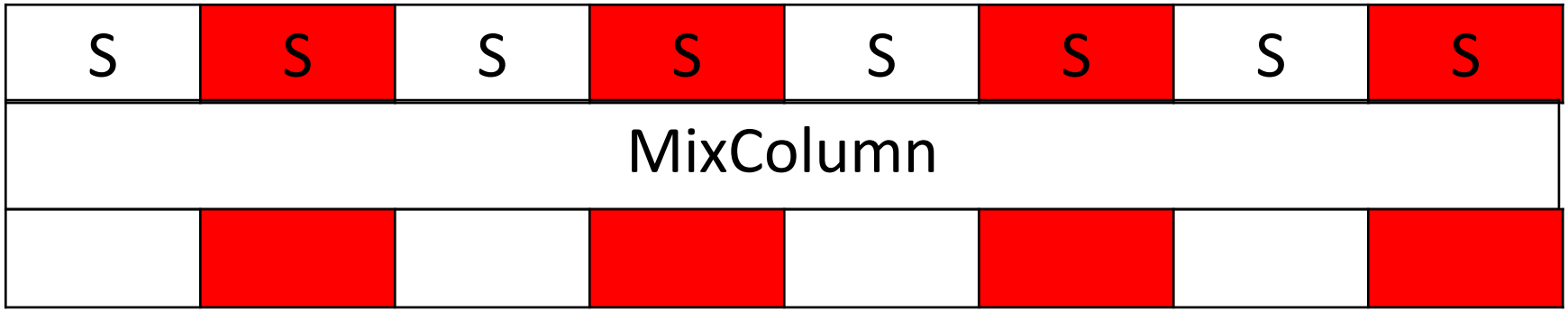
Prob[Sbox(m) $\oplus$ Sbox(m $\oplus$ X)] \in {1,2,..,8}

= 7/15 ~ 2^-1.1

If X \in {B,E}, Prob = 3/4

Key idea

Ensure that differences entering MixColumn are all either in {0,1,..,7} or in {8,9,…,F}, so that its output only has differences in lower nibbles



1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

Black squares = actives nibbles

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

Distinguisher on 6 rounds in ~2^28

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

Distinguisher on 6 rounds in ~2^28

Transform to key-recovery on 7 rounds

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

Transform to key-recovery on 7 rounds

Message modification => 2^23 for an extra pair

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

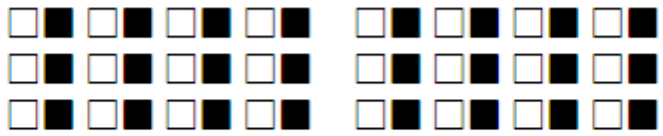
Message modification => 2^23 for an extra pair

Find 6 pairs in <2^29, enough to find 32b subkey

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

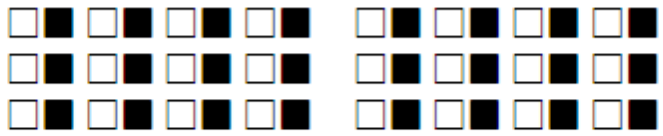
Find 6 pairs in <2^29, enough to find 32b subkey

Repeat for the other 32b half

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

7 round distinguisher? 33.90 > 32…

Filter by checking ability to message-modify a pair

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

7 round distinguisher? 33.90 > 32…

Filter by checking ability to message-modify a pair

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

7 round distinguisher? 33.90 > 32…

If trail followed, an extra pair costs ~2^28

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

A good pair can be identified in ~2^34 encryptions

Find 32b half subkey that gives inactive higher nibbles

1	SubNibbles RotateNibbles MixNibbles		$p_1 \approx 2^{-0.42}$	$2^{-0.42}$
2	SubNibbles RotateNibbles MixNibbles		$p_2 \approx 2^{-4.40}$	$2^{-4.82}$
3	SubNibbles RotateNibbles MixNibbles		$p_3 \approx 2^{-5.82}$	$2^{-10.64}$
4	SubNibbles RotateNibbles MixNibbles		$p_4 \approx 2^{-5.82}$	$2^{-16.45}$
5	SubNibbles RotateNibbles MixNibbles		$p_5 \approx 2^{-5.82}$	$2^{-22.27}$
6	SubNibbles RotateNibbles MixNibbles		$p_6 \approx 2^{-5.82}$	$2^{-28.08}$
7	SubNibbles RotateNibbles MixNibbles		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

Repeat for the other half of the last subkey

=> Recover the full 64b key in <2^35 encryptions

8-round key recovery

<2^35 for 64b key (12 rounds in total)

<2^51 for 80b key (16 rounds in total)

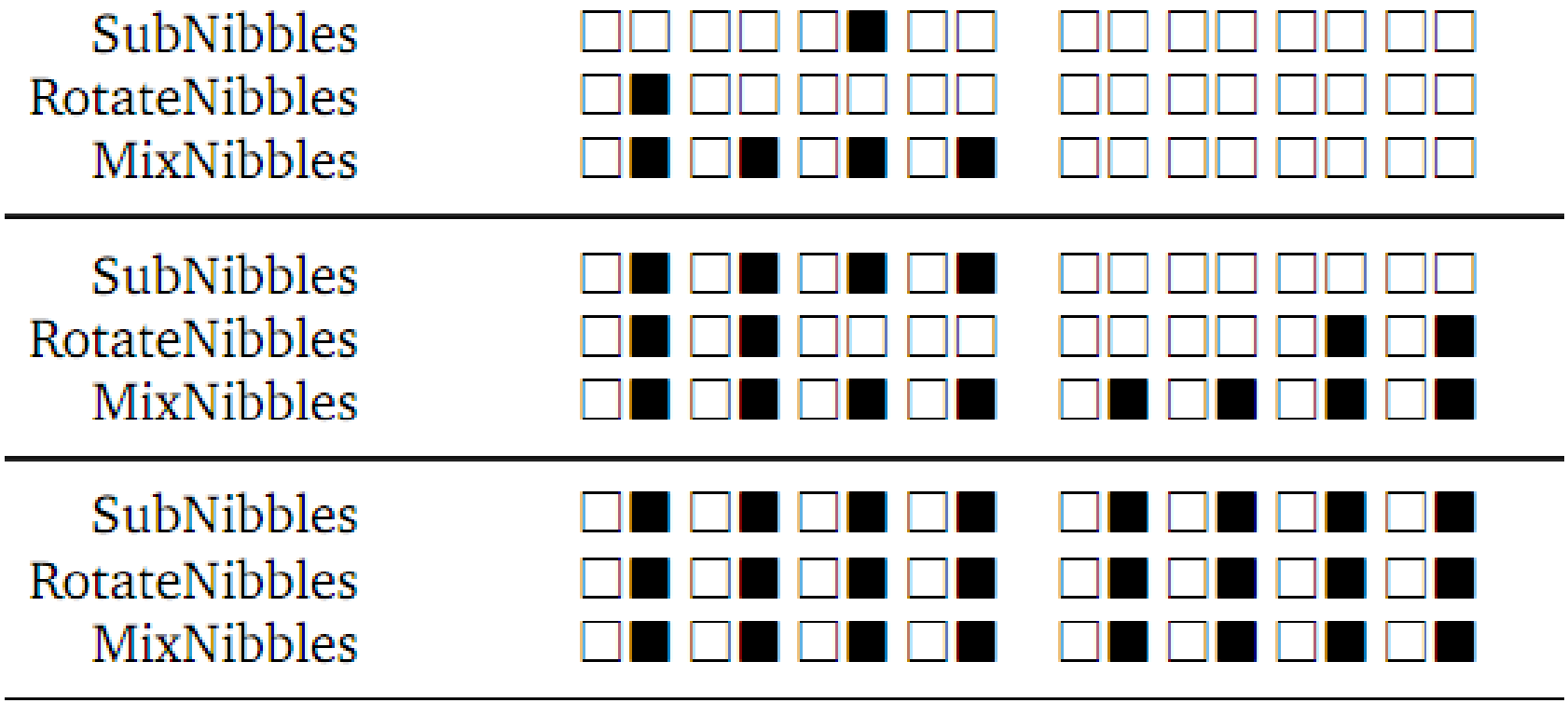
<2^67 for 96b key (20 rounds in total)

```
$ ./attack 8
test vector ok
soundness ok
Pair found in 2^28.21: fb5248c1a424ca3e
Pair found in 2^26.43: 00b848c1a424882f
Pair found in 2^28.54: 180b48c1a4245a09
Pair found in 2^26.78: 1ee948c1a4246b1d
Pair found in 2^25.81: 226848c1a424362e
Pair found in 2^27.56: 2e3548c1a424f161
Subkey lower nibbles recovered:
d42c
d515
Actual subkey lower nibbles:
d42c d515
1344 seconds elapsed
```

Extend to 9 rounds?

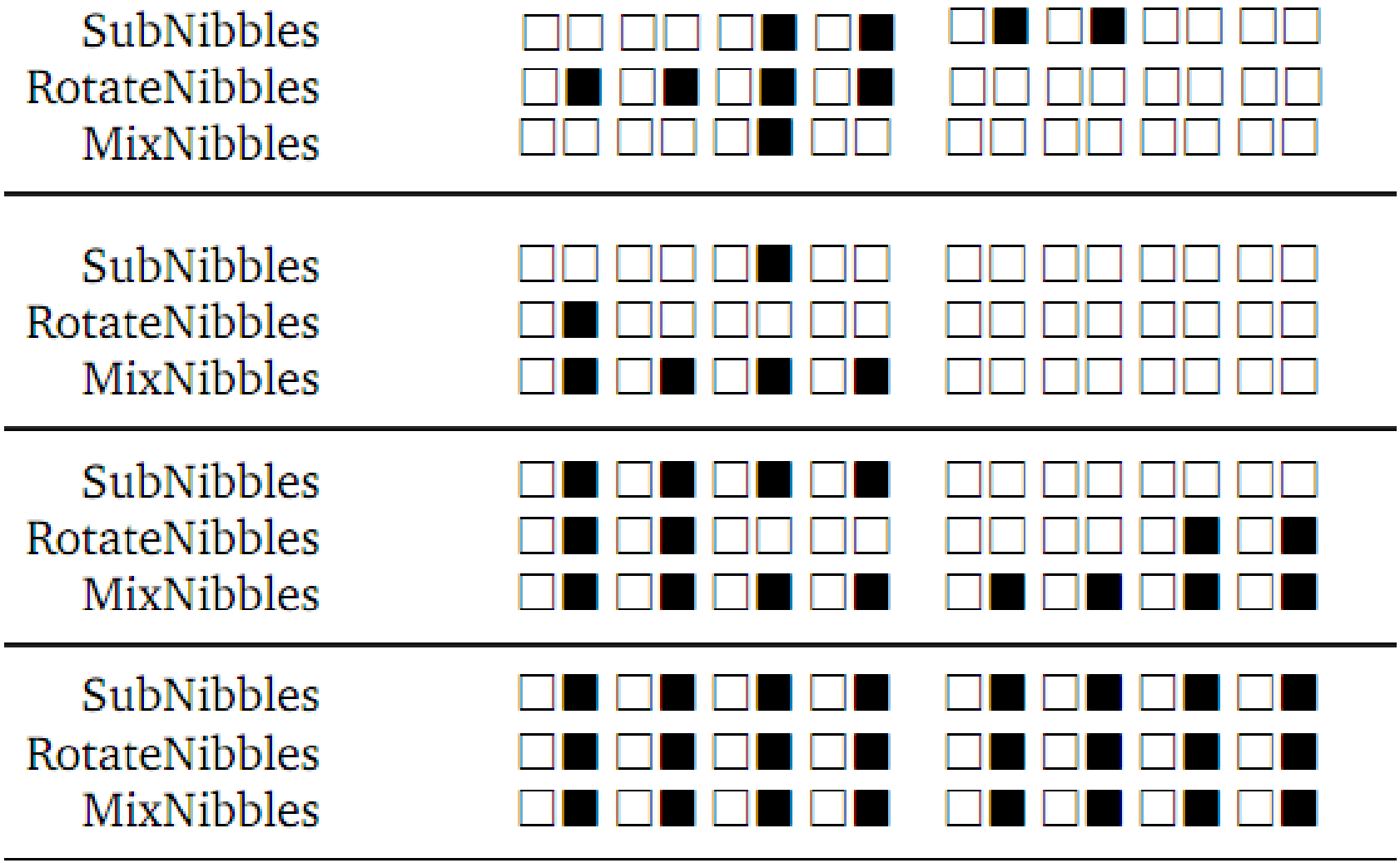
(work in progress with Y. Sasaki)

Prepend a round here



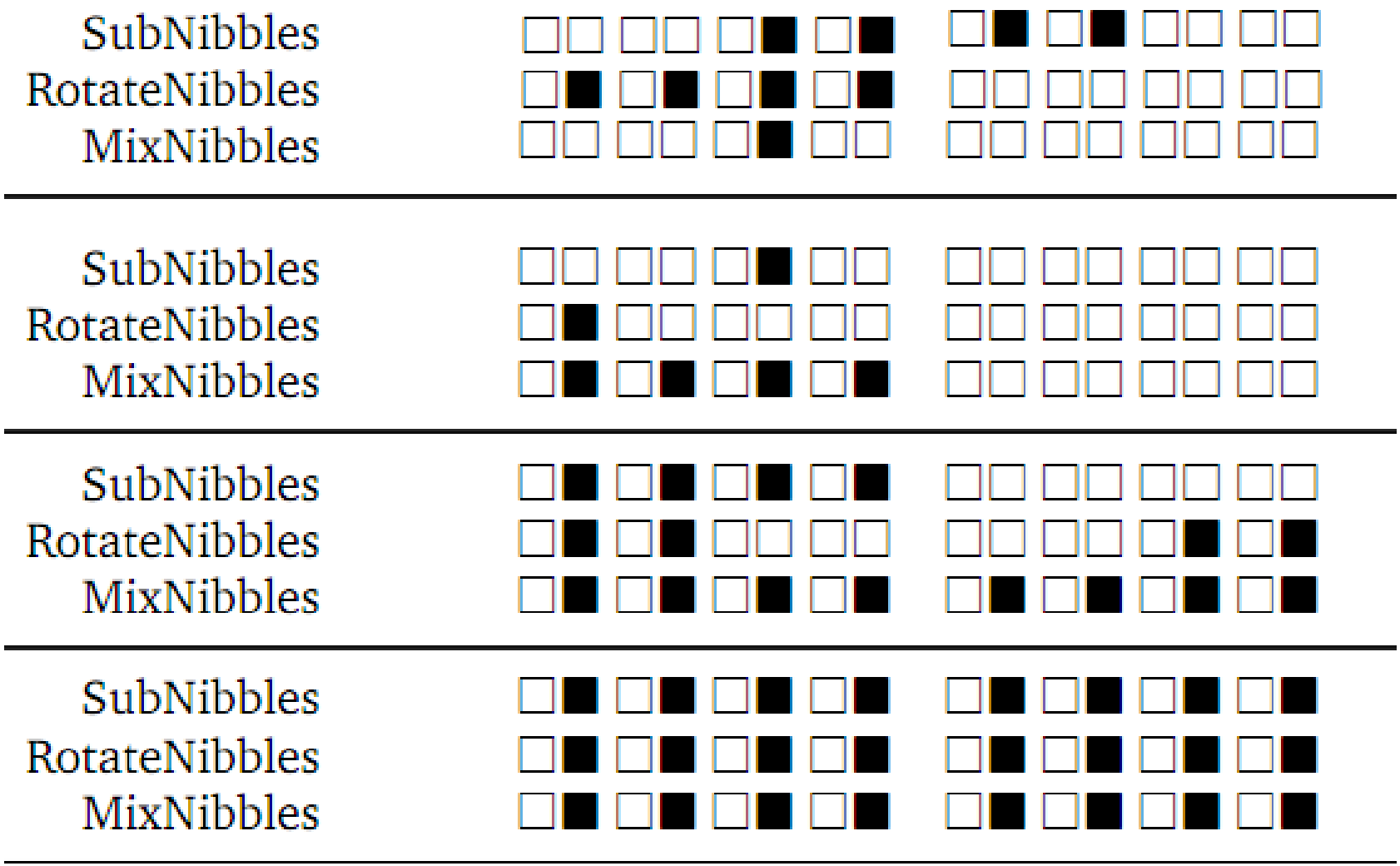
Guess 16 subkey bits of first subkey

Success ⇔ good post-SubNibbles difference



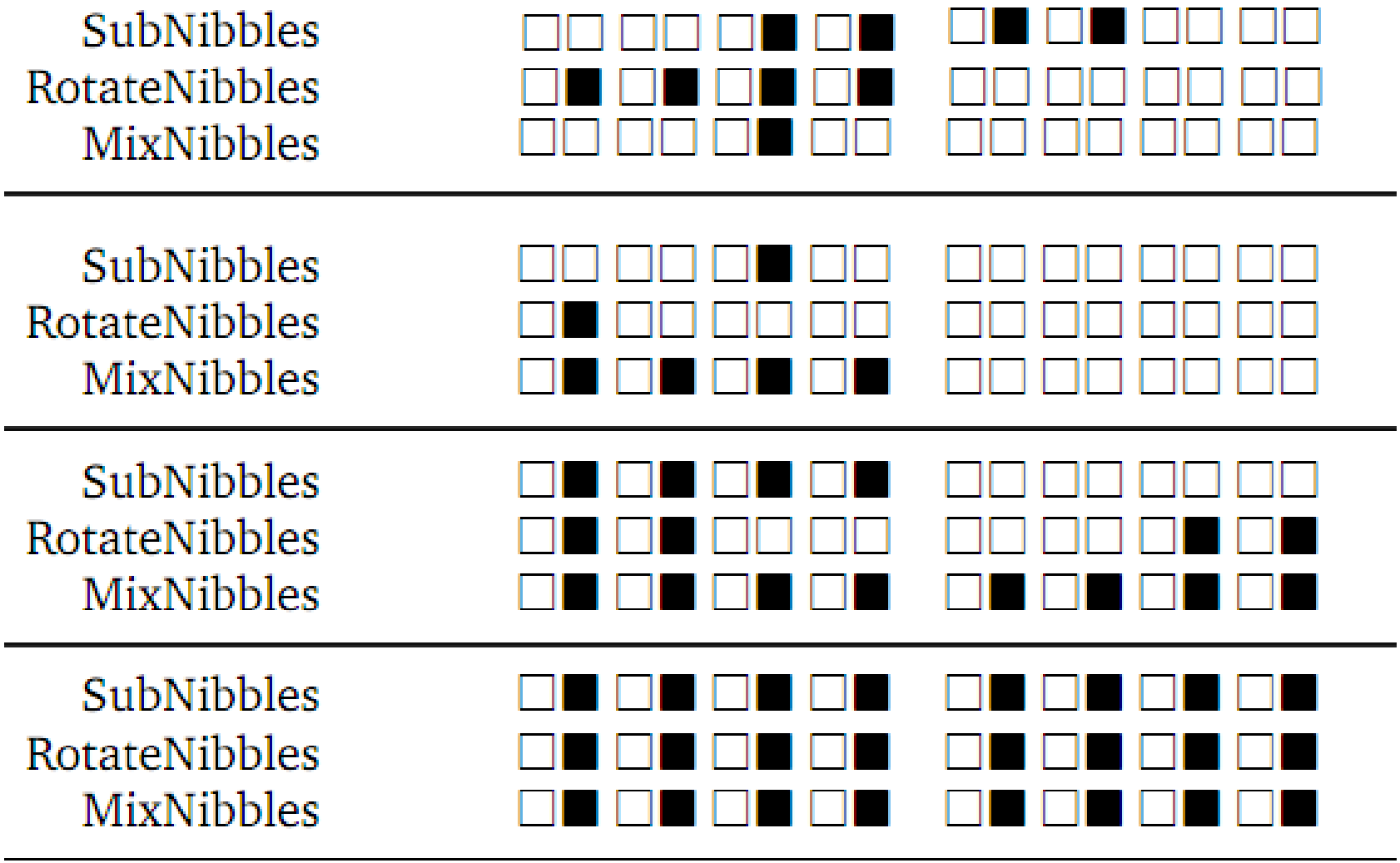
Correct guess + correct pair => 1st round passed

Use structure to reduce data cplexity



After 1st round, same attack as on 8 rounds, without message modification (filtering still possible)

To be verified…



8-round attacks claimed at INSCRYPT 2011

- Similar first-round trick
- Unverified probabilities

INSCRYPT 2011

In Cooperation with IACR

Nov. 30 - Dec. 3, 2011, Beijing

	Feng	and F-FCSR-H v3
48	Nan Li, Yi Mu and Willy Susilo	Efficient Self-Certified Signatures with Batch Verification
49	Jiang Zhang, Xiang Xie, Rui Zhang and Zhenfeng Zhang	A Generic Construction from Selective-IBE to Public-Key Encryption with Non-interactive Opening
53	Xusheng Zhang, Shan Chen and Dongdai Lin	Fast Tate Pairing Computation on Twisted Jacobi Intersections Curves
54	Shao-Zhen Chen and Yi-Bin Dai	Weak-Key Class of MISTY1 for Related-Key Differential Attack
55	Xiaoli Yu, Wenling Wu, Yanjun Li and Lei Zhang	Cryptanalysis of Reduced-Round KLEIN Block Cipher

TODO

- Analyze/implement 9-round attack
- What about hashing modes (DM etc.)?
- 10+ rounds can probably be attacked in <2^64