Practical Attack on 8 Rounds of the Lightweight Block Cipher KLEIN

Jean-Philippe Aumasson

NAGRA, Switzerland

-

María Naya-Plasencia

FHNW, Windisch, Switzerland and University of Versailles, France

-

Markku-Juhani O. Saarinen

Revere Security, USA

INDOCRYPT 2011

Chennai, India – 12 December 2011

KLEIN

KLEIN is a lightweight block cipher family by Z. Gong, S. Nikova, and Y. Wei Law, presented at RFIDSec 2011.

KLEIN has a 64-bit block and versions with 64-, 80-, and 96-bit keys with 12, 16, or 20 rounds, respectively.

A KLEIN round is composed of the following steps:

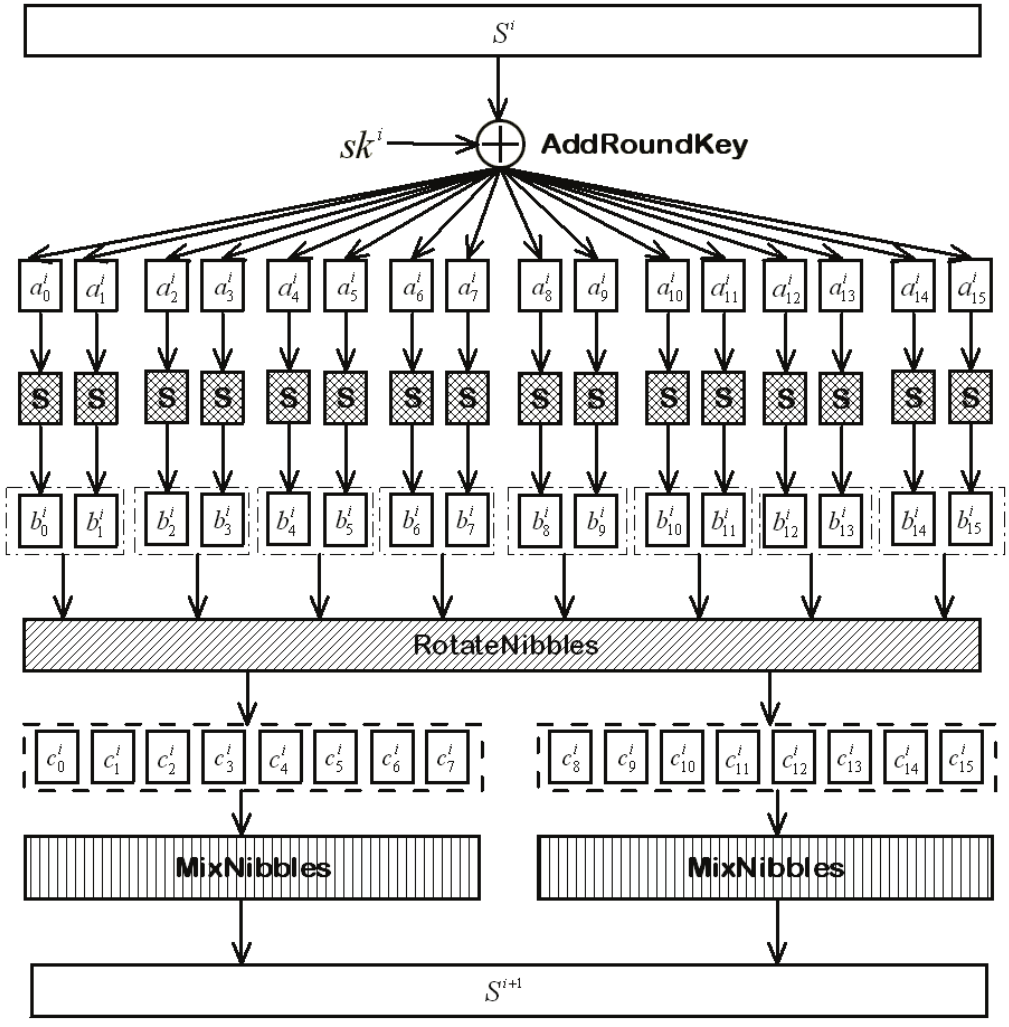
1. *AddRoundKey*: XORs a round key to the 64-bit state.
2. *SubNibbles*: Apply the 4-bit Sbox to each nibble.
3. *RotateNibbles*: Left-rotate the state by 16 bits.
4. *MixNibbles*: Apply two *MixColumn*'s in parallel.

The Sbox used by KLEIN

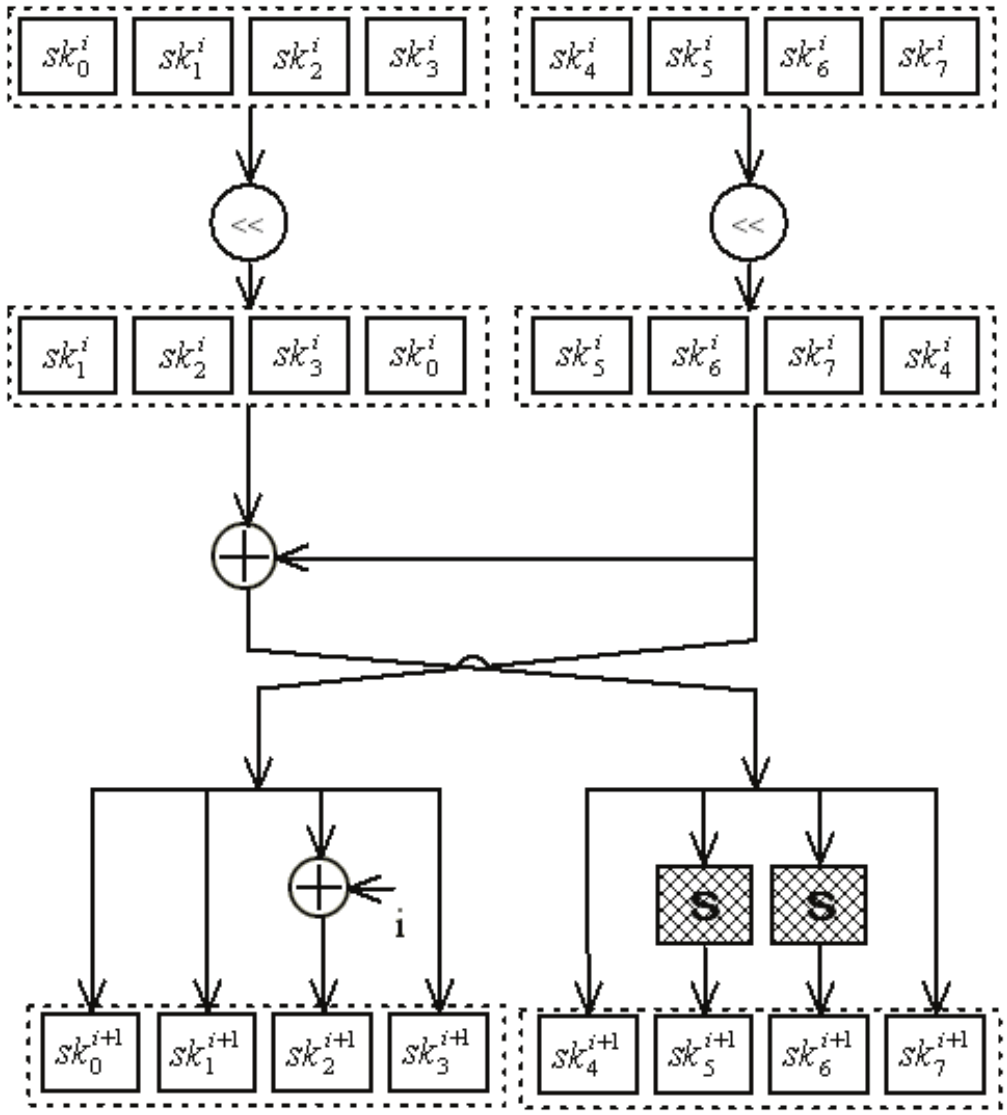
- There is only one S-Box used by KLEIN.
- The S-Box is an ivolution (it's own inverse).
- Found by exhaustive search through all possible 4×4 - bit involutions.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	7	4	a	9	1	f	b	0	c	3	2	6	8	e	d	5

KLEIN Round Function



KLEIN Key Schedule



KLEIN: Differential Cryptanalysis

Differential cryptanalysis has been one of the strongest methods to attack symmetric crypto primitives for the last 20 years.

Security against differential attacks is typically proven by showing lower bounds on the probability of a differential characteristic.

Theorem: Any 4-round differential characteristic of KLEIN has a maximum probability of 2^{-30}.

(This is Lemma 1 in the original KLEIN paper)

KLEIN: Differential Cryptanalysis

Differential cryptanalysis has been one of the strongest methods to attack symmetric crypto primitives for the last 20 years.

Security against differential attacks is typically proven by showing lower bounds on the probability of a differential characteristic.

Theorem: Any 4-round differential characteristic of KLEIN has a maximum probability of 2^{-30}.

To bypass this bound, we use a **collection of characteristics**.

- 4 rounds with probability $2^{-16.45}$!

Observations

Observation 1. If the difference entering MixColumn is of the form `0000000X` where `X` represents a non-zero difference in $\{1, \ldots, 7\}$ – i.e. a nibble with null MSB – then the output difference is of the form `0Y0Y0Y0Y`, where the wildcard `Y` represents a non-zero difference. That is, higher nibbles remain free of difference.

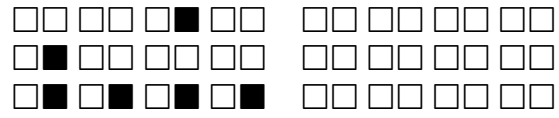
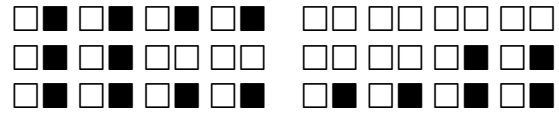
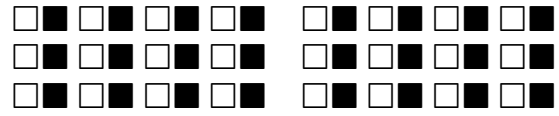
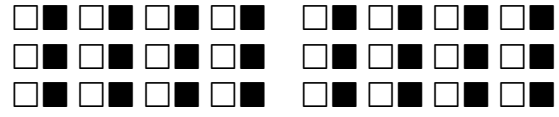
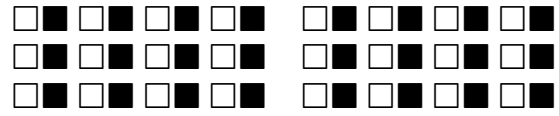
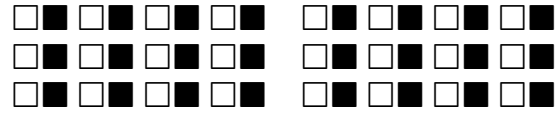
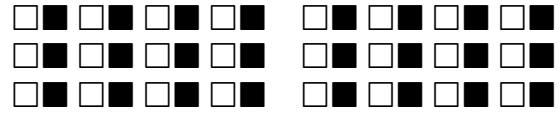
Observation 2. If the difference entering MixColumn is of the form `0X0X0X0X` where the wildcard `X` represents a difference in $\{0, \ldots, 7\}$, then the output difference is of the form `0Y0Y0Y0Y`, where `Y` represents a possibly null difference. Furthermore, the average number of non-zero `Y`'s is 3.75, as one can experimentally verify. For example, the input difference `04020405` leads to the output difference `0f090100`.

Observations

Observation 3. If the difference entering MixColumn is of the form `0X0X0X0X` where the wildcard `X` represents a difference in $\{8, \ldots, f\}$, then the output difference is of the form `0Y0Y0Y0Y`, where `Y` represents a (possibly zero) difference. Furthermore, the average number of non-zero `Y`'s is 3.75. Note that, unlike Observation 2, an `X` cannot be zero. For example, the input difference `0c0a080f` leads to the output difference `010f0708`.

Observation 4. Given a random difference, KLEIN's Sbox returns a difference in $\{1, \ldots, 7\}$ with probability $7/15 \approx 2^{-1.1}$, for a random input. If the difference is `b` or `e`, the probability is $3/4 \approx 2^{-0.42}$. These values can be verified either experimentally or using the difference distribution table in the original KLEIN paper.

A Collection of Differential Characteristics

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		$p_7 \approx 2^{-5.82}$	$2^{-33.90}$

Finding More Right Pairs with Neutral Bits

- A bit is said to be *neutral* with respect to a given differential (characteristic) when flipping this bit in an input conforming to the differential (characteristic) leads to a new input also conforming to that differential.
- In KLEIN, one can observe that the first two and last two input bytes in a plaintext block are neutral with respect to the first two rounds' collection of characteristics.
- Therefore, for example, after a 2^{28} effort to find a pair satisfying the 6-round differential, one can derive 2^{32} pairs for which the full differential is followed with probability $2^{-28.06+4.80} = 2^{23.26}$.

Expanding to Seven and Eight Rounds

- We observe that for a pair conforming to the 6-round differential, the *SubNibbles* of round 7 has all higher nibbles inactive. Therefore a 7-round distinguisher can be built with the same 2^{28} observations data complexity.
- In the eight-round attack one first collects approximately $2^{33.90}$ pairs, and records the ones that conform to the output difference as per our collection of characteristics.
- One expects to record approximately 4 pairs satisfying the difference by chance, and one conforming to the collection of characteristics. The conforming pair can be identified using the neutral bits.

Key Recovery for Eight Rounds

- The attack exploits the invertibility of the final *MixNibbles* and *RotateNibbles* to determine the output differences of each nibble after the last *SubNibbles* (i.e. that of the seventh round.)
- With approximately 2^{34} encryptions, one can identify a conforming pair with high probability.
- Using neutral bits, one expects to produce approximately 8 other conforming pairs after 2^{32} trials. This is more than enough to identify with certainty 32 bits of the last subkey.
- Overall, the 64 bits of the last subkey (and thus of the original key) can be found with complexity below 2^{35} encryptions.

Experimental verification

```
$ ./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
```

Conclusion

- We presented practical, experimentally verified attacks on the lightweight cipher KLEIN-64 reduced to up to 8 rounds, out of 12 in total.
- Our attack is made possible by a high-probability differential described as a large collection of differential characteristics.
- Our results suggest that combining a 4-bit S-Box (as used in Serpent) with the byte-oriented MixColumn linear layer (as used in Rijndael / AES) is not an optimal strategy, as far as security is concerned.
- This work is the first third-party analysis of KLEIN published (to our best knowledge). Future works may seek to extend our attacks to more rounds of KLEIN.