Max
Planck
Institute
for
Software Systems

TweLEX: A tweaked version of the LEX stream cipher

Mainack Mondal,
MPI-SWS, Germany

Avik Chakraborti, Nilanjan Datta
ISI, Kolkata , India

and

Debdeep Mukhopadhyay
IIT Kharagpur, India

WISSec 2010, Nijmegen
29th November, 2010

Outline

- Leak Extraction and LEX
- Related key cryptanalysis of LEX.
- TweLEX: Modification of LEX.
- Future work

Outline

- Leak Extraction and LEX
- Related key cryptanalysis of LEX.
- TweLEX: Modification of LEX.
- Future work

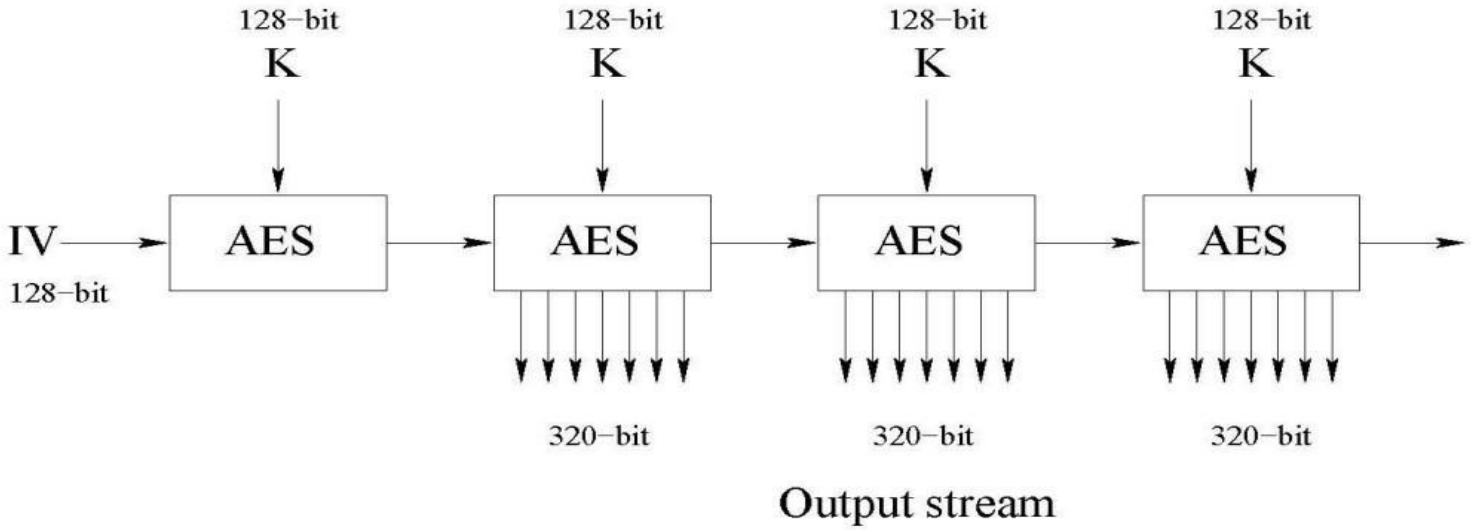
Leak Extraction and LEX

- Block ciphers and Stream ciphers are conceptually different.
- But they serve the same purpose.
- Can we combine them to get some new ciphers?

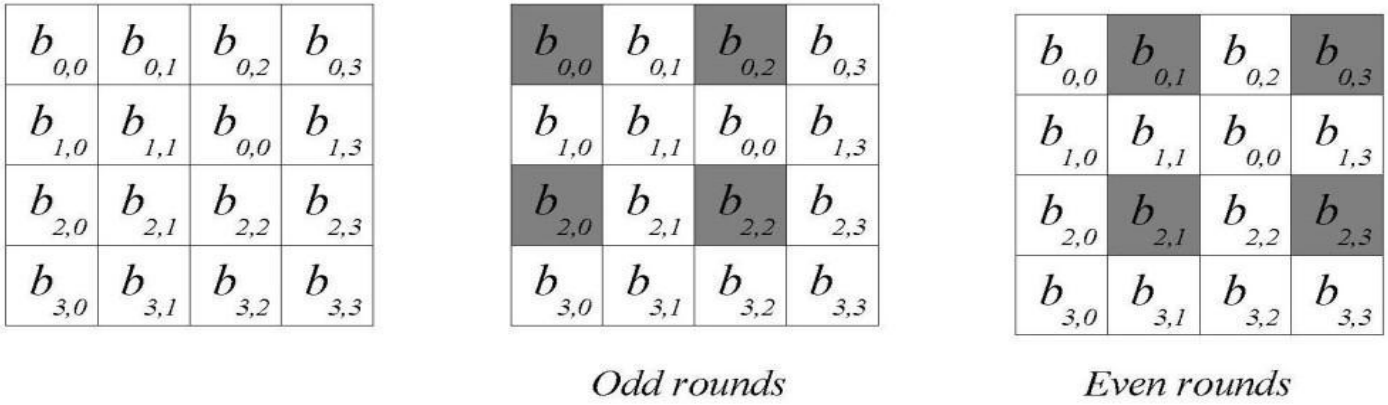
Leak Extraction and LEX

- Alex Biryukov : A new method called 'Leak EXtraction'
  - Run a Block Cipher in Output Feed Back (OFB) mode.
  - Take some bits from internal states of block cipher and output as key stream.
- Used it on AES and called the resulting stream cipher LEX.

Leak Extraction and LEX



Leak Extraction and LEX



Leak Extraction and LEX

- Advantages:
  - Speed-up using existing hardware/software.
  - Reuse existing implementations.
  - Reuse countermeasures.

Leak Extraction and LEX

- Several cryptanalytic efforts on LEX.
- Best known attack on LEX
  - Orr Dunkelman et al [ASIACRYPT, 2008]:
    - Differential cryptanalysis of LEX.

Outline

- Leak Extraction and LEX
- Related key cryptanalysis of LEX.
- TweLEX: Modification of LEX.
- Future work

Related key cryptanalysis of LEX

- LEX use the same key schedule as AES - 128.
- Given, $\alpha = [a \quad b \quad c \quad d]^T, \beta = \text{SubByte}(\alpha >>> 8)$

  We observe the following differential trail in AES - 128 key schedule:

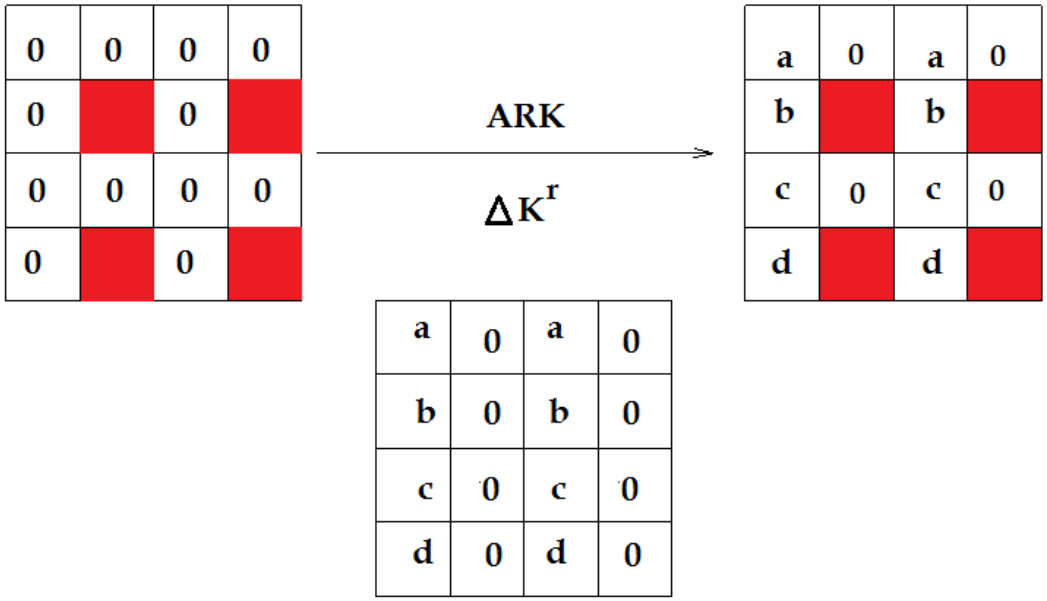
$$(\alpha \oplus \beta, \beta, 0, 0)$$
$$(\alpha \oplus \beta, \alpha, \alpha, \alpha)$$
$$(\alpha, 0, \alpha, 0)$$
$$(\alpha, \alpha, 0, 0)$$
$$(\alpha, 0, 0, 0)$$
$$(\alpha, \alpha, \alpha, \alpha)$$

Related key cryptanalysis of LEX

- Consider two key streams of LEX under related keys K and K*
- we search for a special difference pattern in LEX state matrices.

Related key cryptanalysis of LEX

- Consider two key streams of LEX under related keys K and K*
- we search for a special difference pattern in LEX state matrices.



Related key cryptanalysis of LEX

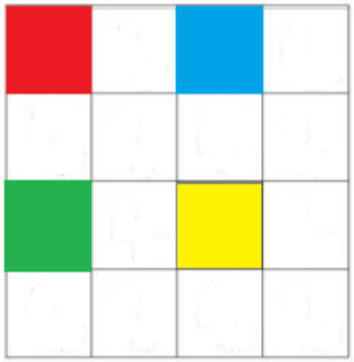
- We use
  - Differential trail in key schedule.
  - Difference pattern in state matrices.
- We retrieve,
  - 24 hidden state bytes.
  - Time complexity 2^{96}.

Outline

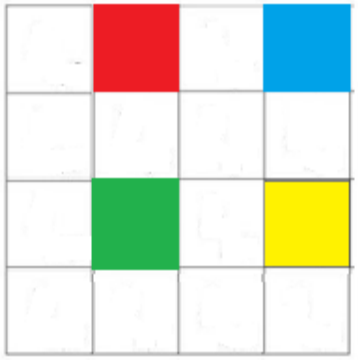
- Leak Extraction and LEX
- Related key cryptanalysis of LEX.
- TweLEX: Modification of LEX.
- Future work

TweLEX: Modification of LEX

- We Tweaked LEX a little: TweLEX
- LEX:



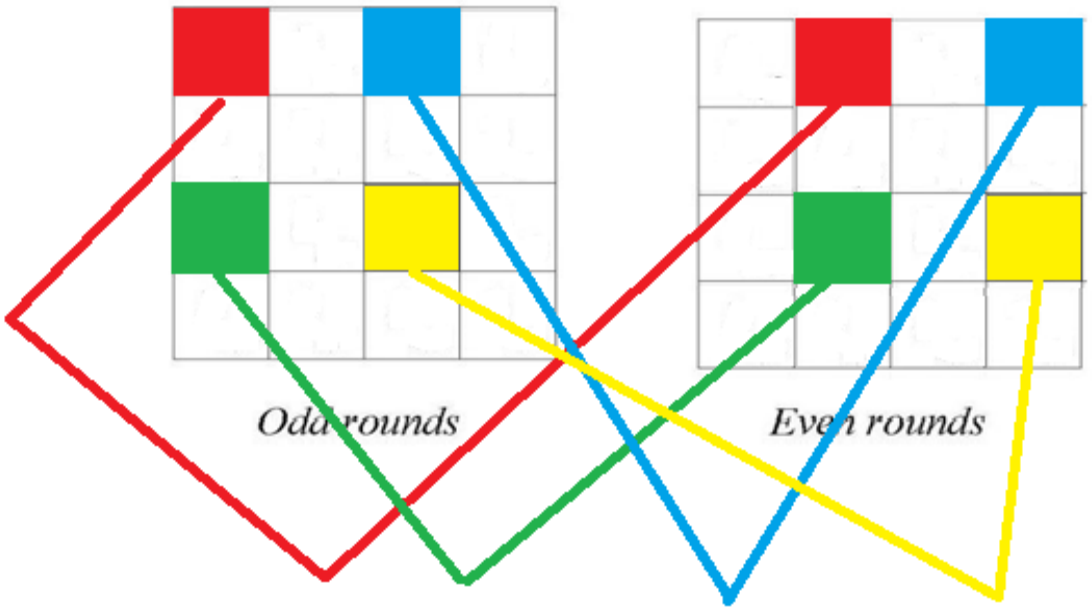
Odd rounds



Even rounds

TweLEX: Modification of LEX

- TweLEX:



TweLEX: Modification of LEX

- Advantages
  - Prevent Dunkelman's attack.
  - Prevent related key attack presented in this paper.
  - Almost no modification of original LEX implementation.

TweLEX: Modification of LEX

- Disadvantage
  - Slow compared to LEX.
    - LEX – 320 bits / AES Encryption
    - TweLEX – 160 bits / AES Encryption
    - AES – 128 bits / AES Encryption

Outline

- Leak Extraction and LEX
- Related key cryptanalysis of LEX.
- TweLEX: Modification of LEX.
- Future work.

Future work

- Explore Leak Extraction further.
- Explore the security of TweLEX in depth.

Questions?

Contact:

mainack@mpi-sws.org

debdeep@cse.iitkgp.ernet.in

Detailed Report:

http://www.mpi-sws.org/~mainack/MtechThesis.pdf

Thank You !