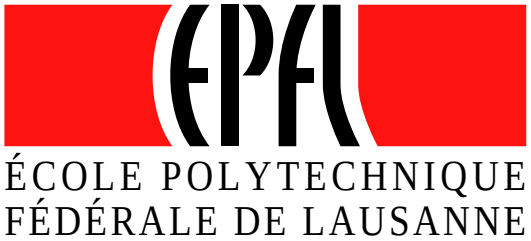
FOX: a New Family of Block Ciphers

Pascal Junod and Serge Vaudenay



Selected Areas in Cryptography '04

University of Waterloo (Canada), August 9, 2004

Outline of this talk

- Preliminaries
- Description of the ciphers
- Security results
- Implementation issues

Do we *really* need new block ciphers ?

- AES, NESSIE, CRYPTREC efforts → many “good” designs
- Most of them (probably) practically secure
- All of them sufficiently fast

So why FOX ?

- Commercial reasons: project initiated by

- Current trends we would like to avoid:
  - Light-weight key schedule algorithms
  - Algebraic constructions for S-boxes

Requirements

- 64-bit and 128-bit block sizes
- Efficient on 8-bit, 32/64-bit architectures, hardware
- Modest RAM/ROM consumption on low-cost architectures
- SECURE !

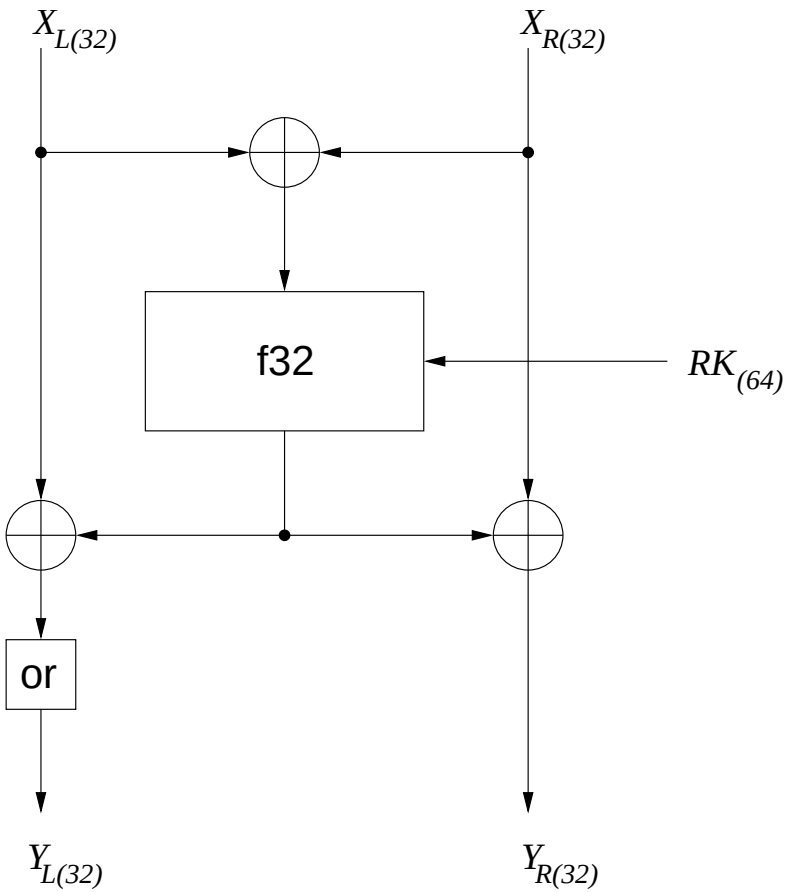
FOX Family of Algorithms

- FOX family : *two* block ciphers
- FOX64 with a 64-bit block size
- FOX128 with a 128-bit block size
- Key length : 0 $\longrightarrow$ 256 bits (multiple of 8)
- Variable rounds number (12 $\longrightarrow$ 255)
- “Generic” versions of FOX: 16 rounds

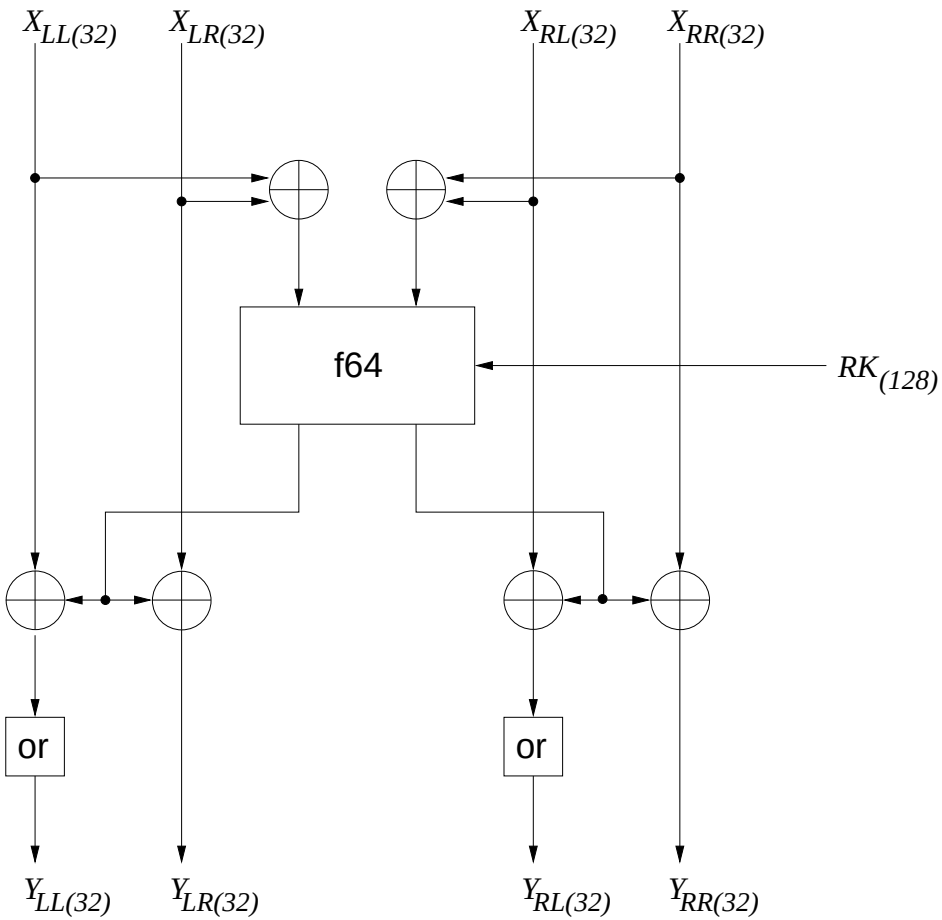
Lai-Massey Scheme

- Lai-Massey scheme with an *orthomorphism*
- Orthormorphism: 1-round Feistel scheme with the identity as round function
- Orthomorphism omitted in the last round

Lai-Massey Scheme (64-bit)



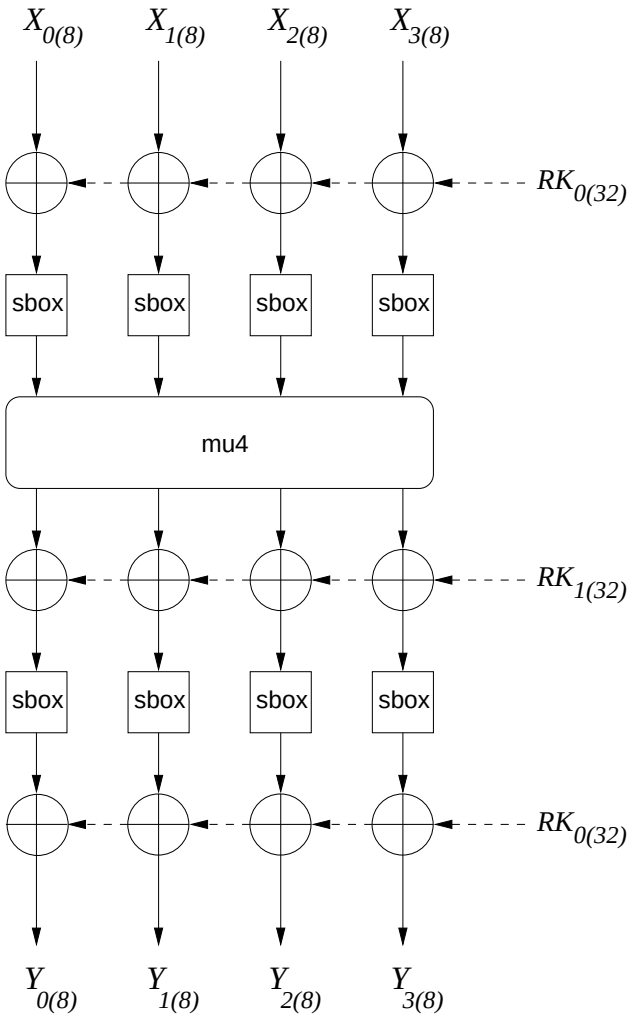
Lai-Massey Scheme (128-bit)



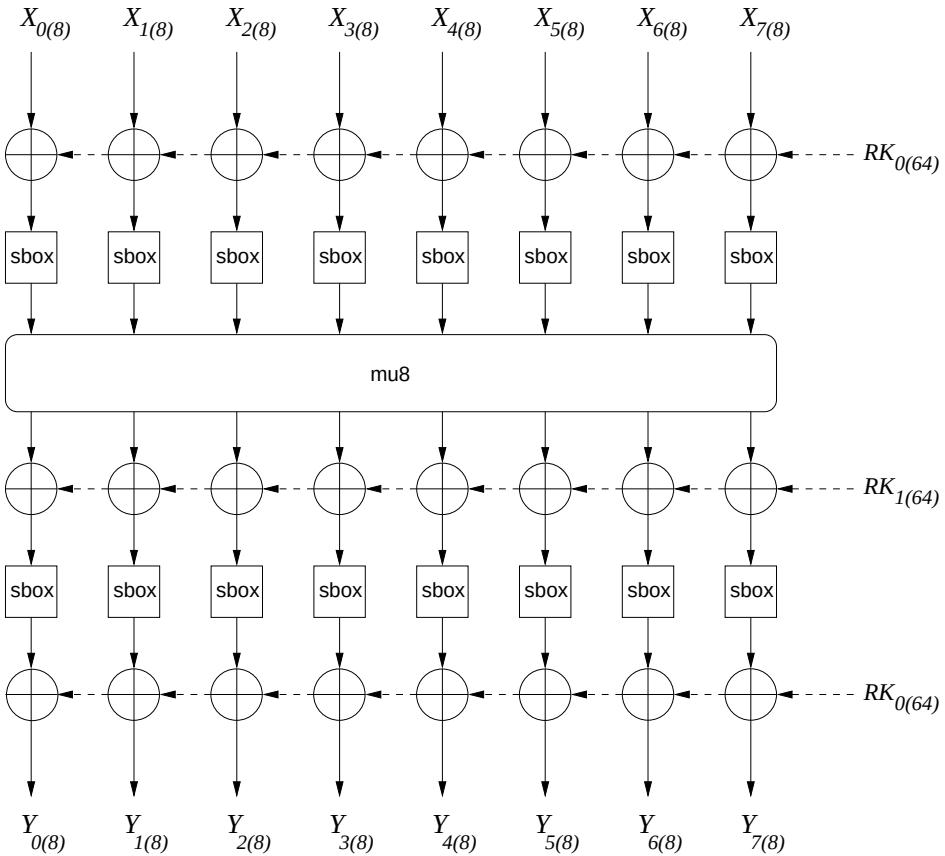
Round Functions

- Based on a Substitution-Permutation Network
- Confusion ensured by 8-bit S-boxes
- Diffusion ensured by a multipermutation (aka MDS matrix)
- Key material combined with XOR operations

FOX64 Round Function



FOX128 Round Function



S-box

- 3-round Lai-Massey scheme
- Round functions are pseudo-randomly generated permutations on $\mathrm{GF}(2^4)$
- $\mathrm{DP}_{\max}^{\text{sbox}} = \mathrm{LP}_{\max}^{\text{sbox}} = 2^{-4}$
- Algebraic degree equal to 6

MDS Matrices

- Linear multipermutations on $\mathrm{GF}(2^8)^n$
- Generated according to my first talk !

$$\text{mu4} \triangleq \begin{pmatrix} \texttt{0x01} & \texttt{0x01} & \texttt{0x01} & \texttt{0x02} \\ \texttt{0x01} & \texttt{0xFD} & \texttt{0x02} & \texttt{0x01} \\ \texttt{0xFD} & \texttt{0x02} & \texttt{0x01} & \texttt{0x01} \\ \texttt{0x02} & \texttt{0x01} & \texttt{0xFD} & \texttt{0x01} \end{pmatrix}$$

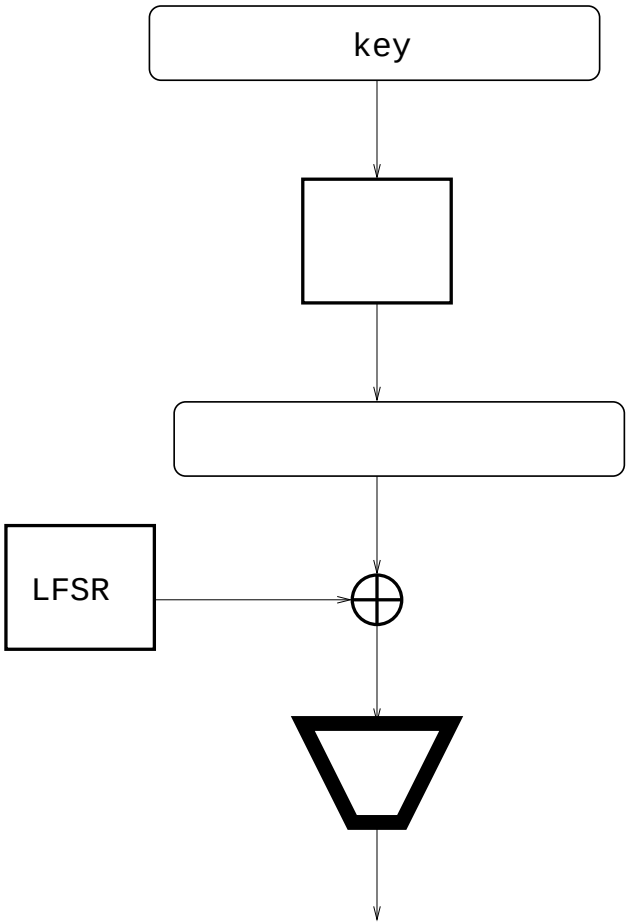
MDS Matrices (2)

$$\text{mu8} \triangleq \begin{pmatrix} 0x01 & 0x01 & 0x01 & 0x01 & 0x01 & 0x01 & 0x01 & 0x03 \\ 0x01 & 0x03 & 0x82 & 0x02 & 0x04 & 0xFC & 0x7E & 0x01 \\ 0x03 & 0x82 & 0x02 & 0x04 & 0xFC & 0x7E & 0x01 & 0x01 \\ 0x82 & 0x02 & 0x04 & 0xFC & 0x7E & 0x01 & 0x03 & 0x01 \\ 0x02 & 0x04 & 0xFC & 0x7E & 0x01 & 0x03 & 0x82 & 0x01 \\ 0x04 & 0xFC & 0x7E & 0x01 & 0x03 & 0x82 & 0x02 & 0x01 \\ 0xFC & 0x7E & 0x01 & 0x03 & 0x82 & 0x02 & 0x04 & 0x01 \\ 0x7E & 0x01 & 0x03 & 0x82 & 0x02 & 0x04 & 0xFC & 0x01 \end{pmatrix}$$

Key Schedule Algorithms

- “Strong” key-schedule algorithms
- Three different versions : KS64, KS64h, and KS128
- Time to compute the subkeys = time to encrypt 6 blocks (12 for KS64h)
- No penalty in the decryption direction (on-the-fly computation)
- Recycling of the components of the round functions

Key Schedule : Skeleton



So, why ... ?

- ... FOX's key-schedule looks like ...

Because ...

- Not especially required for linear/differential cryptanalysis, but ...
- ... more and more frequently, a “light” key-schedule is used to gain one, two, three, ... more rounds during an attack.
- Examples: Muller’s attack against Khazad (Asiacrypt’03), Phan’s impossible differential attack against AES (ILP’04), and many more...
- We estimate that the loss of key agility remains modest.

Lai-Massey and Luby-Rackoff

- Results available for the Lai-Massey scheme in the Luby-Rackoff model
- Equivalent security than for the Feistel scheme
- ***Theorem (Vaudenay, Asiacrypt'99)***
  If or *is an orthomorphism, then the Lai-Massey scheme equipped with independent random round functions is pseudo-random after 3 rounds and super-pseudorandom after 4 rounds.*

Linear/Differential Cryptanalysis

- Easy fact about the Lai-Massey scheme:
- ***Theorem***
  Any differential (linear) characteristic on two rounds must involve at least one round function.
- Using standard results of Hong *et al.* (FSE'00):
- ***Theorem***
  The differential (resp. linear) probability of any single-path characteristic in FOX64$/k/r$ *is upper bounded by* $(\mathrm{DP}_{\max}^{\mathrm{sbox}})^{2r}$ *(resp.* $(\mathrm{LP}_{\max}^{\mathrm{sbox}})^{2r}$*). Similarly, the bounds are* $(\mathrm{DP}_{\max}^{\mathrm{sbox}})^{4r}$ *(resp.* $(\mathrm{LP}_{\max}^{\mathrm{sbox}})^{4r}$*) for* FOX128$/k/r$*.*
- At least 12 rounds since $\mathrm{DP}_{\max}^{\mathrm{sbox}} = \mathrm{LP}_{\max}^{\mathrm{sbox}} = 2^{-4}$.

Integral Attacks

- Simple integral distinguisher on 3 rounds
- Integral distinguisher on 4 rounds (using large precomputed tables)
- Breaks 7 rounds of FOX64 (in 2^{192} ops) and 5 rounds of FOX128 (in 2^{128} ops)

Pure Algebraic S-boxes

- Used by most modern designs because of interesting non-linear properties.
- But ...

FOX S-Box

- Based on *small* three 4-bit S-boxes
- Courtois-Pieprzyk (Asiacrypt'02): *any* such small mapping can be written as an overdefined system of *at least* 21 quadratic equations.
- Checked: exactly 21 equations on $\mathrm{GF}(2)$
- Not aware of any overdefined system over $\mathrm{GF}(2^8)$
- Courtois-Pieprzyk attack *could* break members of the FOX family within a complexity of 2^{171} to 2^{192}.
- Hellman's time-memory tradeoff against any block cipher using 256-bit keys : $2^{\frac{2 \cdot 256}{3}} = 2^{171}$.

8-bit

- Example of an implementation of FOX64/16 on 8051:
  - 16 bytes of RAM
  - 896 bytes of ROM (included pre-computed subkeys)
  - 757 bytes of code
  - 3950 cycles to encrypt one block

32/64-bit

- FOX64/16 (written in pure ASM) needs 295 clock cycles on an Intel Pentium III to encrypt one block
- According to NESSIE's figures, FOX128/16 (written in C) is 30% faster than Camellia on Alpha 21264
- Taking 12 rounds (the minimal amount of rounds), one can find at least one member of the FOX family among the three fastest block ciphers on the common 32/64-bit architectures.

Have a glance at

```
http://lasecwww.epfl.ch
http://www.mediacrypt.com
http://crypto.junod.info
```

for the complete specifications and the very last news about FOX !

Any question ?