# Towards the Optimality of Feistel Ciphers with SP-Functions

Kyoji Shibutani[1] and Andrey Bogdanov[2]

[1]Sony Corporation, Japan

[2]DTU Compute, Denmark

WCC'13, April 2013

# Outline

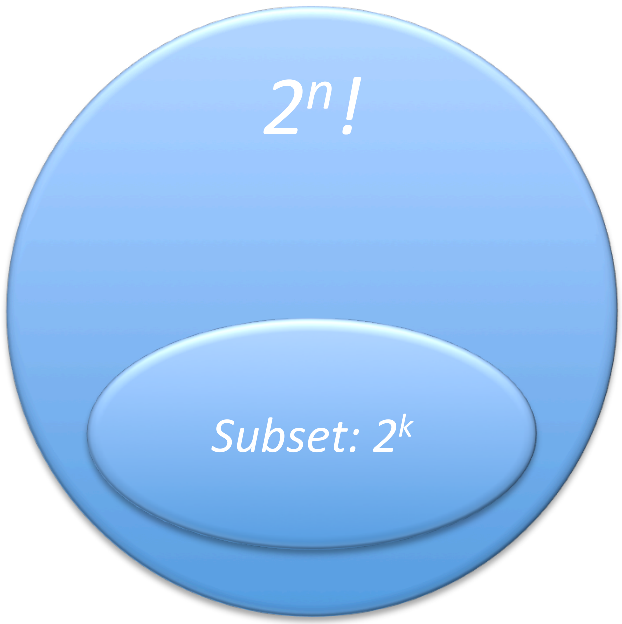
- **Balanced Feistel networks (BFNs)**
  - one of the most popular block cipher constructions
  - explore the optimality of BFNs with SP-type F-functions w.r.t. resistance against differential/linear attacks

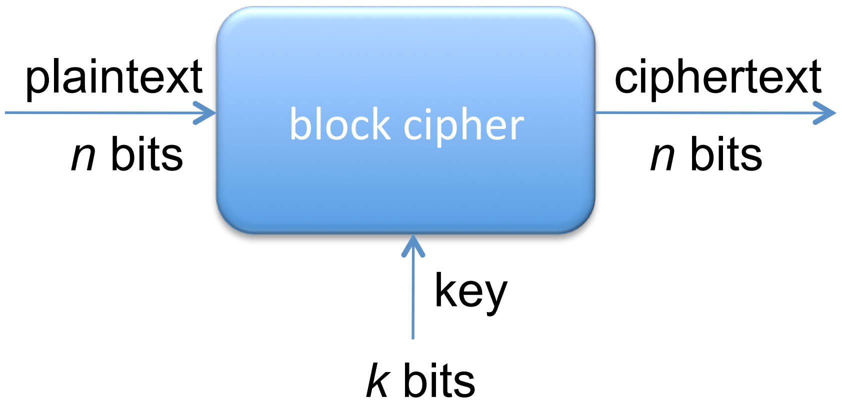
- **For a wide class of BFNs**
  - prove bounds on the number of active S-boxes
  - demonstrate their tightness with MDS
  - compare the efficiency w.r.t. the ratio between active S-boxes and all S-boxes
  - identify the optimal construction(s) in the class

# What is a block cipher?

**Block cipher**

*A block cipher with n-bit block and k-bit key is a subset of $2^k$ permutations among all $2^n!$ permutations on n bits.*



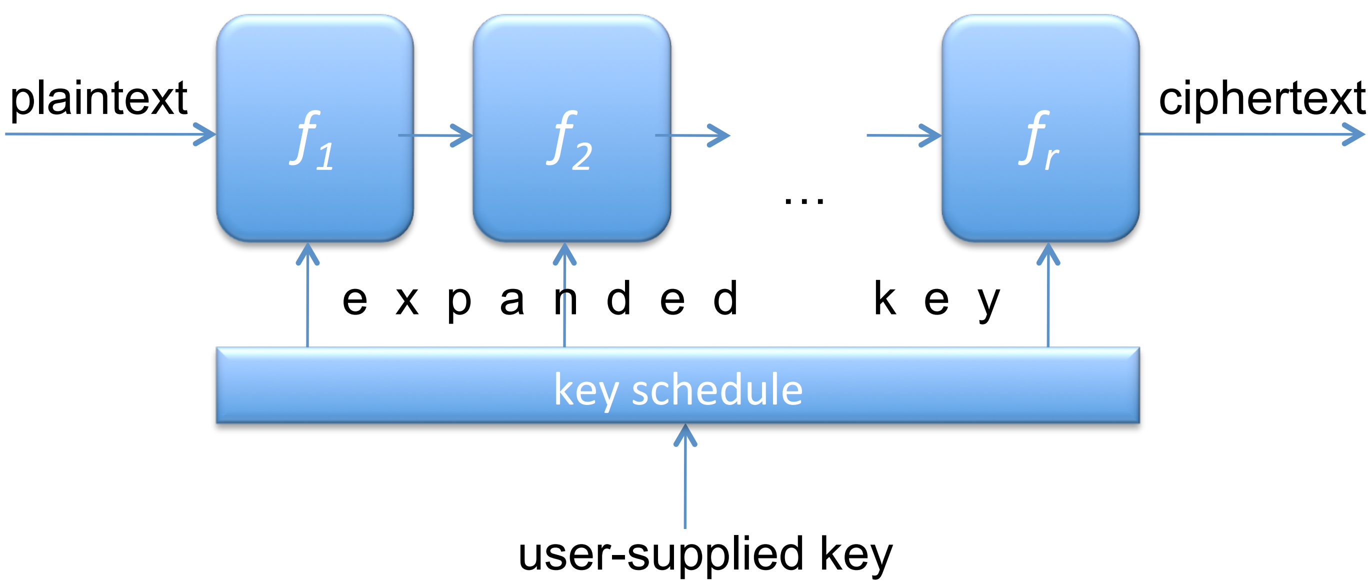
# Why block ciphers?

- Most basic security primitive in nearly all security solutions, e.g. used for constructing
  - stream ciphers,
  - hash functions,
  - message authentication codes,
  - authenticated encryption algorithms,
  - entropy extractors, …
- Probably the best understood cryptographic primitives
- All U.S. symmetric-key encryption standards and recommendations have block ciphers at their core: DES, AES

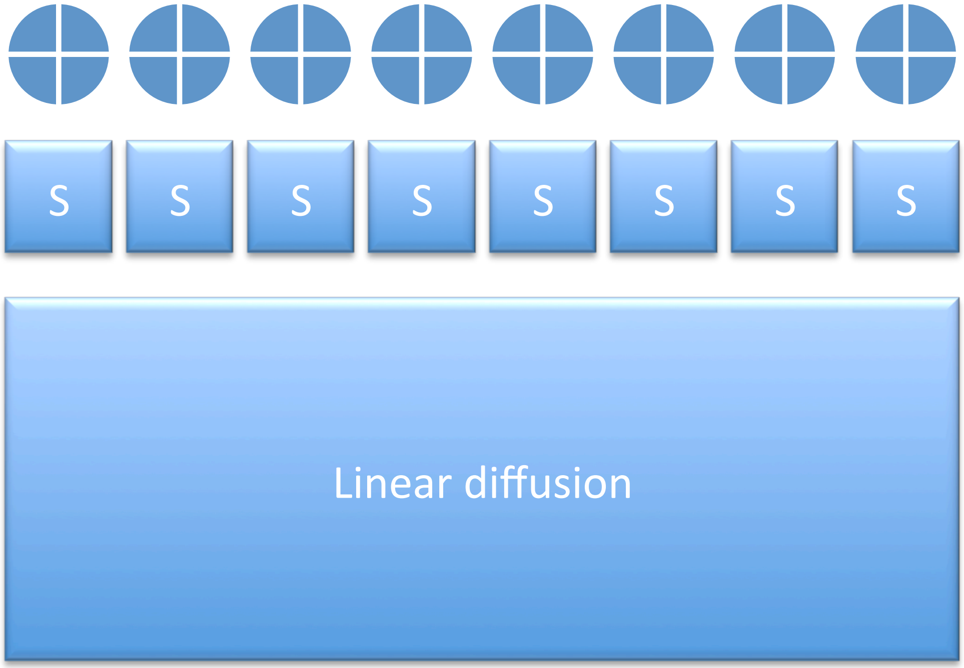
# Block ciphers: iterative construction

## Iterative block cipher and key schedule

*An iterative block cipher consists of r consecutive applications of simpler key-dependent transforms* $f = f_r \circ f_{r-1} \circ \ldots f_2 \circ f_1$



# Building blocks: Substitution-Permutation (SP) function




addition with subkey

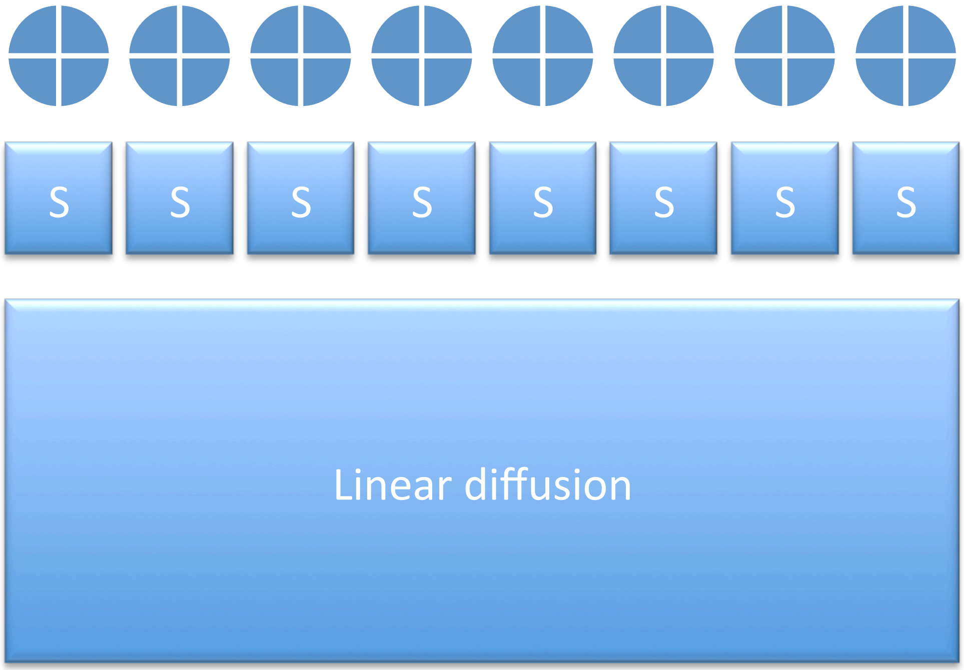
local nonlinear functions

linear operation:
bit permutation,
matrix-vector mult.

Used in many ciphers (DES, AES, Serpent, Present, Camellia, Clefia,…) and hash functions (Whirlwind, Groestl, Spongent, Photon, …)

# Round constructions: Substitution-Permutation networks

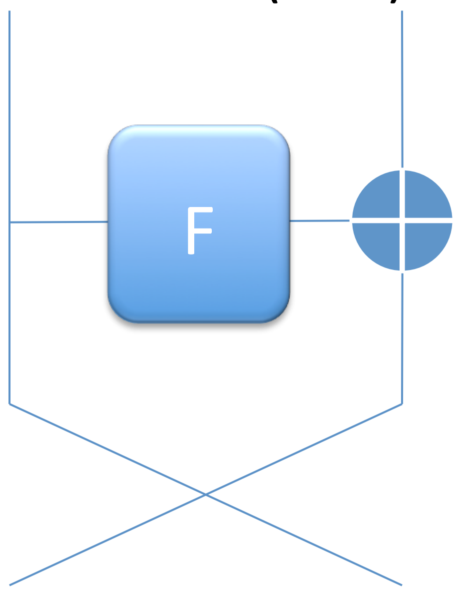
1 round = 1 SP-function




Used in AES (Rijndael), Serpent, Present, Groestl, Photon, Spongent, …

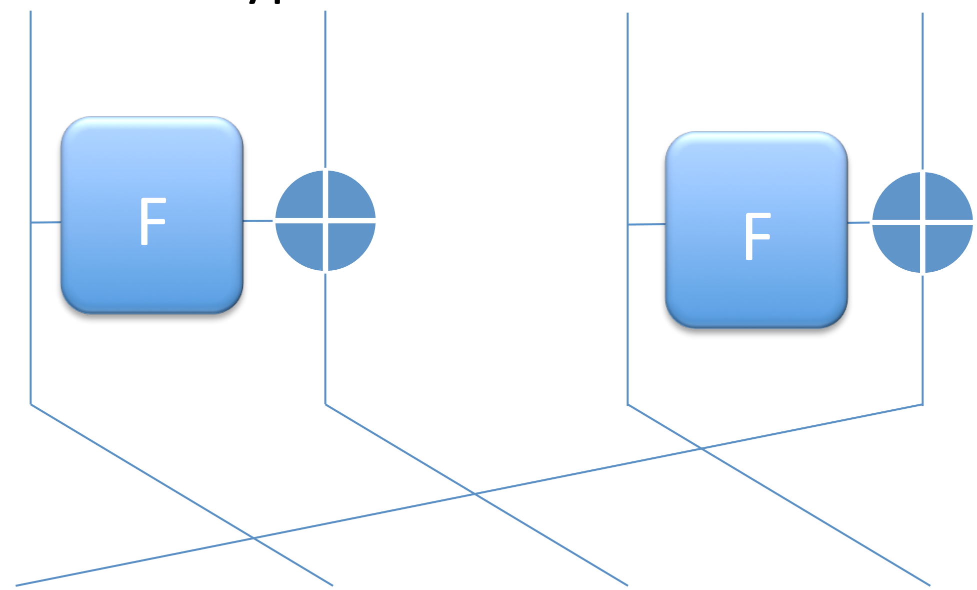
# Round constructions: Balanced and Generalized Feistel

Balanced Feistel Network (BFN)




Used in DES, Camellia, E2, Blowfish, Twofish, CAST128, KASUMI, MISTY, …

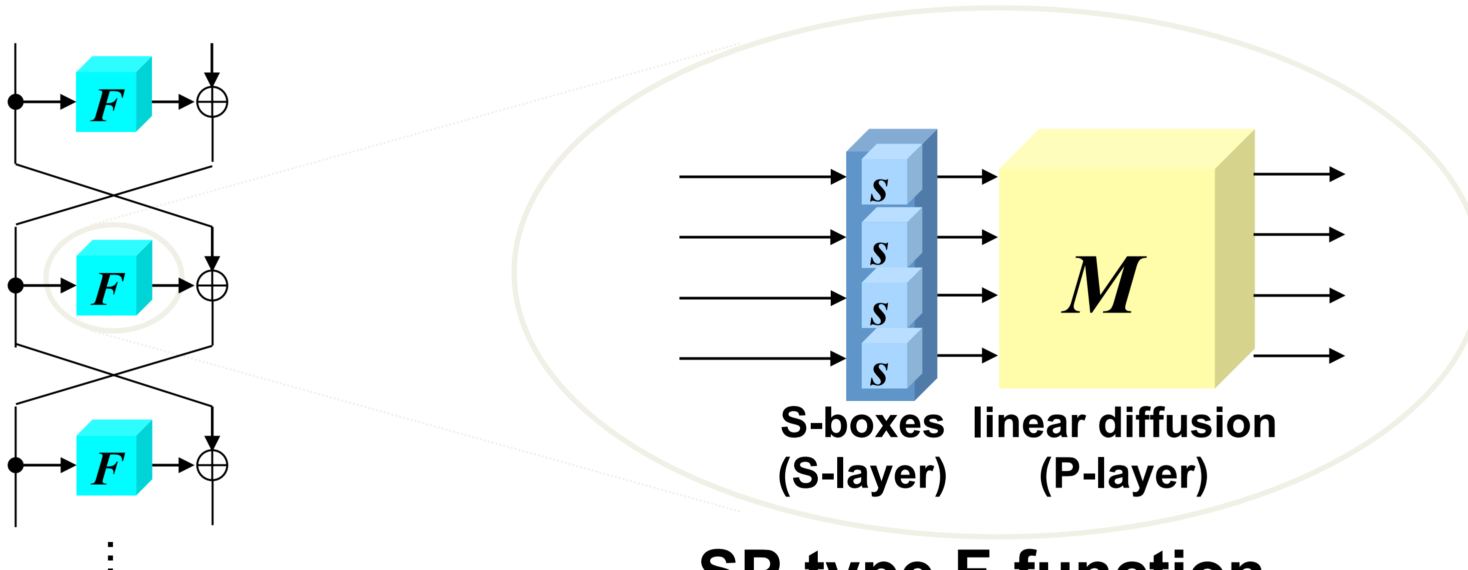
Generalized Feistel Network (GFN)
type-II 4-line GFN




Used in CLEFIA, SHAvite-3, RC6,…

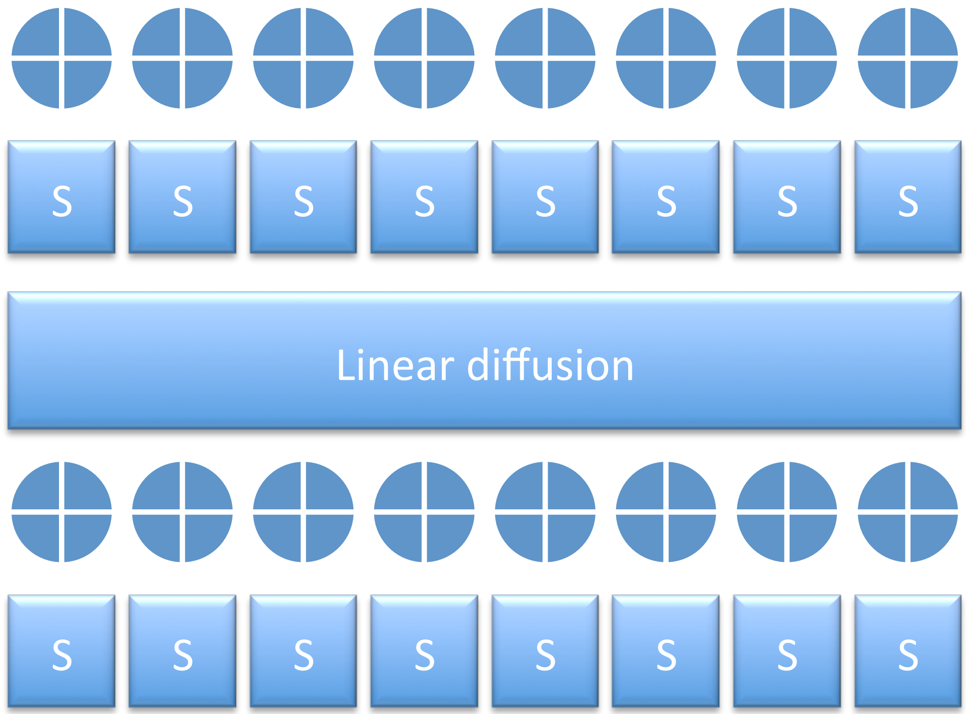
# Feistel with SP-type F-functions

- **Balanced Feistel networks (BFNs)**
  - DES, GOST, KASUMI, ...
- **Substitution-Permutation (SP) type F-function**
  - widely used (Twofish, Camellia, CLEFIA, ...)
  - bijective S-boxes + MDS matrix




**SP-type F-function**

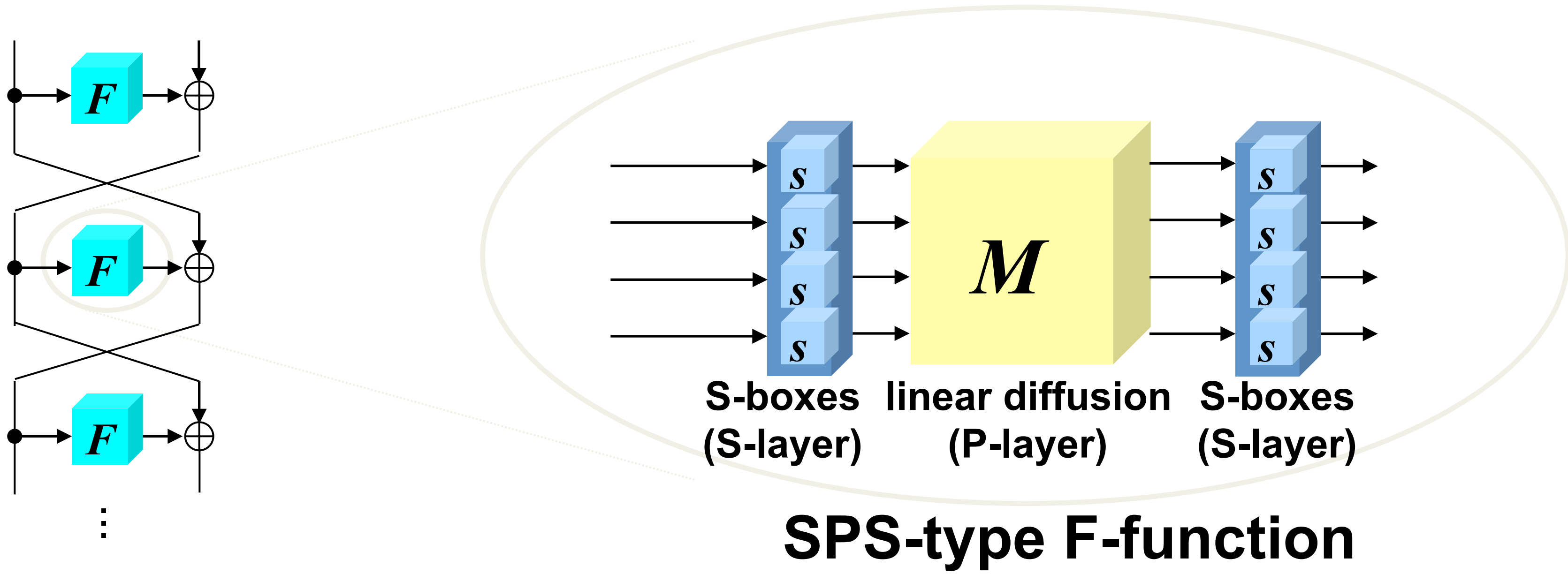
# Building blocks: Substitution-Permutation-Substitution (SPS) function




Used in E2, Picollo, and some other ciphers

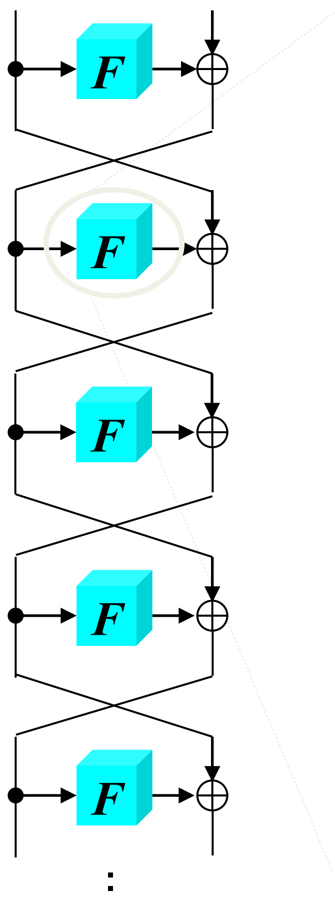
# Feistel with SPS-type F-functions

- **Balanced Feistel networks (BFNs)**
  - DES, GOST, KASUMI, ...
- **Substitution-Permutation-Substitution (SP) type F-function**
  - used in E2, Picollo
  - bijective S-boxes + MDS matrix + bijective S-boxes
  - Analyzed in [B10, BS12, BS13…]



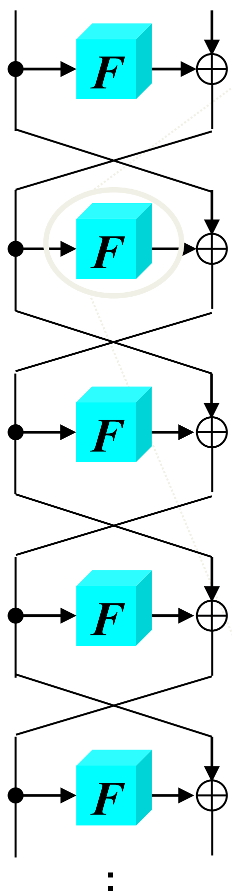
# Target structures

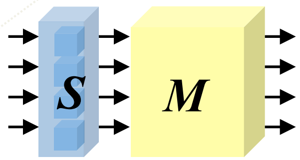
- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer



# Target structures

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer

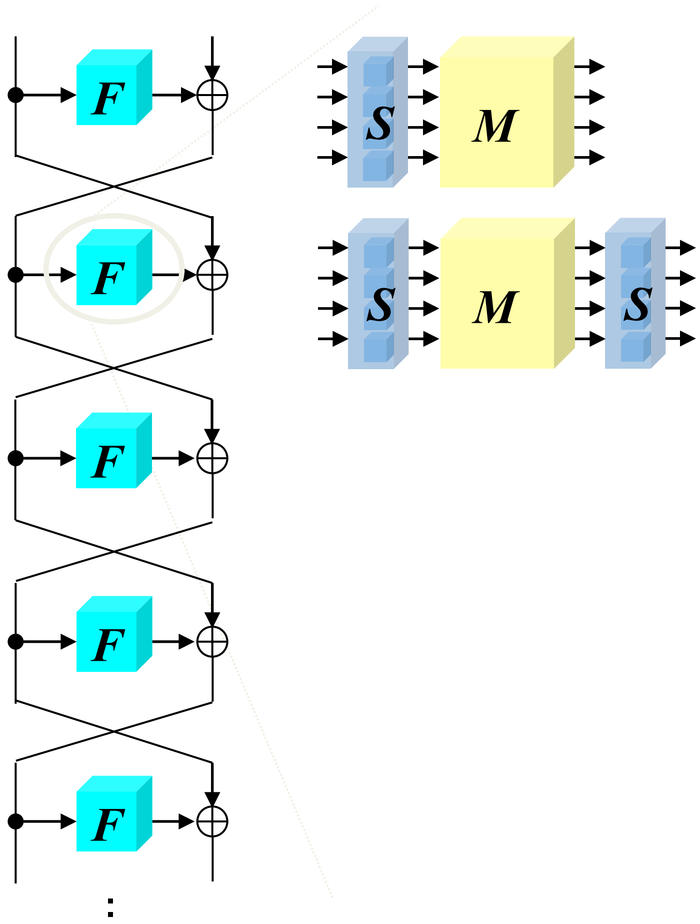



**1 S-layer + 1 P-layer**

# Target structures

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer

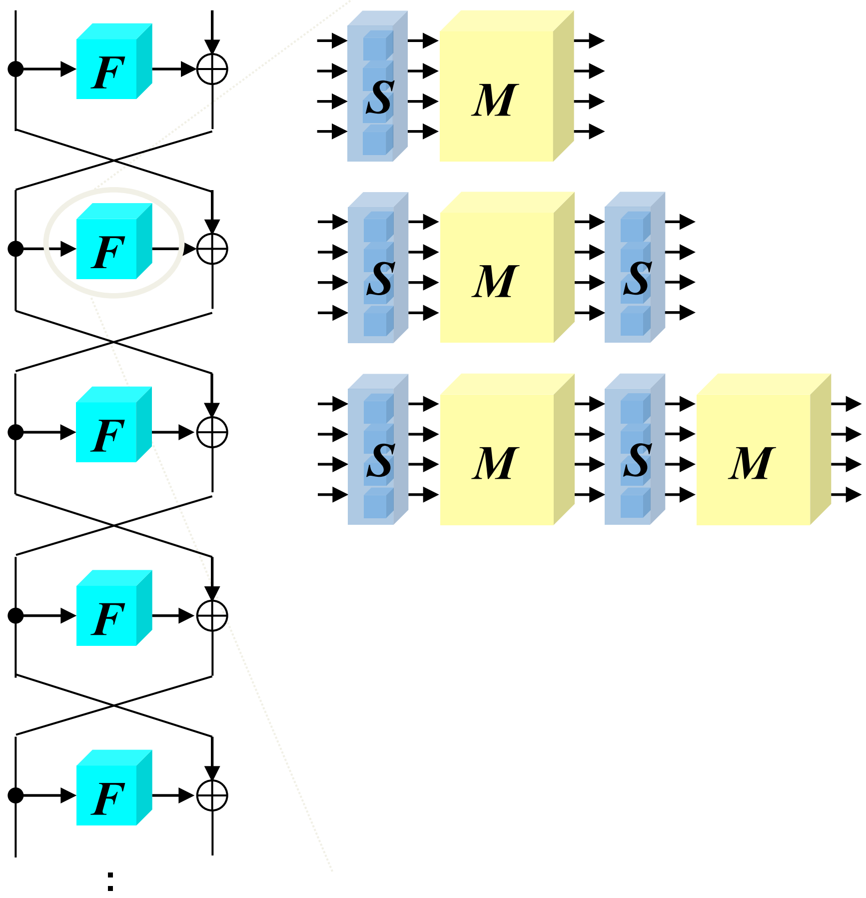



**1 S-layer + 1 P-layer**

**2 S + 1 P**

# Target structures

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer



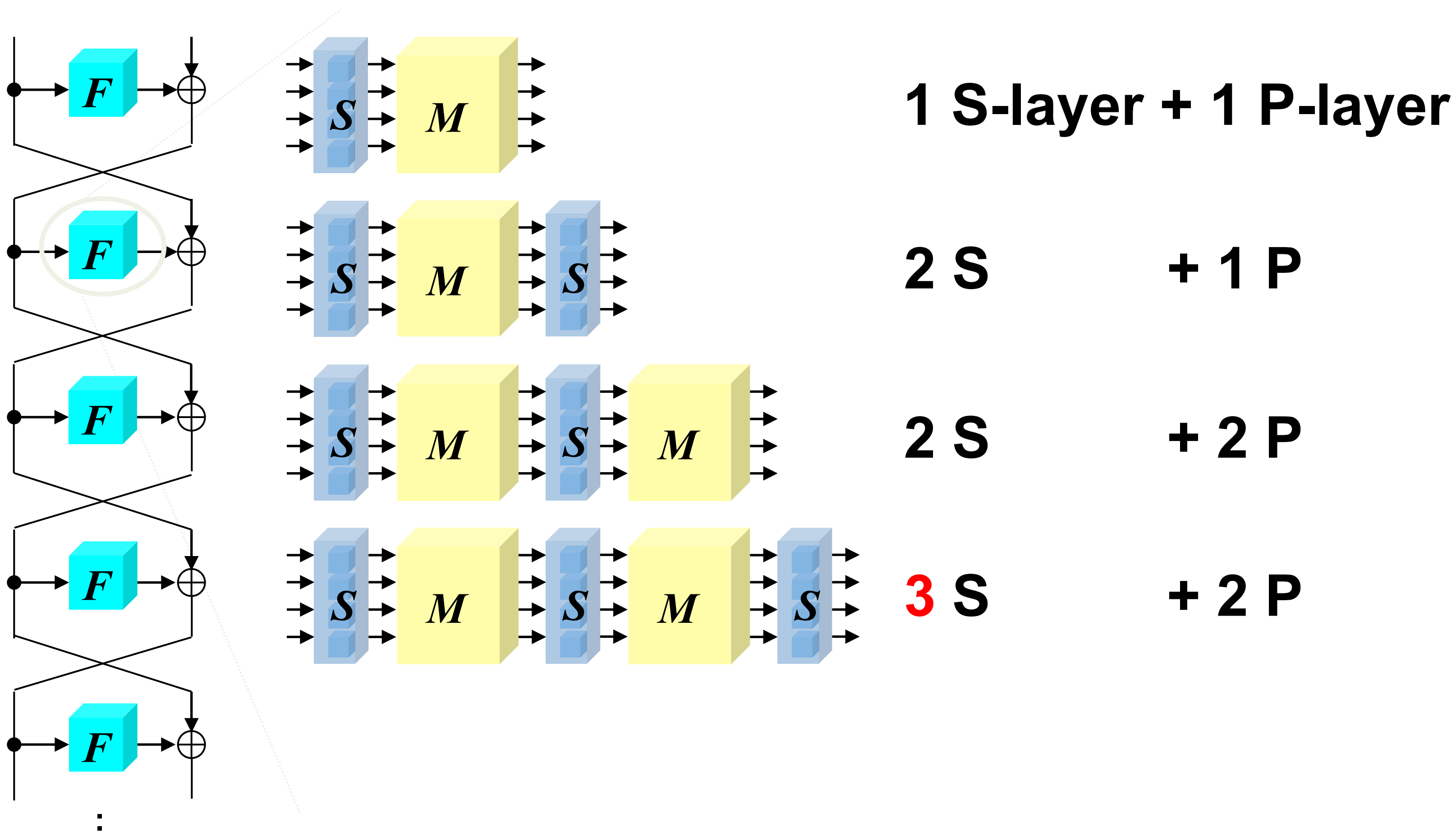

**1 S-layer + 1 P-layer**

**2 S + 1 P**

**2 S + 2 P**

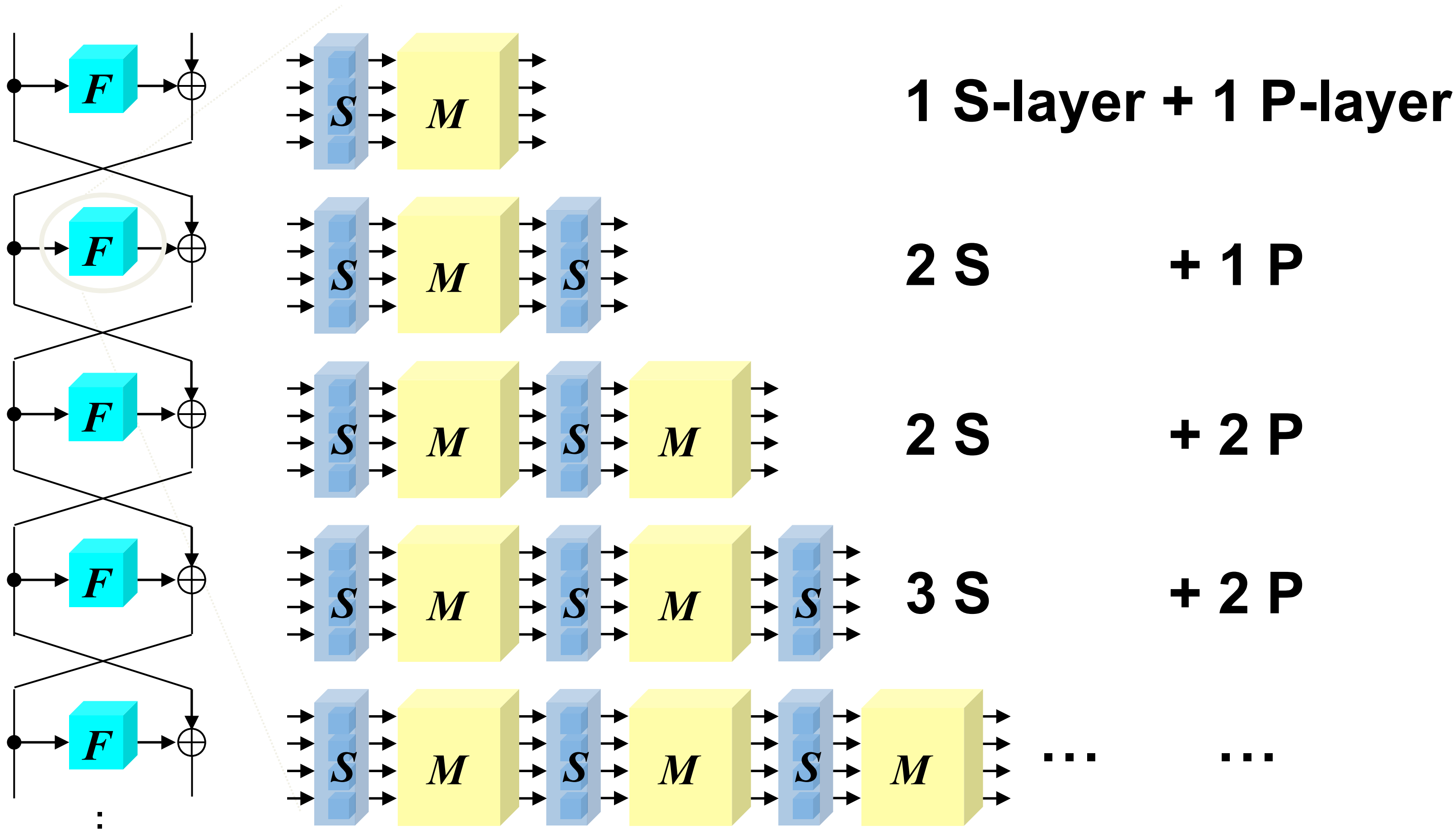
# Target structures

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer



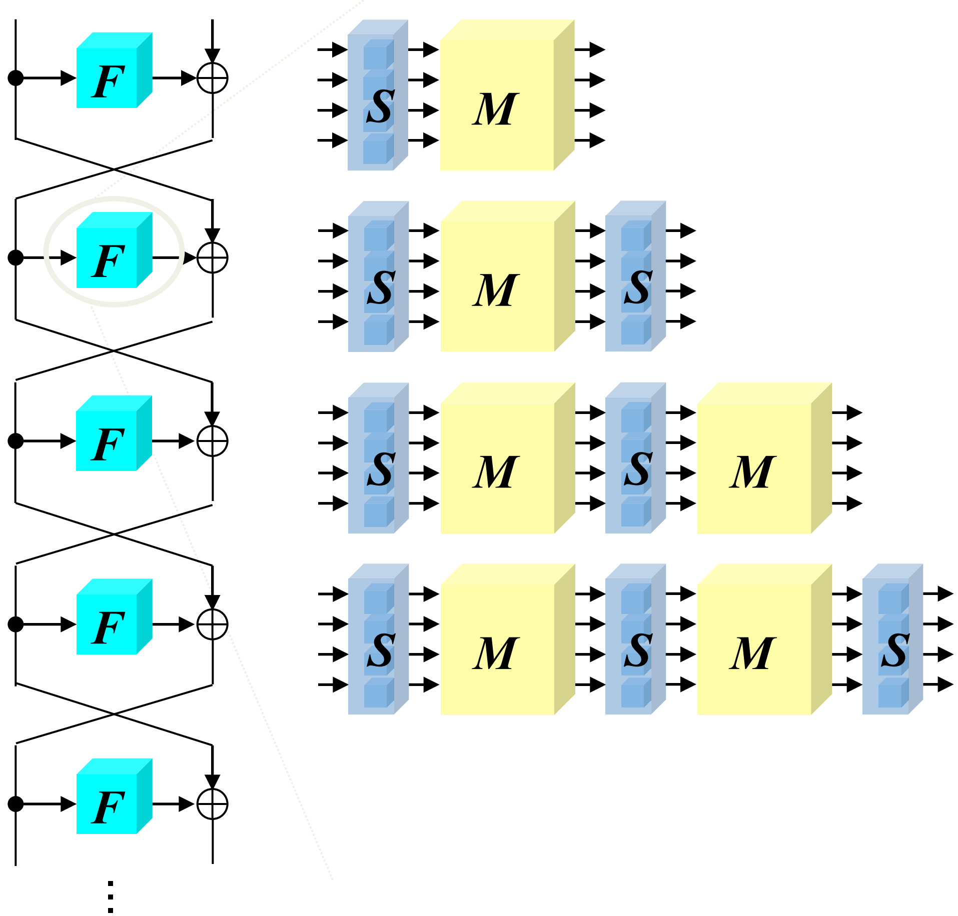
# Target structures

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer



# Target structures

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer




**classification**

(1) $(SP)^{2t+1}$

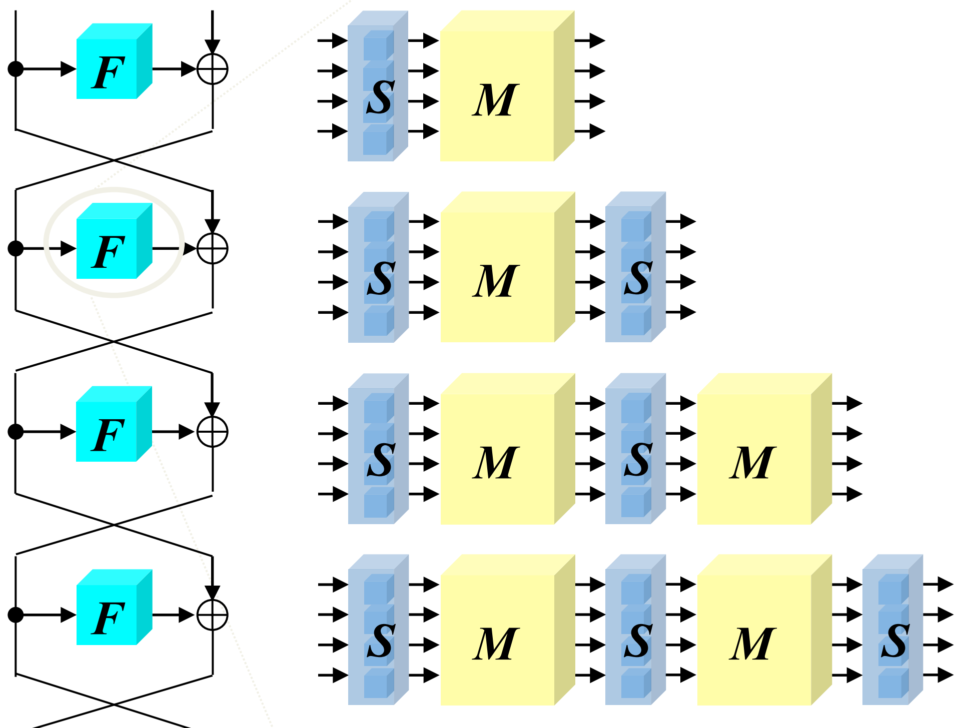
(2) $(SP)^{2t-1}S$

(3) $(SP)^{2t}$

(4) $(SP)^{2t}S$

# Our major question

- Arbitrary number of S-box layers interleaved with P-layer
  - $m$ : # S-boxes in an S-box layer




**classification**

(1) $(SP)^{2t+1}$

(2) $(SP)^{2t-1}S$

(3) $(SP)^{2t}$

(4) $(SP)^{2t}S$

**which construction is most efficient?**

⋮

# Efficiency: Counting # active S-boxes

- widely accepted tool for security evaluation
- show practical security against differential/linear attacks
- no evidence against multiple trails (differentials/linear hulls)
- For SPNs
  - simple and tight bounds are given
  - e.g. AES: 25 active S-boxes / 4-round
- For BFNs
  - more complex to prove
  - due to XOR after F-function, output of F is not directly input to next F (unlike SPNs)

# Efficiency comparison

- a metric used in [Shirai-Preneel04, B11, B12, BS12, BS13,...]
  - proportion of active S-boxes to all S-boxes
  - asymptotic proportion for $r \to \infty$

## Efficiency metric

$$E_m = \lim_{r \to \infty} \frac{A_{m,r}}{S_{m,r}}$$

$m$ : the number of S-boxes in an S-layer

$S_{m,r}$ : the number of S-boxes over $r$ rounds

$A_{m,r}$ : the number of active S-boxes over $r$ rounds

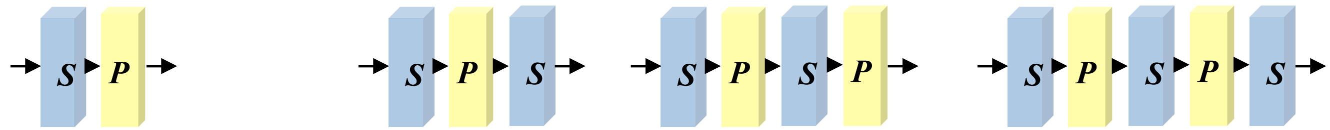
# Two types of proofs

- **I**: trail attaining the min. # active F corresponds to trail attaining the min. # active S
  - (2) BFN-$(SP)^{2t\text{-}1}$S, (3) BFN-$(SP)^{2t}$, and (4) BFN-$(SP)^{2t}$S
  - # active S is proportional to # active F
  - easy to prove

# Two types of proofs

- **I**: trail attaining the min. # active F corresponds to trail attaining the min. # active S
  - (2) BFN-$(SP)^{2t\text{-}1}$S, (3) BFN-$(SP)^{2t}$, and (4) BFN-$(SP)^{2t}$S
  - # active S is proportional to # active F
  - easy to prove
- **II**: trail attaining the min. # active F does not correspond to the trail attaining the min. # active S
  - (1) BFN-$(SP)^{2t+1}$
  - a more involved proof

# Bounds on # active S for BFNs

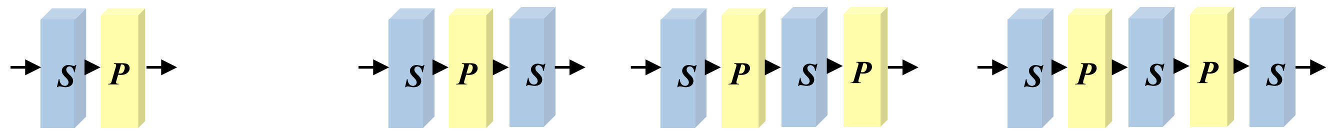



| # rounds | (1) $(SP)^{2t+1}$ ($t$>0) | (2) $(SP)^{2t-1}S$ | (3) $(SP)^{2t}$ | (4) $(SP)^{2t}S$ |
|---|---|---|---|---|
| $3R$ | $(2t+1)\mathcal{B}R - \mathcal{B} + 2$ | $2t\mathcal{B}R$ | $2t\mathcal{B}R$ | $2(t\mathcal{B}+1)R$ |
| $3R+1$ | $(2t+1)\mathcal{B}R$ | $2t\mathcal{B}R$ | $2t\mathcal{B}R$ | $2(t\mathcal{B}+1)R$ |
| $3R+2$ | $(2t+1)\mathcal{B}R + t\mathcal{B} + 1$ | $2t\mathcal{B}R + t\mathcal{B}$ | $2t\mathcal{B}R + t\mathcal{B}$ | $2(t\mathcal{B}+1)R + t\mathcal{B} + 1$ |

| # rounds | (1) $(SP)^{2t+1}$ ($t$=0) |
|---|---|
| $4R$ | $(\mathcal{B}+1)R - 1$ |
| $4R+1$ | $(\mathcal{B}+1)R$ |
| $4R+2$ | $(\mathcal{B}+1)R + 1$ |
| $4R+3$ | $(\mathcal{B}+1)R + 2$ |

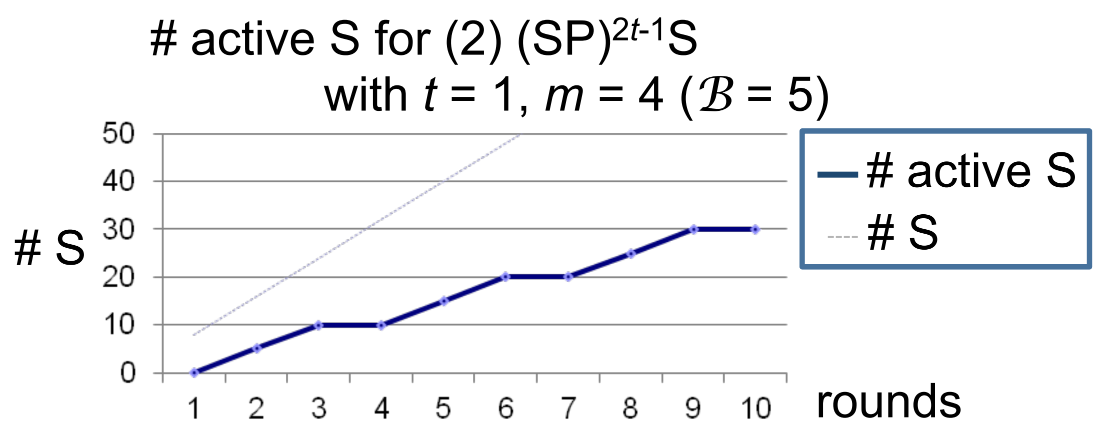
$\mathcal{B}$: branch number of P
If P is MDS, $\mathcal{B} = m + 1$

# Bounds on # active S for BFNs

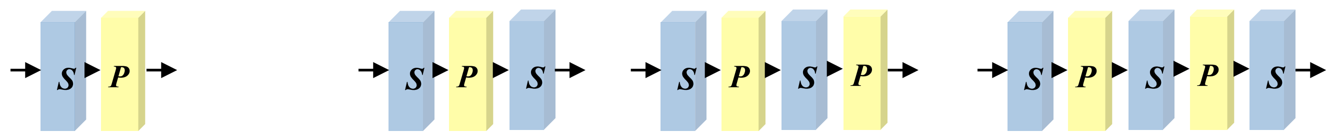



| # rounds | (1) $(SP)^{2t+1}$ ($t$>0) | (2) $(SP)^{2t-1}S$ | (3) $(SP)^{2t}$ | (4) $(SP)^{2t}S$ |
|---|---|---|---|---|
| $3R$ | $(2t + 1)\mathcal{B}R - \mathcal{B} + 2$ | $2t\mathcal{B}R$ | $2t\mathcal{B}R$ | $2(t\mathcal{B} + 1)R$ |
| $3R + 1$ | $(2t + 1)\mathcal{B}R$ | $2t\mathcal{B}R$ | $2t\mathcal{B}R$ | $2(t\mathcal{B} + 1)R$ |
| $3R + 2$ | $(2t + 1)\mathcal{B}R + t\mathcal{B} + 1$ | $2t\mathcal{B}R + t\mathcal{B}$ | $2t\mathcal{B}R + t\mathcal{B}$ | $2(t\mathcal{B} + 1)R + t\mathcal{B} + 1$ |

| # rounds | (1) $(SP)^{2t+1}$ ($t$=0) |
|---|---|
| $4R$ | $(\mathcal{B} + 1)R - 1$ |
| $4R + 1$ | $(\mathcal{B} + 1)R$ |
| $4R + 2$ | $(\mathcal{B} + 1)R + 1$ |
| $4R + 3$ | $(\mathcal{B} + 1)R + 2$ |

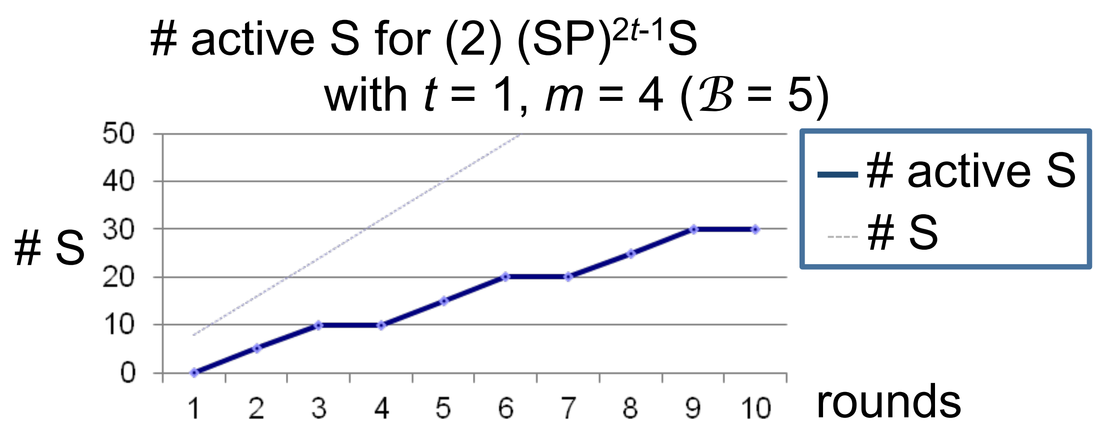


# Bounds on # active S for BFNs



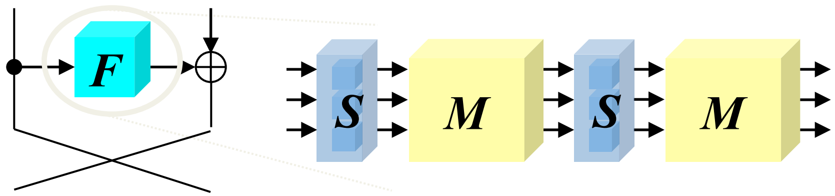

| # rounds | (1) $(SP)^{2t+1}$ ($t$>0) | (2) $(SP)^{2t-1}S$ | (3) $(SP)^{2t}$ | (4) $(SP)^{2t}S$ |
|---|---|---|---|---|
| $3R$ | $(2t + 1)\mathcal{B}R - \mathcal{B} + 2$ | $2t\mathcal{B}R$ | $2t\mathcal{B}R$ | $2(t\mathcal{B} + 1)R$ |
| $3R + 1$ | $(2t + 1)\mathcal{B}R$ | $2t\mathcal{B}R$ | $2t\mathcal{B}R$ | $2(t\mathcal{B} + 1)R$ |
| $3R + 2$ | $(2t + 1)\mathcal{B}R + t\mathcal{B} + 1$ | $2t\mathcal{B}R + t\mathcal{B}$ | $2t\mathcal{B}R + t\mathcal{B}$ | $2(t\mathcal{B} + 1)R + t\mathcal{B} + 1$ |

| # rounds | (1) $(SP)^{2t+1}$ ($t$=0) |
|---|---|
| $4R$ | $(\mathcal{B} + 1)R - 1$ |
| $4R + 1$ | $(\mathcal{B} + 1)R$ |
| $4R + 2$ | $(\mathcal{B} + 1)R + 1$ |
| $4R + 3$ | $(\mathcal{B} + 1)R + 2$ |




**These bounds can be actually tight**

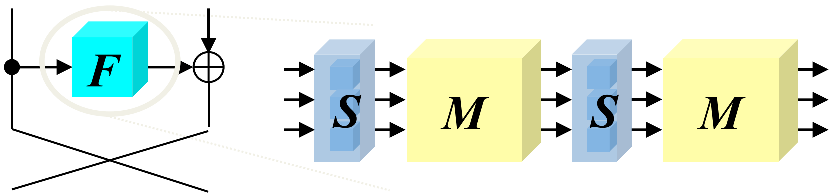
# Example of tightness: Iterative trail for BFN-(SP)$^{2t}$




$2t\mathcal{B}R$ active S / $3R$-round
$2t\mathcal{B}R$ active S / $(3R+1)$-round
$(2t\mathcal{B}R + t\mathcal{B})$ active S / $(3R+2)$-round

| # rounds | # active S |
|---|---|
| 1 | 0 |
| 2 | $t\mathcal{B}$ |
| 3 | $2t\mathcal{B}$ |
| 4 | $2t\mathcal{B}$ |
| 5 | $3t\mathcal{B}$ |
| 6 | $4t\mathcal{B}$ |
| 7 | $4t\mathcal{B}$ |
| 8 | $5t\mathcal{B}$ |
| | |

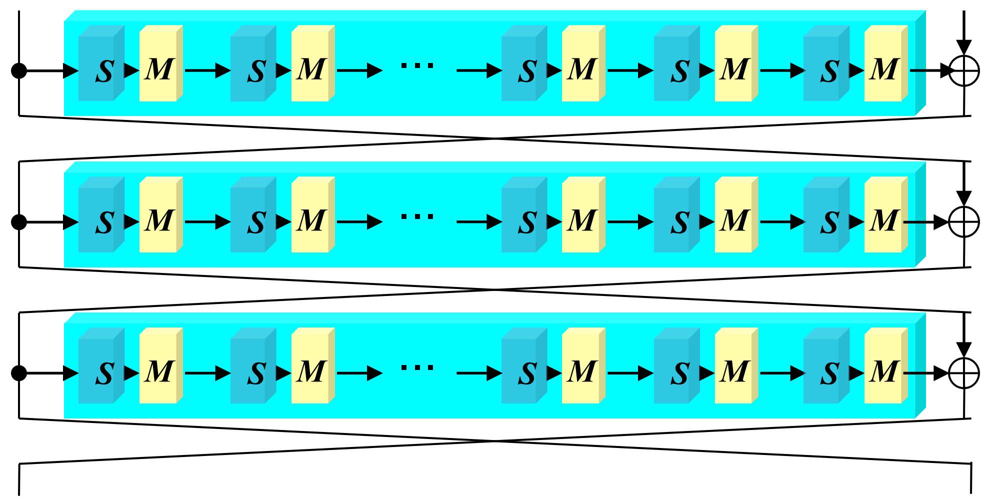
# Example of tightness: Iterative trail for BFN-(SP)$^{2t}$



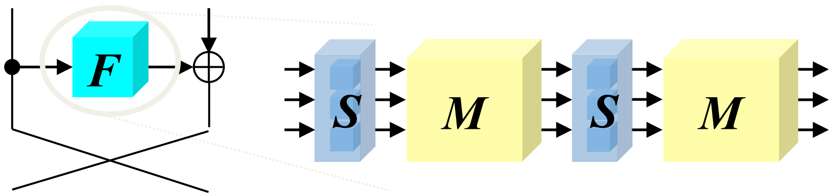

$2t\mathcal{B}R$ active S / $3R$-round
$2t\mathcal{B}R$ active S / $(3R+1)$-round
$(2t\mathcal{B}R + t\mathcal{B})$ active S / $(3R+2)$-round

Δ : truncated difference (100...00)
∇ : truncated difference (111...11)
◯ : difference cancellation

| # rounds | # active S |
|---|---|
| 1 | 0 |
| 2 | $t\mathcal{B}$ |
| 3 | $2t\mathcal{B}$ |
| 4 | $2t\mathcal{B}$ |
| 5 | $3t\mathcal{B}$ |
| 6 | $4t\mathcal{B}$ |
| 7 | $4t\mathcal{B}$ |
| 8 | $5t\mathcal{B}$ |



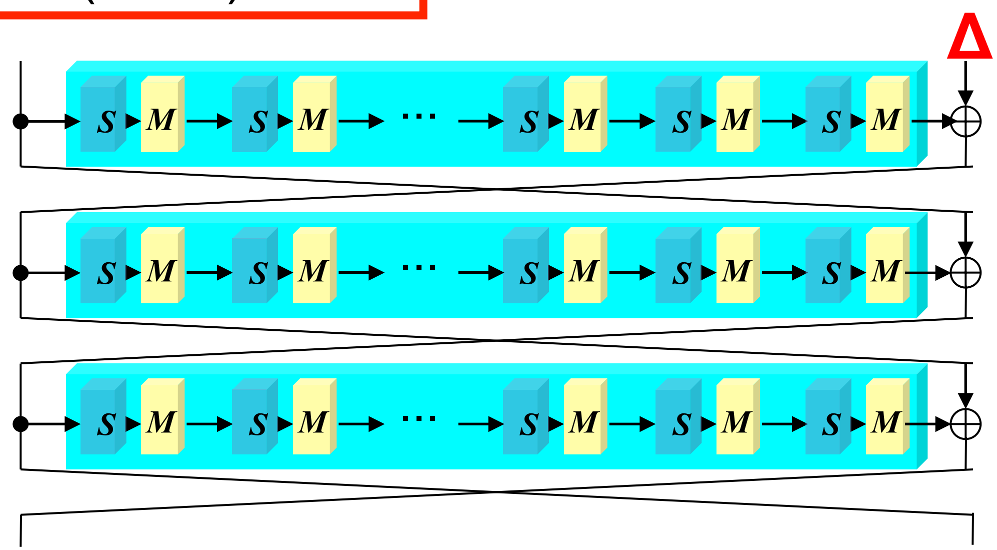
# Example of tightness: Iterative trail for BFN-(SP)$^{2t}$



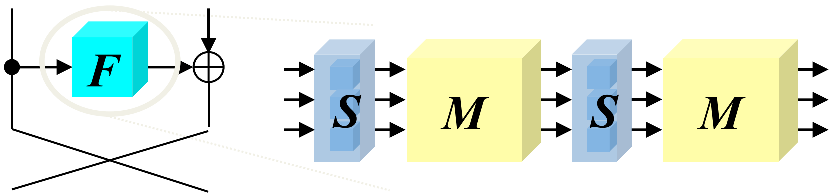

$2t\mathcal{B}R$ active S / $3R$-round
$2t\mathcal{B}R$ active S / $(3R+1)$-round
$(2t\mathcal{B}R + t\mathcal{B})$ active S / $(3R+2)$-round

Δ : truncated difference (100...00)
∇ : truncated difference (111...11)
◌ : difference cancellation

| # rounds | # active S |
|---|---|
| 1 | 0 |
| 2 | $t\mathcal{B}$ |
| 3 | $2t\mathcal{B}$ |
| 4 | $2t\mathcal{B}$ |
| 5 | $3t\mathcal{B}$ |
| 6 | $4t\mathcal{B}$ |
| 7 | $4t\mathcal{B}$ |
| 8 | $5t\mathcal{B}$ |
| | |



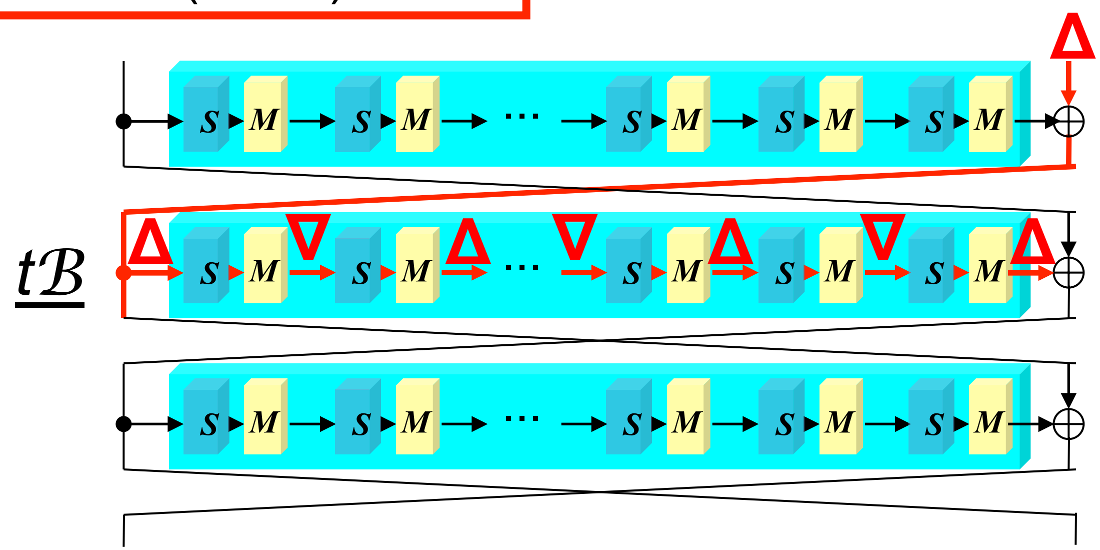
# Example of tightness: Iterative trail for BFN-(SP)$^{2t}$



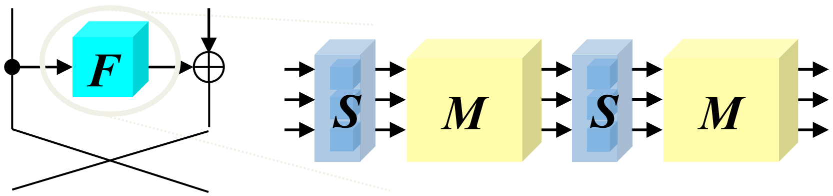

| |
|---|
| $2t\mathcal{B}R$ active S / $3R$-round |
| $2t\mathcal{B}R$ active S / $(3R+1)$-round |
| $(2t\mathcal{B}R + t\mathcal{B})$ active S / $(3R+2)$-round |

Δ : truncated difference (100...00)
∇ : truncated difference (111...11)
: difference cancellation

| # rounds | # active S |
|---|---|
| 1 | 0 |
| 2 | $t\mathcal{B}$ |
| 3 | $2t\mathcal{B}$ |
| 4 | $2t\mathcal{B}$ |
| 5 | $3t\mathcal{B}$ |
| 6 | $4t\mathcal{B}$ |
| 7 | $4t\mathcal{B}$ |
| 8 | $5t\mathcal{B}$ |



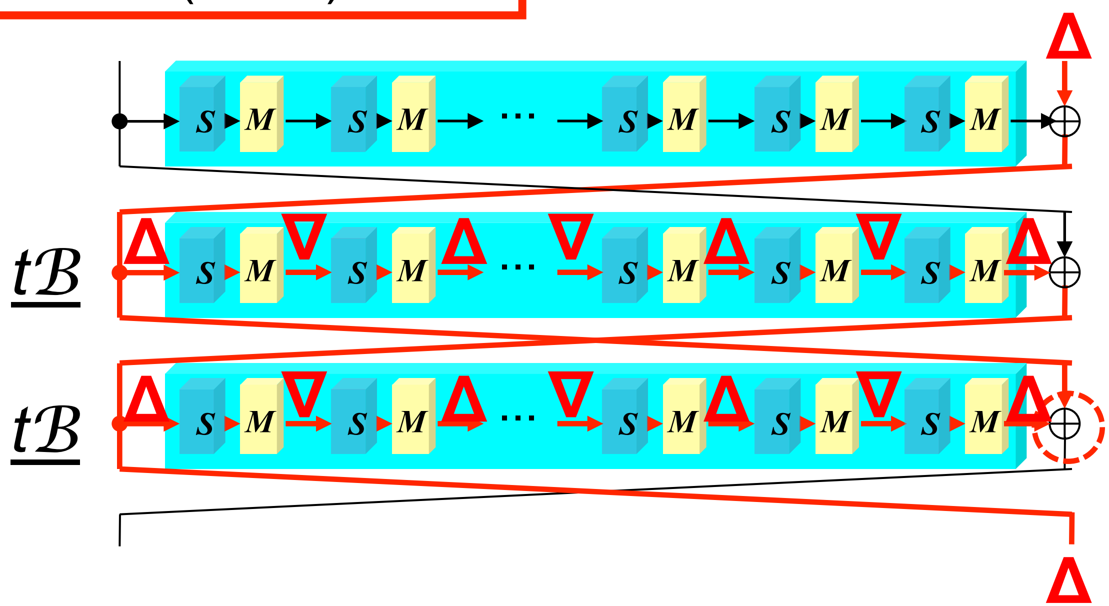
# Example of tightness: Iterative trail for BFN-(SP)$^{2t}$



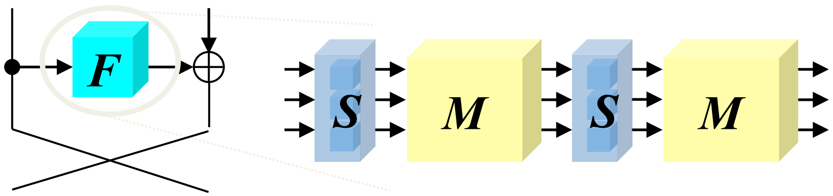

$2t\mathcal{B}R$ active S / $3R$-round
$2t\mathcal{B}R$ active S / $(3R+1)$-round
$(2t\mathcal{B}R + t\mathcal{B})$ active S / $(3R+2)$-round

Δ : truncated difference (100…00)
∇ : truncated difference (111…11)
◌ : difference cancellation

| # rounds | # active S |
|---|---|
| 1 | 0 |
| 2 | $t\mathcal{B}$ |
| 3 | $2t\mathcal{B}$ |
| 4 | $2t\mathcal{B}$ |
| 5 | $3t\mathcal{B}$ |
| 6 | $4t\mathcal{B}$ |
| 7 | $4t\mathcal{B}$ |
| 8 | $5t\mathcal{B}$ |
| | |



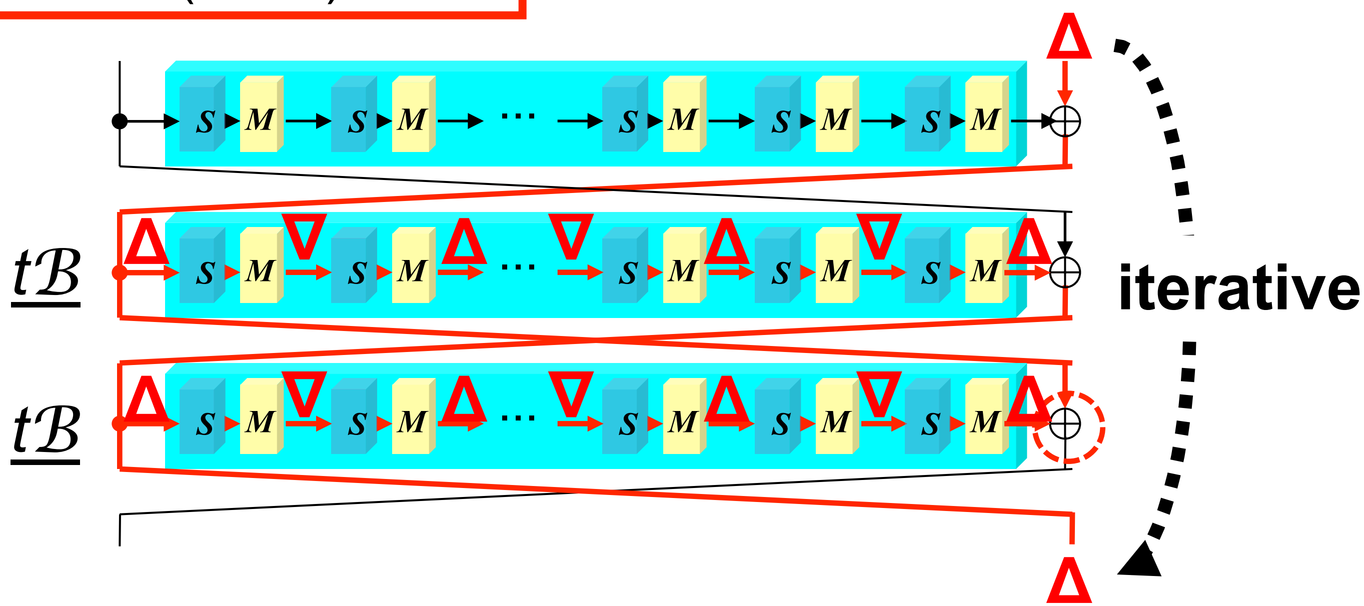
# Example of tightness: Iterative trail for BFN-(SP)$^{2t}$



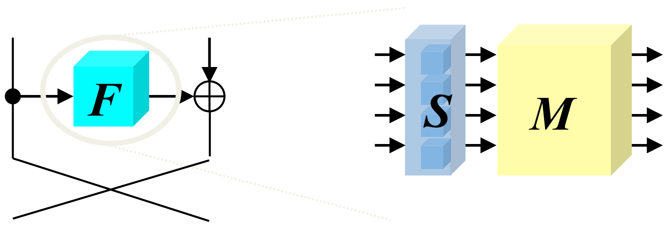

$2t\mathcal{B}R$ active S / $3R$-round
$2t\mathcal{B}R$ active S / $(3R+1)$-round
$(2t\mathcal{B}R + t\mathcal{B})$ active S / $(3R+2)$-round

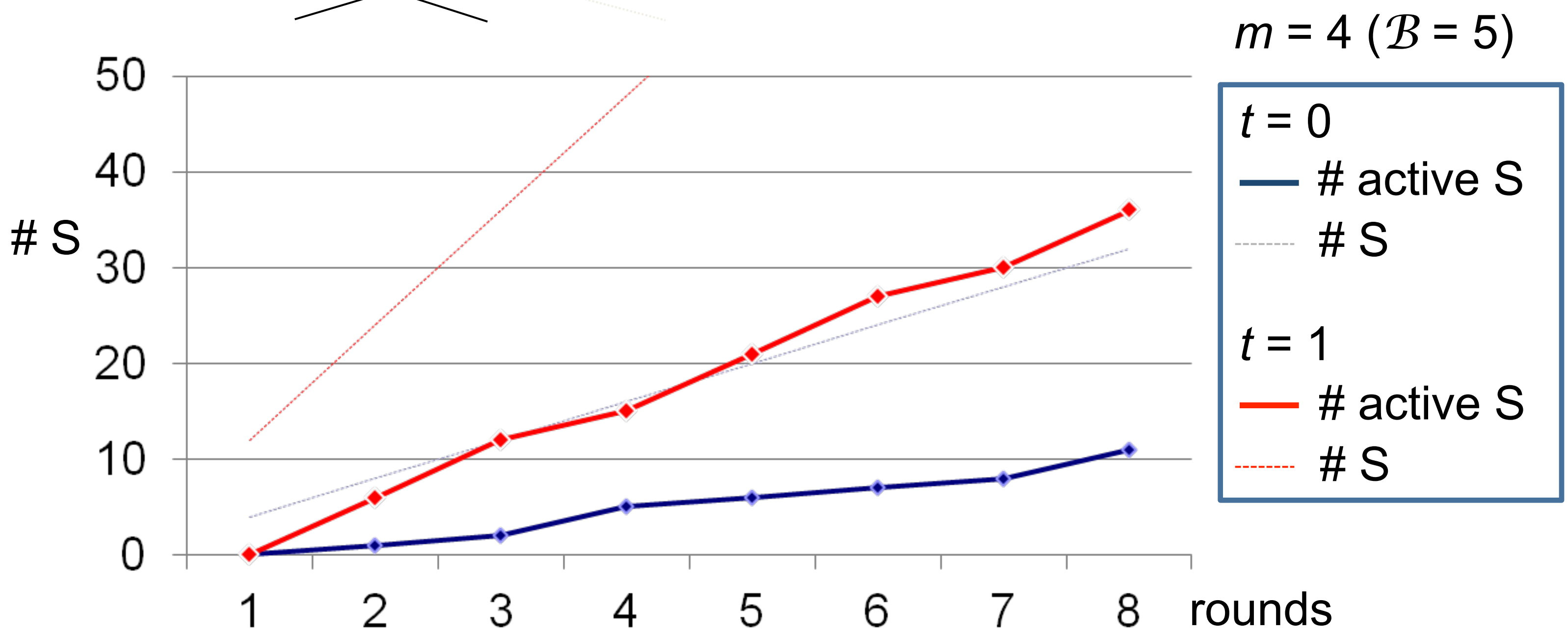
| # rounds | # active S |
|---|---|
| 1 | 0 |
| 2 | $t\mathcal{B}$ |
| 3 | $2t\mathcal{B}$ |
| 4 | $2t\mathcal{B}$ |
| 5 | $3t\mathcal{B}$ |
| 6 | $4t\mathcal{B}$ |
| 7 | $4t\mathcal{B}$ |
| 8 | $5t\mathcal{B}$ |
| | |

Δ : truncated difference (100...00)
∇ : truncated difference (111...11)
◌ : difference cancellation



# Bounds on # active S-boxes for BFN-$(SP)^{2t+1}$ with $m = 4$



# Efficiency comparison

- a metric used in [Shirai-Preneel04, B11, BS12, …]
  - proportion of active S-boxes to all S-boxes
  - asymptotic proportion for $r \to \infty$

## Efficiency metric

$$E_m = \lim_{r \to \infty} \frac{A_{m,r}}{S_{m,r}}$$

$m$ : the number of S-boxes in an S-layer

$S_{m,r}$ : the number of S-boxes over $r$ rounds

$A_{m,r}$ : the number of active S-boxes over $r$ rounds

# $E_m$ for BFNs with SP-type F and MDS

| Construction | $E_m = \lim_{r \to \infty} \frac{A_{m,r}}{S_{m,r}}$ |
| --- | --- |
| BFN-(SP)$^{2t}$<br>BFN-(SP)$^{2t-1}$S | $\frac{m+1}{3m}$ |
| BFN-(SP)$^{2t+1}$ | $\frac{m+1}{3m}$ |
| BFN-SP | $\frac{m+2}{4m}$ |
| BFN-(SP)$^{2t}$S | $\frac{2t(m+1)+2}{3(2t+1)m}$ |

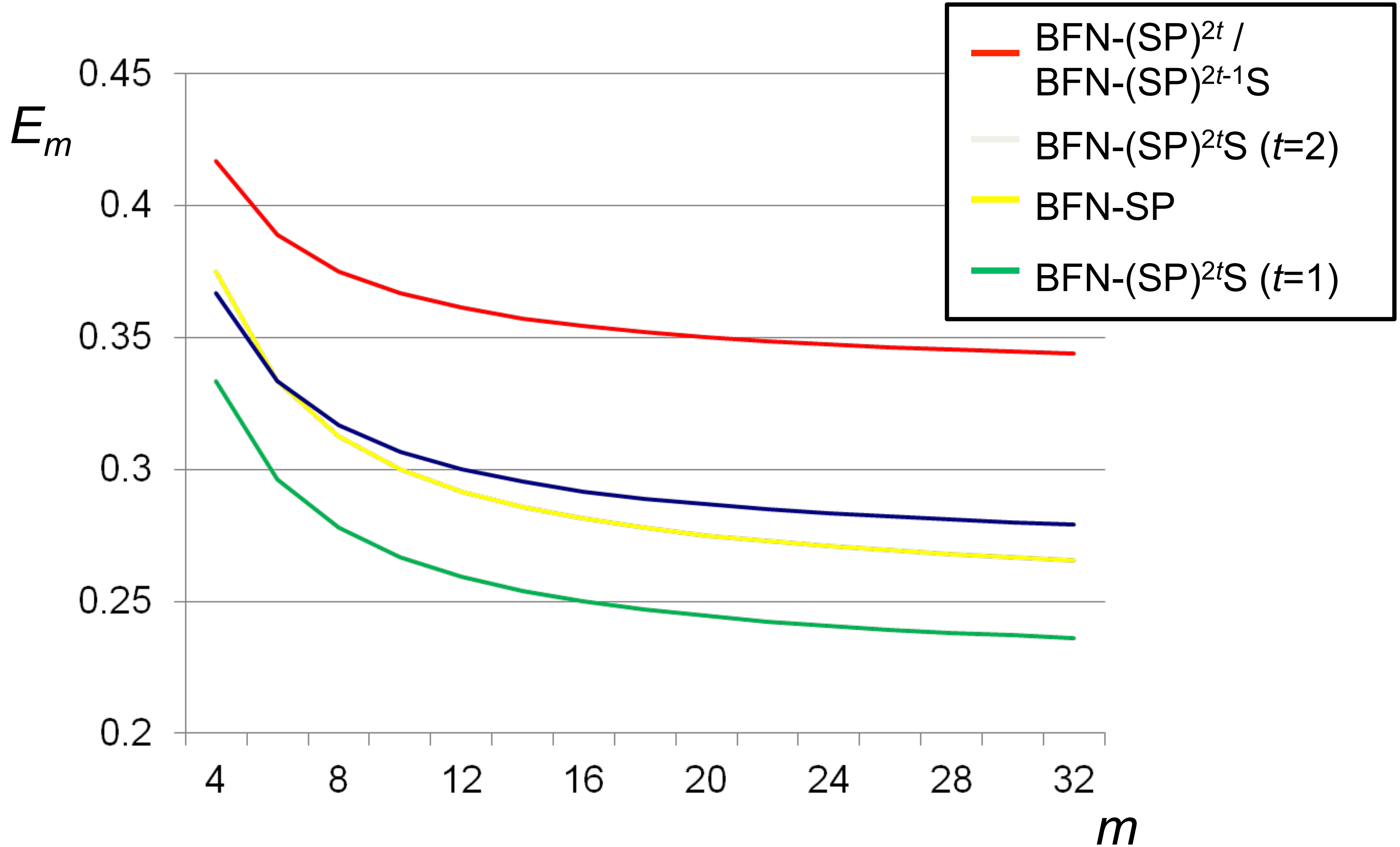
# Optimality result

## Optimality

For BFNs with MDS-based SP-type F-function and $m \geq 2$, BFN-$(SP)^{2t}$ and BFN-$(SP)^{2t-1}S$ provide a higher or equal proportion of active S-boxes than the others for any $t$.

Thus, BFN-SPSP and BFN-SPS are optimal w.r.t. $E_m$

# Efficiency comparison



# Conclusions

- Proven tight lower bounds on # active S-boxes for a wide class of BFNs (any number of rounds)
- BFN-SPS/BFN-SPSP are the most efficient constructions w.r.t. ratio between active S-boxes and all S-boxes in this class
- **Conjecture:** For most other reasonable Feistel constructions, it is also best to take SPS or SPSP F-functions to optimize for $E_m$ if MDS diffusion

# References

[Shirai-Preneel04] Taizo Shirai, Bart Preneel: On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds. ASIACRYPT 2004: 1-15

[B10] Andrey Bogdanov: On the differential and linear efficiency of balanced Feistel networks. Inf. Process. Lett. 110(20): 861-866 (2010)

[B11] Andrey Bogdanov: On unbalanced Feistel networks with contracting MDS diffusion. Des. Codes Cryptography 59(1-3): 35-58 (2011)

[BS11] Andrey Bogdanov, Kyoji Shibutani: Double SP-Functions: Enhanced Generalized Feistel Networks - Extended Abstract. ACISP 2011: 106-119

[BS13] Andrey Bogdanov, Kyoji Shibutani: Generalized Feistel networks revisited. Des. Codes Cryptography 66(1-3): 75-97 (2013)