Constructing S-boxes for lightweight cryptography with Feistel Structure

Yongqiang Li

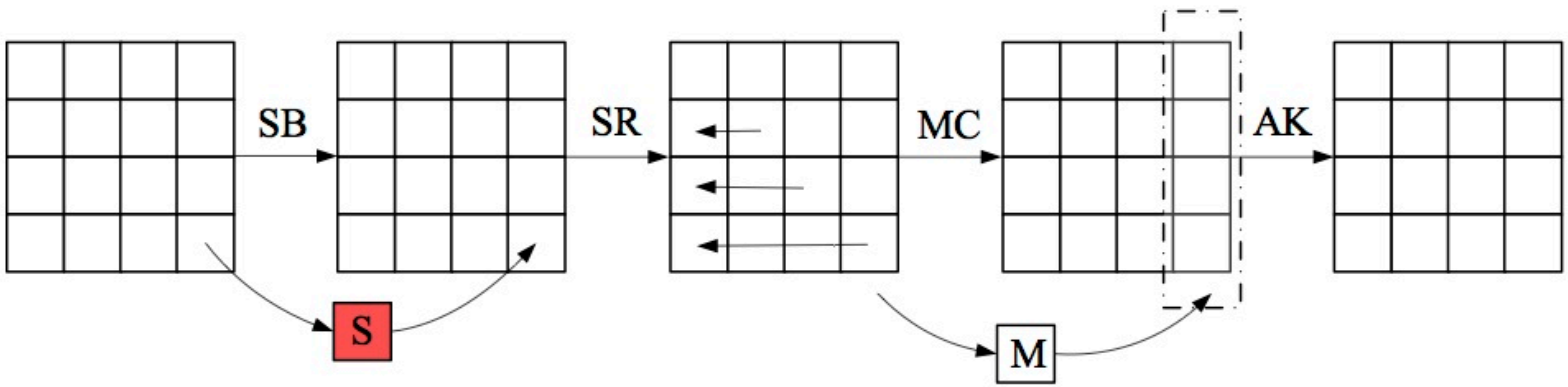
Joint work with Mingsheng Wang

State Key Laboratory of Information Security

Institute of Information Engineering, Chinese Academy of Sciences

CHES 2014, Busan, Korea

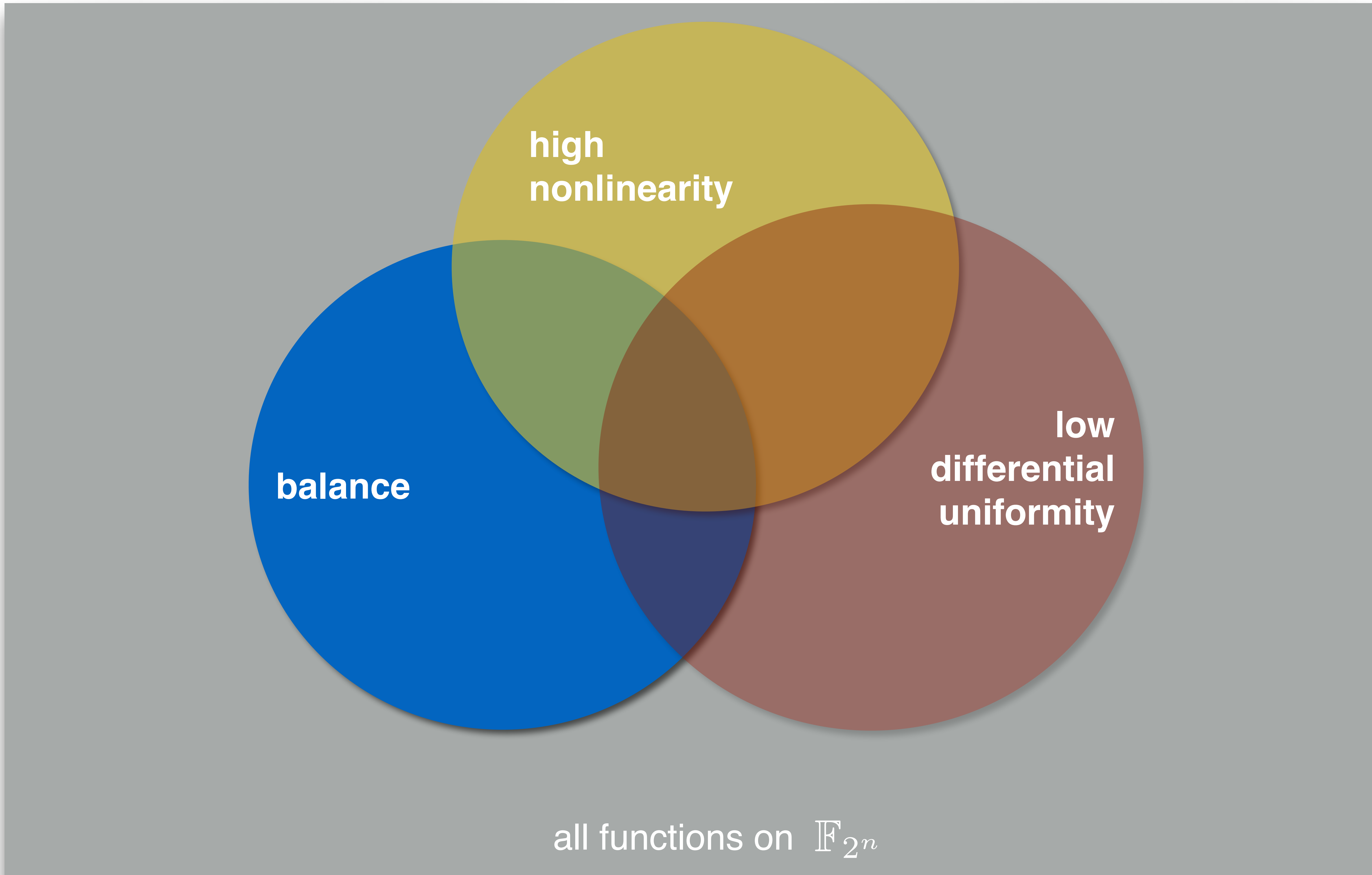
The role of S-boxes in symmetric cryptography



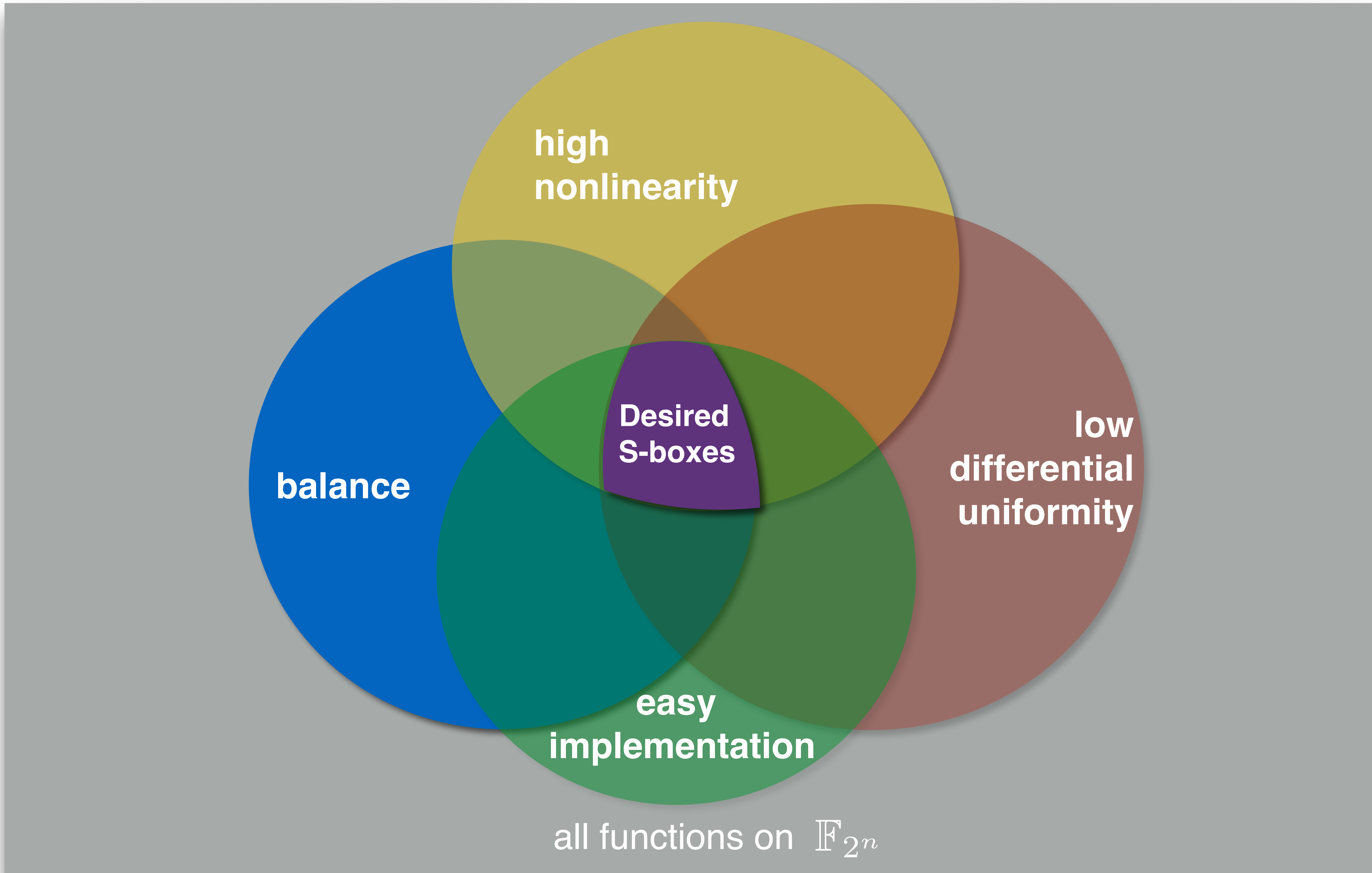
- Provide ``confusion";
- Only nonlinear part of round functions for most algorithms.

Remark: All S-boxes in this talk are n-bit S-boxes.

Basic cryptographic properties of S-boxes



S-boxes for lightweight cryptography

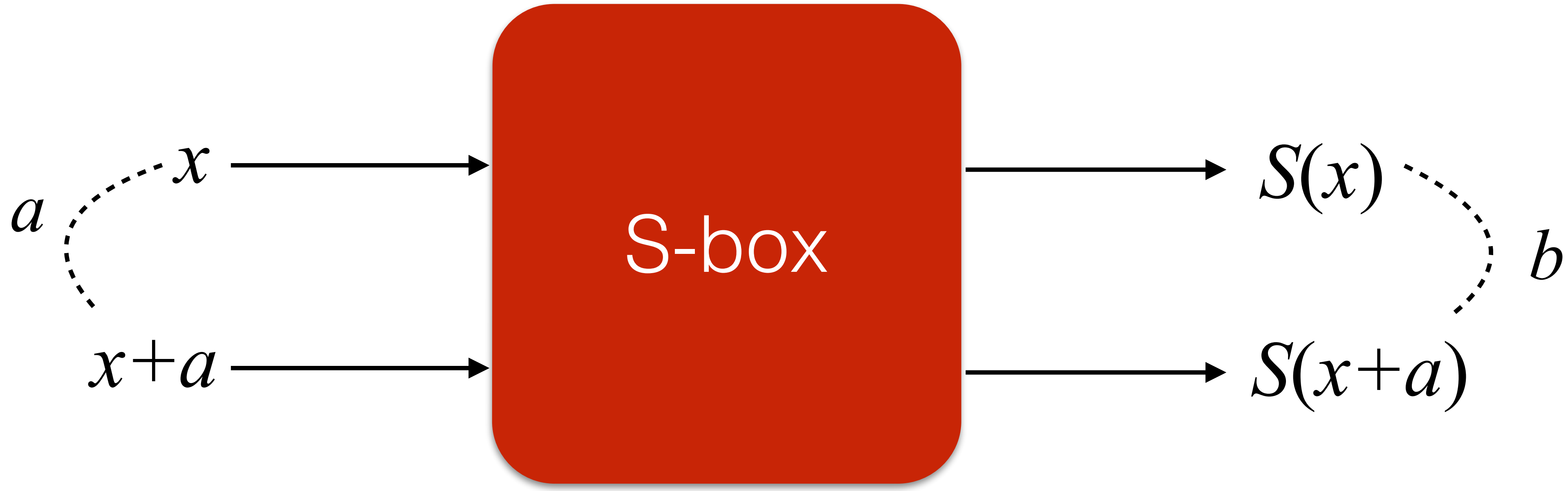


Differential uniformity

$$\Delta(S) = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} : S(x) + S(x+a) = b\}|$$

$$\Delta(S) \geq 2$$

Functions with equality holds are called almost perfect nonlinear (APN) functions.



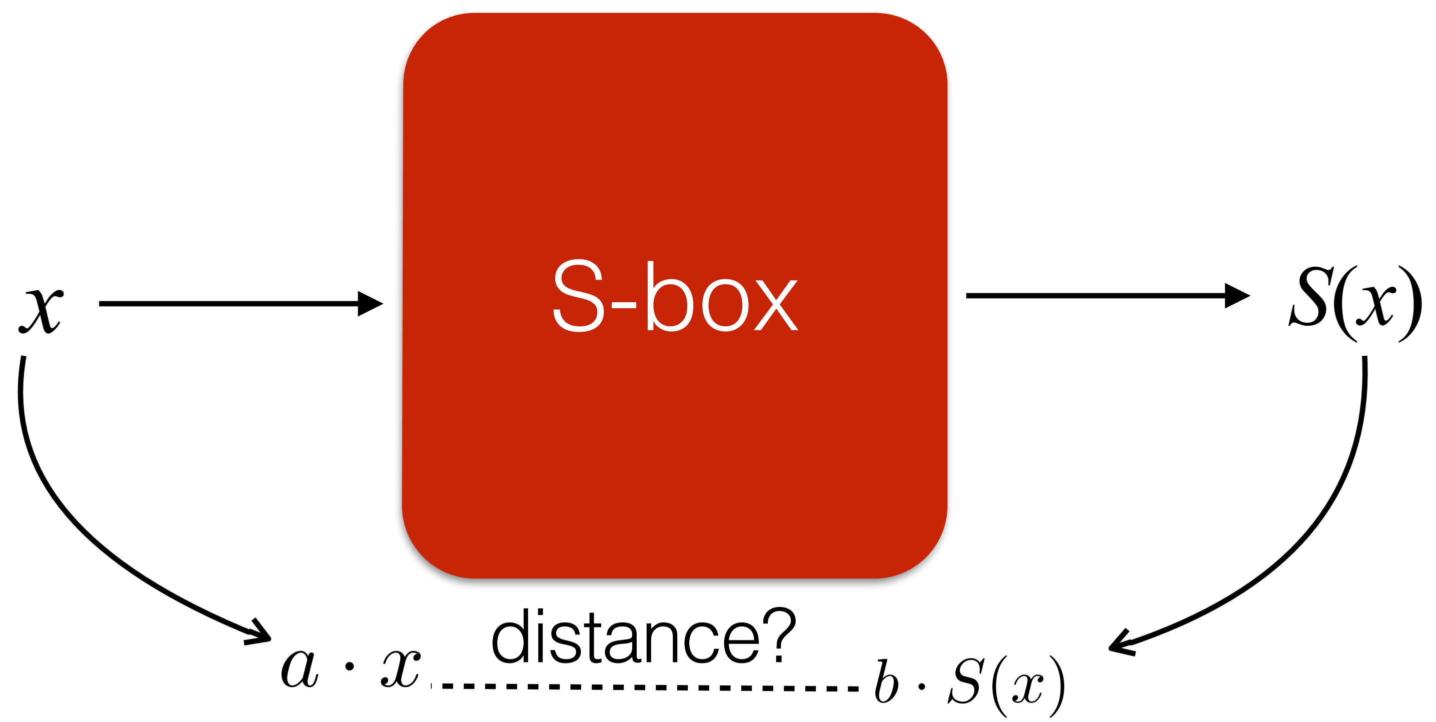
S-boxes with lower differential uniformity posses better resistance to differential attack.

Nonlinearity

The minimal distance of all the components of $S(x)$ to affine Boolean functions.

$$\lambda_S(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bS(x)+ax)}$$

$$\mathcal{NL}(S) = 2^{n-1} - \frac{1}{2}\max\{|\lambda_S(a,b)| : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$$



S-boxes with higher nonlinearity posses better resistance to linear attack.

The best performance of nonlinearity and differential uniformity of permutations over $\mathbb{F}_{2^n}$

nonlinearity

$$\mathcal{NL}(S) \leq \begin{cases} 2^{n-1} - 2^{\frac{n-1}{2}} & n \text{ odd} \\ 2^{n-1} - 2^{\frac{n}{2}} & n \text{ even} \end{cases}$$

differential uniformity

$$\Delta(S) \geq \begin{cases} 2 & n \text{ odd} \\ 4 & n = 4 \\ 2 & n = 6 \\ 4 & n \geq 8 \text{ even} \end{cases}$$

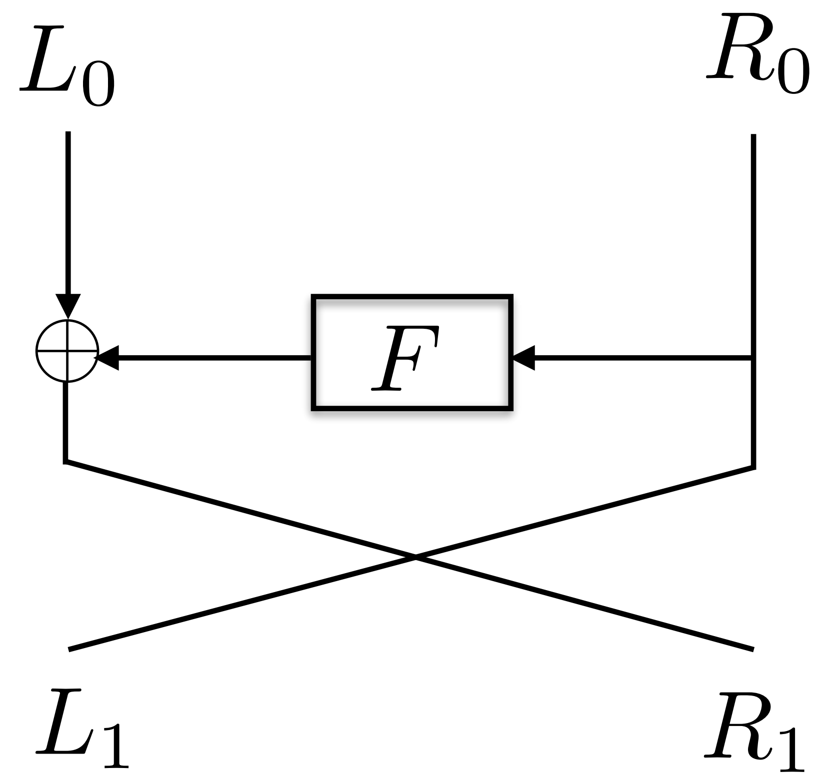
The two red bounds above are not proven yet.

The main problem

Construct S-boxes with the following properties:

- n even, permutation;
- Lowest differential uniformity; 4
- The best known nonlinearity; $2^{n-1} - 2^{\frac{n}{2}}$
- Easy implementation;

Feistel structure

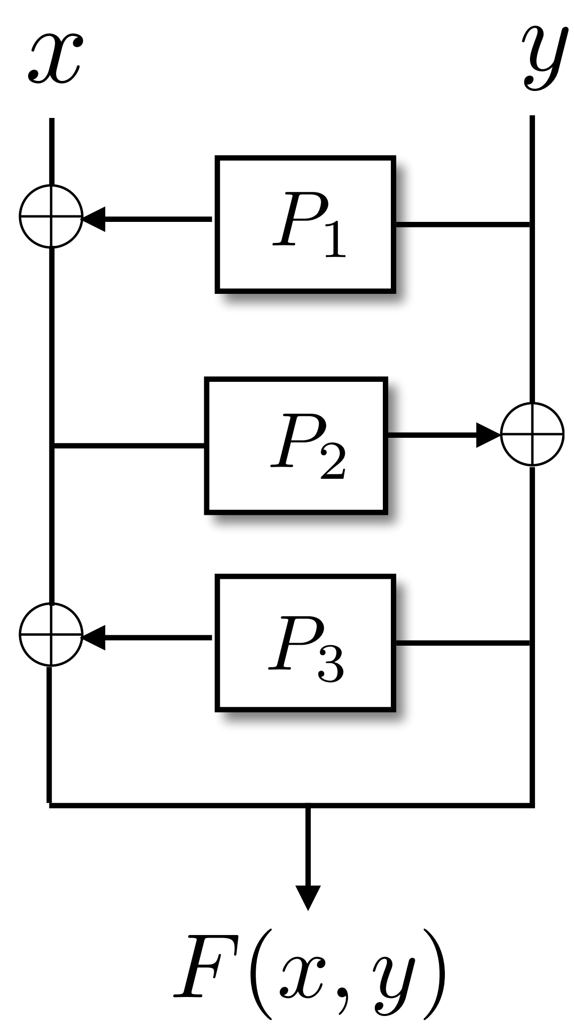


$$(L_0, R_0) \to (R_0, L_0 + F(R_0))$$

Feistel structure has low implementation cost.

S-boxes constructed with 3-round Feistel structure

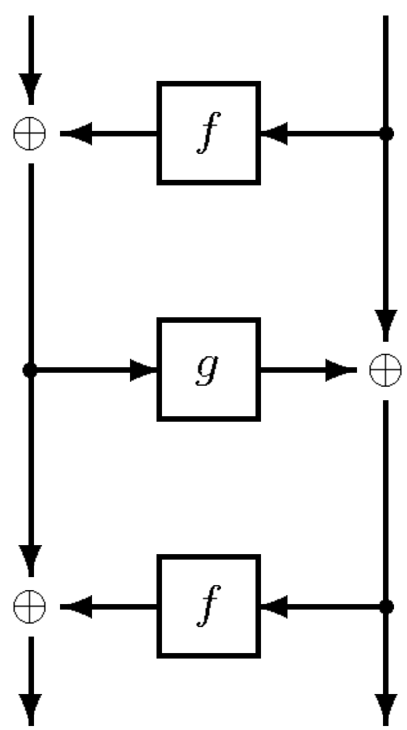
$$x, y \in \mathbb{F}_{2^k}, P_1, P_2, P_3 \in \mathbb{F}_{2^k}[x].\ F(x, y) : \mathbb{F}_{2^k}^2 \longrightarrow \mathbb{F}_{2^k}^2$$



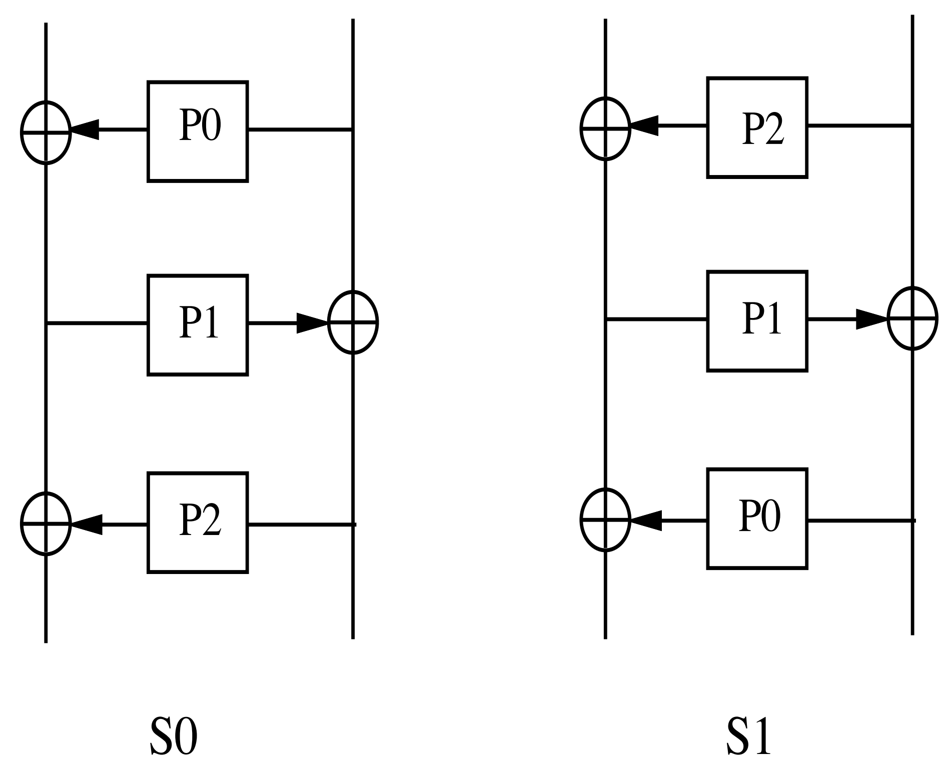
$$F(x, y) = (x + P_1(y) + P_3(y + P_2(x + P_1(y))), y + P_2(x + P_1(y)))$$

S-boxes constructed with 3-round Feistel structure

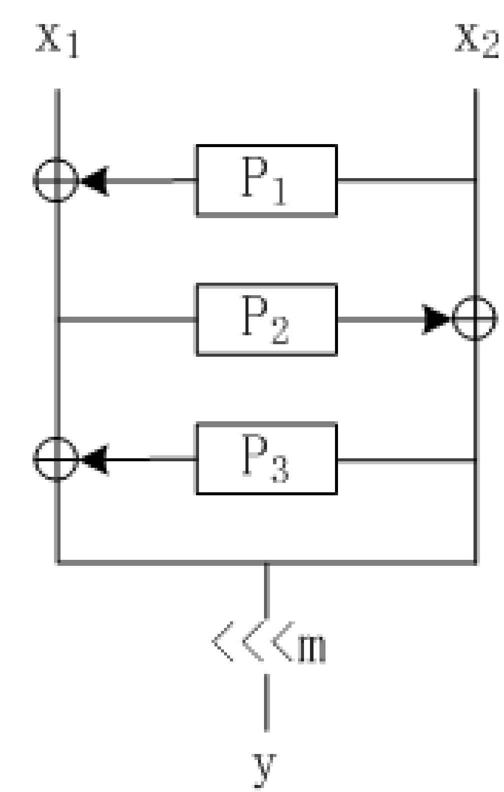
CS-CIPHER



CRYPTON



ZUC



Algorithm/S-box	Differential uniformity	Nonlinearity	Algebraic degree
CS-CIPER/P	16	96	5
CRYPTON/S_0, S_1	8	96	5
ZUC/S_0	8	96	5

Bounds on S-boxes constructed with 3-round Feistel structure

Bounds on differential uniformity

Let $F(x, y)$ be an S-box constructed as previous. Then

- If $P_2(x)$ is not a permutation over $\mathbb{F}_{2^k}$, then $\Delta(F) \geq 2^{k+1}$.
- If $P_2(x)$ is a permutation over $\mathbb{F}_{2^k}$, then $\Delta(F) \geq 2\Delta(P_2)$.

Bounds on S-boxes constructed with 3-round Feistel structure

Bounds on differential uniformity

Let $F(x,y)$ be an S-box constructed as previous. Then

- If $P_2(x)$ is not a permutation over $\mathbb{F}_{2^k}$, then $\Delta(F) \geq 2^{k+1}$.
- If $P_2(x)$ is a permutation over $\mathbb{F}_{2^k}$, then $\Delta(F) \geq 2\Delta(P_2)$.

Bounds on nonlinearity

Let $F(x,y)$ be an S-box constructed as previous, $\lambda_k = \begin{cases} 2^{\frac{k+1}{2}} & k \text{ odd}, \\ 2^{\frac{k}{2}+1} & k \text{ even}. \end{cases}$.

If for any $a \in \mathbb{F}_{2^k}^*$, there exists $b \in \mathbb{F}_{2^k}^*$, such that $|\lambda_{P_2}(a,b)| \geq \lambda_k$, then
$\mathcal{NL}(F(x,y)) \leq \begin{cases} 2^{2k-1} - 2^k & k \text{ odd}, \\ 2^{2k-1} - 2^{k+1} & k \text{ even}. \end{cases}$

Bounds on S-boxes constructed with 3-round Feistel structure

Bounds of 8-bit S-boxes

Let $F_{P_1,P_2,P_3}(x,y)$ be an S-box over $\mathbb{F}_{2^4}^2$ constructed with 3-round Feistel structure. Then

- $\Delta(F_{P_1,P_2,P_3}) \geq 8$.
- If $\Delta(F_{P_1,P_2,P_3}) = 8$, then $\mathcal{NL}(F_{P_1,P_2,P_3}) \leq 96$.

Bounds on S-boxes constructed with 3-round Feistel structure

Bounds of 8-bit S-boxes

Let $F_{P_1,P_2,P_3}(x,y)$ be an S-box over $\mathbb{F}_{2^4}^2$ constructed with 3-round Feistel structure. Then

- $\Delta(F_{P_1,P_2,P_3}) \geq 8$.
- If $\Delta(F_{P_1,P_2,P_3}) = 8$, then $\mathcal{NL}(F_{P_1,P_2,P_3}) \leq 96$.

Algorithm/S-box	Differential uniformity	Nonlinearity	Algebraic degree
CS-CIPER/P	16	96	5
CRYPTON/S_0, S_1	8	96	5
ZUC/S_0	8	96	5

Bounds on S-boxes constructed with 3-round Feistel structure

Algorithm/S-box	Differential uniformity	Nonlinearity	Algebraic degree
CS-CIPER/P	16	96	5
CRYPTON/S_0, S_1	8	96	5
ZUC/S_0	8	96	5

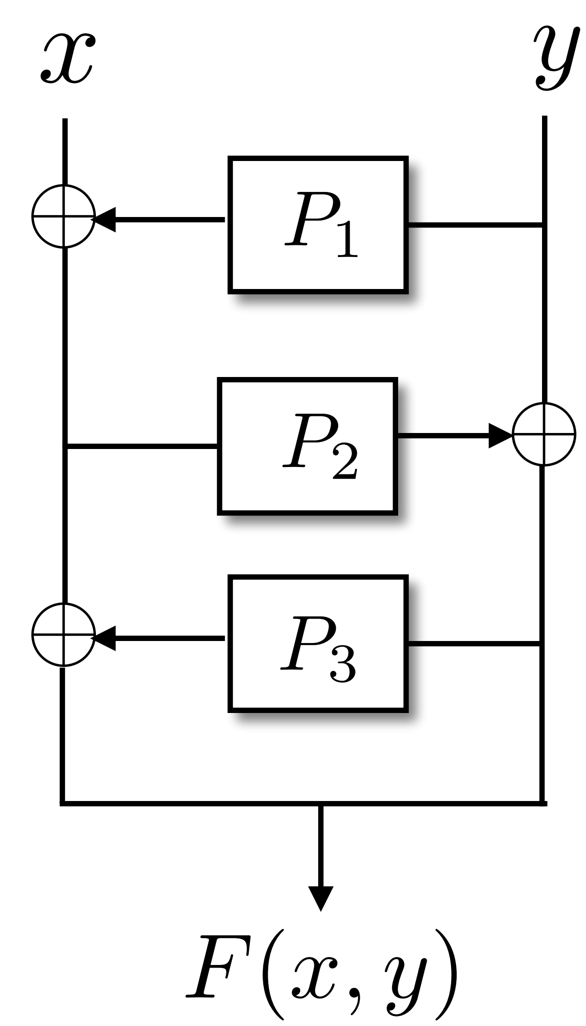
An improved example

$P_1 = x^3$, $P_2 = x + g^6 * x^{10} + g^3 * x^{13}$, $(g^4 + g + 1 = 0)$, $P_3 = \sum_{i=4}^{14} x^i$. F_{P_1,P_2,P_3}, F_{P_3,P_2,P_3} are with differential uniformity 8, nonlinearity 96, and algebraic degree 6.

General construction of big S-boxes

- n even, permutation; ✓
- Lowest differential uniformity; 4
- The best know nonlinearity; $2^{n-1} - 2^{\frac{n}{2}}$
- Easy implementation; ✓

P_2 must be an APN permutation



General construction of big S-boxes

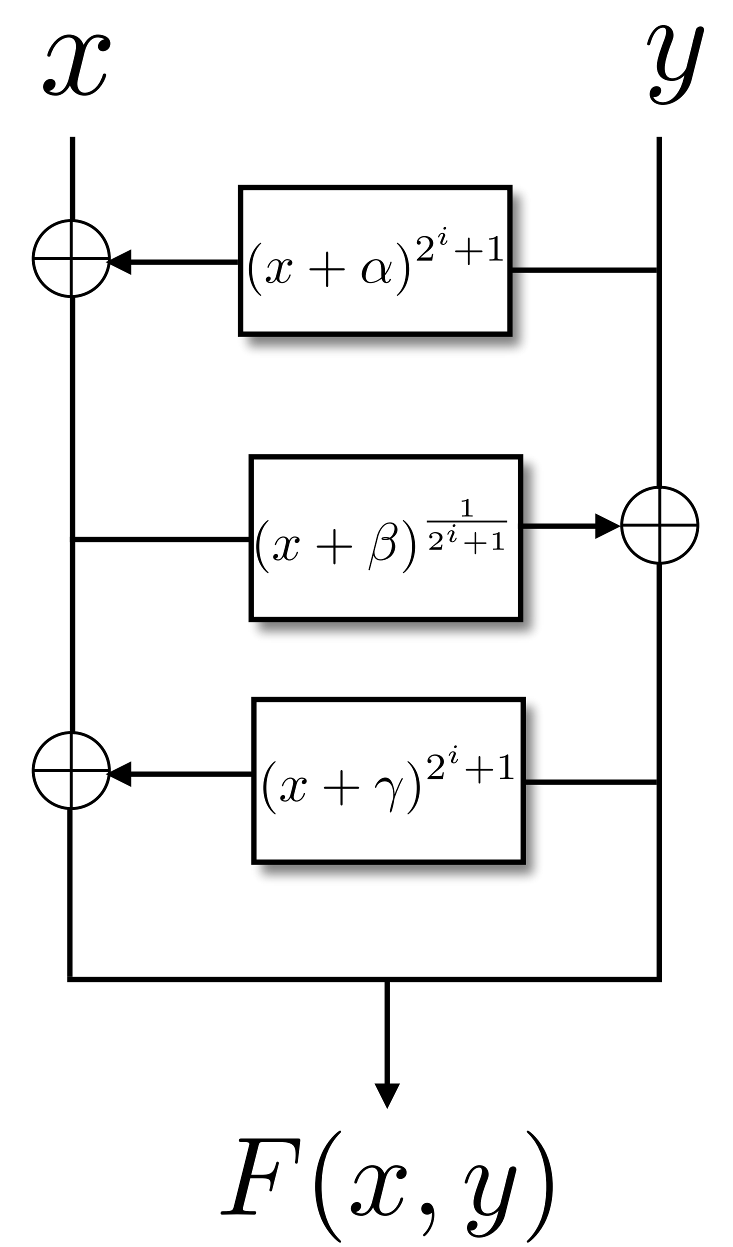
- n even, permutation; ✓
- Lowest differential uniformity; 4
- The best know nonlinearity; $2^{n-1} - 2^{\frac{n}{2}}$
- Easy implementation; ✓

k odd, $(\lambda_k = 2^{\frac{k+1}{2}})$

- there are APN permutations over $\mathbb{F}_{2^k}$;
- $\mathcal{NL}(F) \leq 2^{2k-1} - 2^k$,

General construction of big S-boxes

- k odd, $\gcd(i,k) = 1$.
- x^{2^i+1} is an APN permutation.
- $x^{\frac{1}{2^i+1}}$ compositional inverse.
- $\alpha, \beta, \gamma \in \mathbb{F}_{2^k}$.



General construction of big S-boxes

Theorem

k odd, $\gcd(i,k)=1$. Let $F(x,y)=(x+(y+\alpha)^{2^i+1}+(y+\gamma+(x+\beta+(y+\alpha)^{2^i+1})^{\frac{1}{2^i+1}})^{2^i+1}, y+(x+\beta+(y+\alpha)^{2^i+1})^{\frac{1}{2^i+1}})$, be an S-box constructed as previous. Then

- When $\alpha=\gamma$, $F(x,y)$ is an involution on $\mathbb{F}_{2^k}^2$.
- Its differential uniformity equals 4. differential spectrum $\{0,4\}$.
- Its nonlinearity equals $2^{2k-1}-2^k$. Walsh spectrum $\{0,\pm 2^{k+1}\}$.
- Its algebraic degree equals k.

General construction of big S-boxes

Theorem

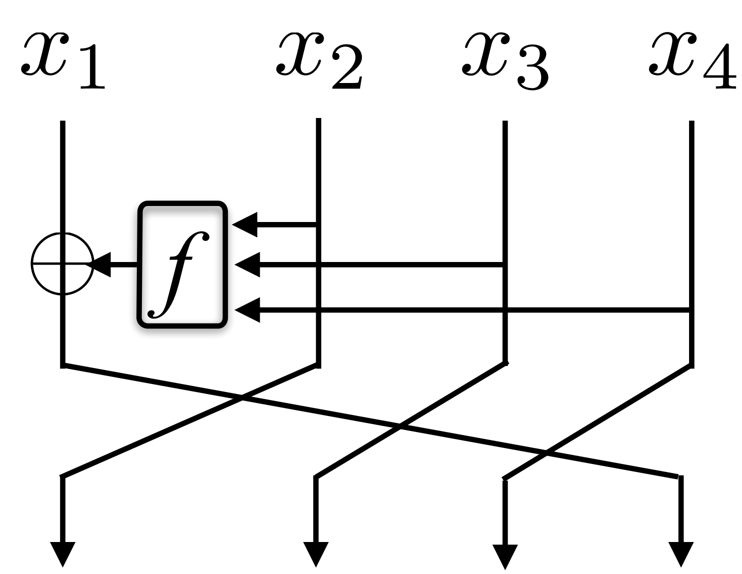
k odd, $\gcd(i,k)=1$. Let $F(x,y)=(x+(y+\alpha)^{2^i+1}+(y+\gamma+(x+\beta+(y+\alpha)^{2^i+1})^{\frac{1}{2^i+1}})^{2^i+1}, y+(x+\beta+(y+\alpha)^{2^i+1})^{\frac{1}{2^i+1}})$, be an S-box constructed as previous. Then

- When $\alpha=\gamma$, $F(x,y)$ is an involution on $\mathbb{F}_{2^k}^2$.
- Its differential uniformity equals 4. differential spectrum $\{0,4\}$.
- Its nonlinearity equals $2^{2k-1}-2^k$. Walsh spectrum $\{0,\pm 2^{k+1}\}$.
- Its algebraic degree equals k.

K. Aoki [SAC 98]: "Characterizing the F-functions whose maximum differential probability with keys is small"

Construction of S-boxes with unbalanced Feistel structure

$$x_i \in \mathbb{F}_{2^k},\ f : \mathbb{F}_{2^k}^3 \mapsto \mathbb{F}_{2^k}.\ \ P_f : \mathbb{F}_{2^k}^4 \mapsto \mathbb{F}_{2^k}^4$$

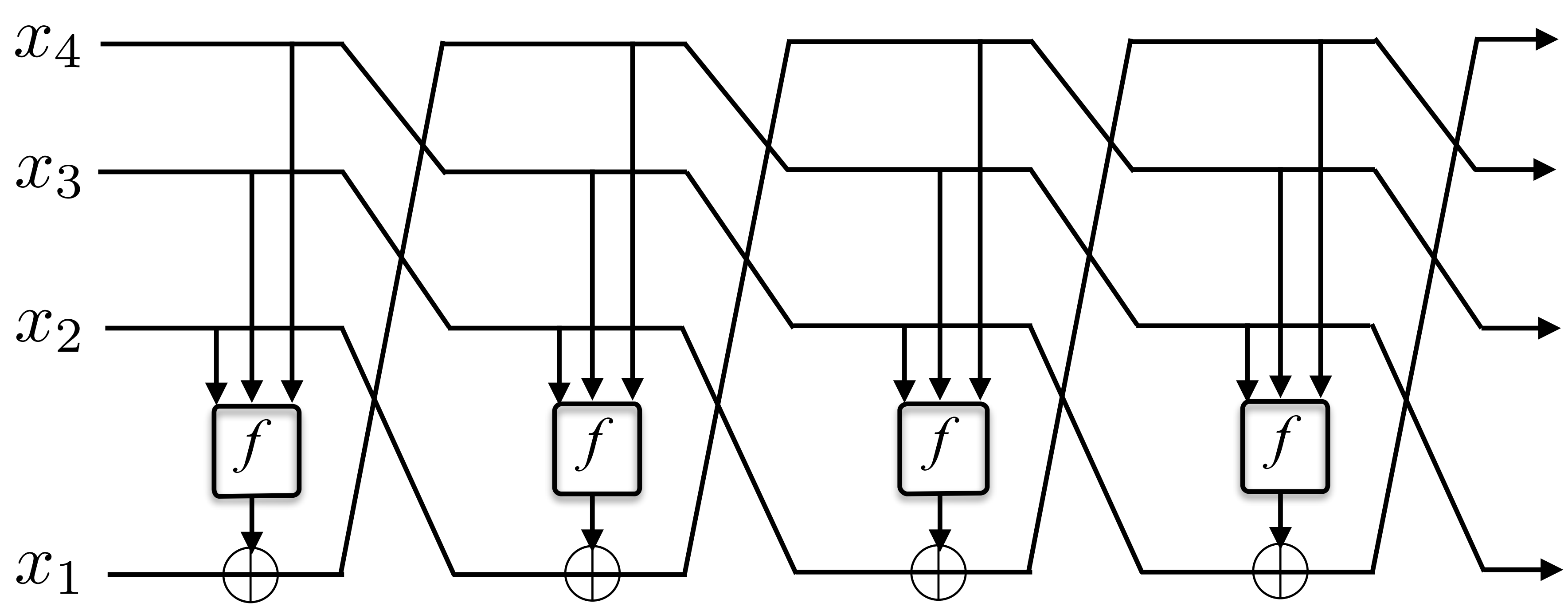


$$P_f(x_1, x_2, x_3, x_4) = (x_2, x_3, x_4, x_1 + f(x_2, x_3, x_4))$$

$$P_f^t = P_f(P_f^{t-1}), P_f^1 = P_f$$

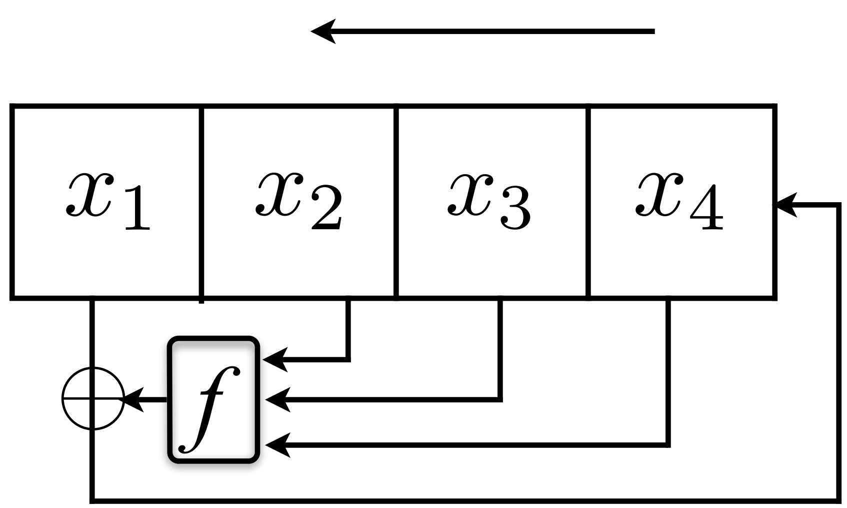
Construction of S-boxes with unbalanced Feistel structure

Implementation of P_f^4



Construction of S-boxes with unbalanced Feistel structure

Implementation of P_f^4



4 round NLFSR

Optimal 4-bit S-boxes

$$k = 1, x_i \in \mathbb{F}_2, P_f^4, P_f^5 : \mathbb{F}_2^4 \mapsto \mathbb{F}_2^4.$$

Optimal 4-bit S-box [G. Leander, A. Poschmann 07]

- A 4-bit S-box is called optimal if it is a permutation over $\mathbb{F}_{2^4}$ with differential uniformity 4 and nonlinearity 4.
- There are 16 classes of optimal 4-bit S-boxes up to affine equivalence.

Construction of optimal 4-bit S-boxes, 4-round

f	Operations	G_i	f	Operations	G_i
x_2x_3	(1, 1, 0)	8	x_2x_3+1	(1, 1, 1)	8
x_3x_4	(1, 1, 0)	8	x_3x_4+1	(1, 1, 1)	8
$(x_3+1)x_4$	(1, 1, 1)	8	$(x_3+1)x_4+1^\star$	(1, 1, 2)	8
$x_2(x_3+1)$	(1, 1, 1)	8	$x_2(x_3+1)+1^\star$	(1, 1, 2)	8
$x_3(x_4+1)$	(1, 1, 1)	8	$x_3(x_4+1)+1^\star$	(1, 1, 2)	8
$(x_2+1)x_3$	(1, 1, 1)	8	$(x_2+1)x_3+1^\star$	(1, 1, 2)	8
$(x_2+1)(x_3+1)+1$	(1, 1, 3)	8	$(x_2+1)(x_3+1)$	(1, 1, 2)	8
$(x_3+1)(x_4+1)+1$	(1, 1, 3)	8	$(x_3+1)(x_4+1)$	(1, 1, 2)	8
$x_2x_3+x_4$	(2, 1, 0)	8	$x_2x_3+x_4+1^\star$	(2, 1, 1)	8
$x_2+x_3x_4$	(2, 1, 0)	8	$x_2+x_3x_4+1^\star$	(2, 1, 1)	8
$x_2+(x_3+1)x_4$	(2, 1, 1)	8	$x_2+(x_3+1)x_4+1$	(2, 1, 2)	8
$(x_2+1)x_3+x_4$	(2, 1, 1)	8	$(x_2+1)x_3+x_4+1$	(2, 1, 2)	8
$x_2+x_3(x_4+1)$	(2, 1, 1)	8	$x_2+x_3(x_4+1)+1$	(2, 1, 2)	8
$x_2(x_3+1)+x_4$	(2, 1, 1)	8	$x_2(x_3+1)+x_4+1$	(2, 1, 2)	8
$x_2+(x_3+1)(x_4+1)+1$	(2, 1, 3)	8	$x_2+(x_3+1)(x_4+1)^\star$	(2, 1, 2)	8
$(x_2+1)(x_3+1)+x_4+1$	(2, 1, 3)	8	$(x_2+1)(x_3+1)+x_4^\star$	(2, 1, 2)	8
$x_2(x_3+x_4)+x_3x_4$	(3, 2, 0)	1	$x_2(x_3+x_4)+x_3x_4+1$	(3, 2, 1)	1
$x_2(x_4+x_3+1)+(x_3+1)x_4$	(3, 2, 1)	1	$x_2(x_4+x_3+1)+(x_3+1)x_4+1$	(3, 2, 2)	1
$x_2(x_3+x_4+1)+x_3(x_4+1)$	(3, 2, 1)	1	$x_2(x_3+x_4+1)+x_3(x_4+1)+1$	(3, 2, 2)	1
$(x_2+1+x_4)x_3+(x_2+1)x_4$	(3, 2, 1)	1	$(x_2+1+x_4)x_3+(x_2+1)x_4+1$	(3, 2, 2)	1

Table 2. Boolean functions such that P_f^4 are optimal 4-bit S-boxes

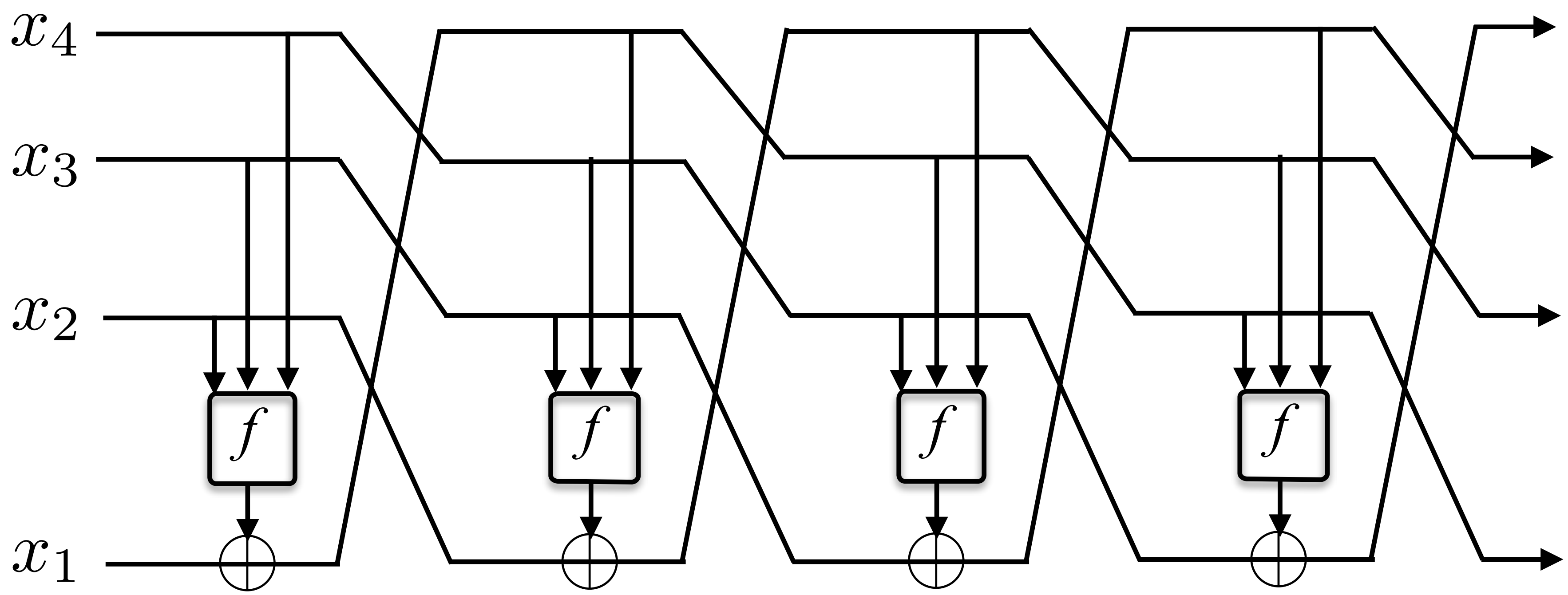
Construction of optimal 4-bit S-boxes, 5-round

f	Operations	G_i	f	Operations	G_i
$x_2(x_3+x_4)+1$	(2, 1, 1)	7	$(x_2+x_4)x_3+1^\star$	(2, 1, 1)	4
$(x_2+x_3)x_4+1$	(2, 1, 1)	7	$(x_2+x_4)(x_3+1)+1^\star$	(2, 1, 2)	4
$(x_2+x_3)(x_4+1)+1$	(2, 1, 2)	7	$(x_2+1)(x_3+x_4)+1$	(2, 1, 2)	7
$x_2x_3+(x_2+1)x_4$	(2, 2, 1)	13	$x_2(x_4+1)+x_3x_4$	(2, 2, 1)	13
$x_2x_4+x_3(x_4+1)+1$	(2, 2, 2)	13	$x_2(x_3+1)+x_3(x_4+1)$	(2, 2, 2)	4
$(x_2+1)x_3+x_2x_4+1$	(2, 2, 2)	13	$x_2x_4+(x_3+1)(x_4+1)^\star$	(2, 2, 2)	13
$x_2x_3+(x_2+1)(x_4+1)^\star$	(2, 2, 2)	13	$(x_2+1)(x_4+1)+x_3x_4^\star$	(2, 2, 2)	13
$(x_2+1)(x_3+1)+x_2x_4^\star$	(2, 2, 2)	13	$(x_2+1)x_3+(x_3+1)x_4$	(2, 2, 2)	4
$x_2((x_3+1)x_4+1)+x_3(x_4+1)$	(2, 3, 3)	11	$(x_2(x_4+1)+1)x_3+(x_2+1)x_4$	(2, 3, 3)	11
$(x_2x_3+1)x_4+(x_2+1)(x_3+1)$	(2, 3, 3)	11	$x_2(x_3x_4+1)+(x_3+1)(x_4+1)$	(2, 3, 3)	11
$(x_2x_3+1)x_4+(x_2+1)(x_3+1)+1$	(2, 3, 4)	11	$(x_2x_4+1)x_3+(x_2+1)(x_4+1)+1$	(2, 3, 4)	3
$x_2(x_3x_4+1)+(x_3+1)(x_4+1)+1$	(2, 3, 4)	11	$x_2(x_3(x_4+1)+1)+(x_3+1)x_4+1$	(2, 3, 4)	3
$(x_2(x_4+1)+1)x_3+(x_2+1)x_4+1$	(2, 3, 4)	11	$x_2((x_3+1)x_4+1)+x_3(x_4+1)+1$	(2, 3, 4)	11

Table 3. Boolean functions such that P_f^5 are optimal 4-bit S-boxes

Construction of 8-bit S-box with unbalanced Feistel structure

$$k = 2, x_i \in \mathbb{F}_{2^2}, P_f^4 : \mathbb{F}_{2^2}^4 \mapsto \mathbb{F}_{2^2}^4.$$



For any f in Table 2, P_f^4 is an 8-bit S-boxes with

- differential uniformity 16;
- nonlinearity 96.

THANK YOU!

yongq.lee@gmail.com