Parallelizing the Camellia and SMS4 Block Ciphers

Huihui Yap[1,2], Khoongming Khoo [1,2] and **Axel Poschmann**[2]

[1]DSO National Laboratories, Singapore

[2]Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

Africacrypt 2010, 3-6 May

Outline of Talk

Motivation

- Object of interest: Parallelizable n-cell GF-NLFSR structures
- Encryption speed faster by up to n times
- Nonlinear round functions such as SDS structures too complex $\Rightarrow$ not suitable for space and speed efficient implementation
- SPN round functions use relatively less resources
- $\Rightarrow$ We investigate practical security against DC and LC of bijective SPN round functions

Our Contribution

- Provide a neat and concise proof for the minimum number of differential active S-boxes
- Parallelizing Camellia and SMS4: p-Camellia and p-SMS4
- Ensure that p-Camellia and p-SMS4 are secure against other block cipher cryptanalysis
- Hardware implementation advantages: Achieves higher maximum frequency with lower area and power demands

SPN round function

- F-function comprises: key addition layer, S-function, P-function.
- Neglect the effect of the round key since by assumption, the round key consists of independent and uniformly random bits, and is bitwise XORed with data
- S-function: non-linear transformation layer with m parallel d-bit bijective S-boxes
- P-function is a linear transformation layer

SPN round function

- Throughout, assume S-function and P-function bijective

$$\begin{aligned}
S &: GF(2^d)^m \to GF(2^d)^m\ ,\ X = (x_1, \cdots, x_m) \mapsto Z = S(X) = (s_1(x_1), \cdots, s_n(x_n)) \\
P &: GF(2^d)^m \to GF(2^d)^m\ ,\ Z = (z_1, \cdots, z_m) \mapsto Y = P(Z) = (y_1, \cdots, y_n) \\
F &: GF(2^d)^m \to GF(2^d)^m\ ,\ X \mapsto Y = F(X) = P(S(X))
\end{aligned}$$

Differential and Linear Probabilities

Definition

Let $x, z \in GF(2^d)$. Denote the differences and the mask values of x and z by Δx, Δz, and, Γx, Γz respectively. The differential and linear probabilities of each S-box s_i are defined as:

$$DP^{s_i}(\Delta x \rightarrow \Delta z) = \frac{\#\{x \in GF(2^d) | s_i(x) \oplus s_i(x \oplus \Delta x) = \Delta z\}}{2^d},$$

$$LP^{s_i}(\Gamma z \rightarrow \Gamma x) = (2 \times \frac{\#\{x \in GF(2^d) | x \cdot \Gamma x = s_i(x) \cdot \Gamma z\}}{2^d} - 1)^2.$$

Differential and Linear Probabilities

Definition

The maximum differential and linear probabilities of S-boxes are defined as:

$$p_s = \max_i \max_{\Delta x \neq 0, \Delta z} DP^{s_i}(\Delta x \rightarrow \Delta z),$$

$$q_s = \max_i \max_{\Gamma x, \Gamma z \neq 0} LP^{s_i}(\Gamma z \rightarrow \Gamma x).$$

Hamming Weight and Branch Number

Definition

Let $X = (x_1, x_2, \cdots, x_m) \in GF(2^d)^m$. Then the Hamming weight of X is denoted by $H_w(X) = \#\{i | x_i \neq 0\}$.

Hamming Weight and Branch Number

Definition

Let $X = (x_1, x_2, \cdots, x_m) \in GF(2^d)^m$. Then the Hamming weight of X is denoted by $H_w(X) = \#\{i | x_i \neq 0\}$.

Definition

The branch number $\mathcal{B}$ of linear transformation θ is defined as follows:

$$\mathcal{B} = \min_{x \neq 0}(H_w(x) + H_w(\theta(x))).$$

Branch Number - DC and LC

- **Differential case:**
- $\mathcal{B} = \min_{\Delta X \neq 0}(H_w(\Delta X) + H_w(\Delta Y))$
- ΔX is an input difference into the S-function, ΔY is an output difference of the P-function

Branch Number - DC and LC

- **Differential case:**
- $\mathcal{B} = \min_{\Delta X \neq 0}(H_w(\Delta X) + H_w(\Delta Y))$
- ΔX is an input difference into the S-function, ΔY is an output difference of the P-function

- **Linear case:**
- $\mathcal{B} = \min_{\Gamma Y \neq 0}(H_w(P^*(\Gamma Y)) + H_w(\Gamma Y))$
- ΓY is an output mask value of the P-function
- P^* is a diffusion function of mask values concerning the P-function
- Throughout, $\mathcal{B}$ is used to denote differential or linear branch number, depending on the context

Number of active S-boxes

Definition

A differential active S-box is defined as an S-box given a non-zero input difference. Similarly, a linear active S-box is defined as an S-box given a non-zero output mask value.

Number of active S-boxes

Definition

A differential active S-box is defined as an S-box given a non-zero input difference. Similarly, a linear active S-box is defined as an S-box given a non-zero output mask value.

Theorem

Let $\mathcal{D}^{(r)}$ and $\mathcal{L}^{(r)}$ be the minimum number of all differential and linear active S-boxes for an r-round Feistel cipher respectively. Then the maximum differential and linear characteristic probabilities of the r-round cipher are bounded by $p_s^{D^{(r)}}$ and $q_s^{L^{(r)}}$ respectively.

Kanda's result

Theorem

The minimum number of differential (and linear) active S-boxes $\mathcal{D}^{(4r)}$ for $4r$-round Feistel ciphers with SPN round function is at least $r\mathcal{B} + \lfloor \frac{r}{2} \rfloor$.

Structure of *n*-cell GF-NLFSR

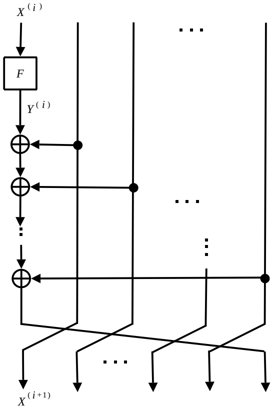


Figure: *i*-th round of GF-NLFSR

- Proposed in (CCKY ACISP'09)
- *n*-cell extension of the outer function *FO* of KASUMI (2-cell)
- Parallelizable, up to *n* times
- $$X^{(i+n)} = Y^{(i)} \oplus X^{(i+1)} \oplus \cdots \oplus X^{(i+n-1)}$$
  for $i = 1, 2, \cdots$.

Practical Security against DC

- Aim: investigate the upper bound of the maximum differential characteristic probability of GF-NLFSR cipher
- $\Rightarrow$ Need to find lower bound for $\mathcal{D}^{(r)}$

Lemma

For n-cell GF-NLFSR cipher, the minimum number of differential active S-boxes in any 2n consecutive rounds satisfies $\mathcal{D}^{(2n)} \geq \mathcal{B}$.

Practical Security against DC

Proof.

- Assume that the $2n$ consecutive rounds run from the first round to the $2n$-th round
- For $j = 1, \cdots, n$, at least one of $\Delta X^{(j)} \neq 0$
- Let i be the smallest integer such that $\Delta X^{(i)} \neq 0$, where $1 \leq i \leq n$. Then

$$\mathcal{D}^{(2n)} = H_w(\Delta X^{(1)}) + H_w(\Delta X^{(2)}) + \cdots + H_w(\Delta X^{(2n)})$$

Practical Security against DC

Proof.

- Assume that the $2n$ consecutive rounds run from the first round to the $2n$-th round
- For $j = 1, \cdots, n$, at least one of $\Delta X^{(j)} \neq 0$
- Let i be the smallest integer such that $\Delta X^{(i)} \neq 0$, where $1 \leq i \leq n$. Then

$$\begin{aligned}\mathcal{D}^{(2n)} &= H_w(\Delta X^{(1)}) + H_w(\Delta X^{(2)}) + \cdots + H_w(\Delta X^{(2n)}) \\ &\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)}) \cdots + H_w(\Delta X^{(i+n)})\end{aligned}$$

Practical Security against DC

Proof.

- Assume that the $2n$ consecutive rounds run from the first round to the $2n$-th round
- For $j = 1, \cdots, n$, at least one of $\Delta X^{(j)} \neq 0$
- Let i be the smallest integer such that $\Delta X^{(i)} \neq 0$, where $1 \leq i \leq n$. Then

$$
\begin{aligned}
\mathcal{D}^{(2n)} &= H_w(\Delta X^{(1)}) + H_w(\Delta X^{(2)}) + \cdots + H_w(\Delta X^{(2n)}) \\
&\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)}) \cdots + H_w(\Delta X^{(i+n)}) \\
&\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)} \oplus \cdots \oplus \Delta X^{(i+n)}),
\end{aligned}
$$

Practical Security against DC

Proof.

- Assume that the $2n$ consecutive rounds run from the first round to the $2n$-th round
- For $j = 1, \cdots, n$, at least one of $\Delta X^{(j)} \neq 0$
- Let i be the smallest integer such that $\Delta X^{(i)} \neq 0$, where $1 \leq i \leq n$. Then

$$
\begin{aligned}
\mathcal{D}^{(2n)} &= H_w(\Delta X^{(1)}) + H_w(\Delta X^{(2)}) + \cdots + H_w(\Delta X^{(2n)}) \\
&\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)}) \cdots + H_w(\Delta X^{(i+n)}) \\
&\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)} \oplus \cdots \oplus \Delta X^{(i+n)}), \\
&= H_w(\Delta X^{(i)}) + H_w(\Delta Y^{(i)})
\end{aligned}
$$

Practical Security against DC

Proof.

- Assume that the $2n$ consecutive rounds run from the first round to the $2n$-th round
- For $j = 1, \cdots, n$, at least one of $\Delta X^{(j)} \neq 0$
- Let i be the smallest integer such that $\Delta X^{(i)} \neq 0$, where $1 \leq i \leq n$. Then

$$\begin{aligned}
\mathcal{D}^{(2n)} &= H_w(\Delta X^{(1)}) + H_w(\Delta X^{(2)}) + \cdots + H_w(\Delta X^{(2n)}) \\
&\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)}) \cdots + H_w(\Delta X^{(i+n)}) \\
&\geq H_w(\Delta X^{(i)}) + H_w(\Delta X^{(i+1)} \oplus \cdots \oplus \Delta X^{(i+n)}), \\
&= H_w(\Delta X^{(i)}) + H_w(\Delta Y^{(i)}) \\
&\geq \mathcal{B}.
\end{aligned}$$

Practical Security against DC

Remark

- With probability $1 - \frac{1}{M}$, where M is the size of each cell, i.e. most of the time, $\Delta X^{(1)} \neq 0$
- $\Rightarrow$ Able to achieve at least $\mathcal{B}$ number of differential active S-boxes over $(n+1)$-round most of the time

Practical Security against DC

With the previous lemma, straightforward to prove:

Theorem

The minimum number of differential active S-boxes for 2nr-round n-cell GF-NLFSR cipher with bijective SPN round function satisfies

$$\mathcal{D}^{(2nr)} \geq r\mathcal{B} + \lfloor \frac{r}{2} \rfloor.$$

Practical Security against DC

Observations:

- When $n = 2$, $\mathcal{D}^{(4r)} \geq r\mathcal{B} + \lfloor \frac{r}{2} \rfloor$
- $\Rightarrow$ Similar security against DC as Feistel ciphers with bijective SPN round function
- 2-cell GF-NLFSR has added advantage: parallelizable

Practical Security against LC

- Need to find lower bound for $\mathcal{L}^{(r)}$

Lemma

For 2-cell GF-NLFSR cipher with bijective SPN round function and linear branch number $\mathcal{B} = 5$, the minimum number of linear active S-boxes in any 4 consecutive rounds satisfies $\mathcal{L}^{(4)} \geq 3$.

Practical Security against LC

Outline of proof:

- $\Gamma X^{(i)}$ and $\Gamma Y^{(i)}$: input, output mask values to the i-th round F function
- Assume that the 4 consecutive rounds run from the first round to the 4th round
- $\mathcal{L}^{(4)} = H_w(\Gamma Y^{(1)}) + H_w(\Gamma Y^{(2)}) + H_w(\Gamma Y^{(3)}) + H_w(\Gamma Y^{(4)})$
- Duality between differential characteristic and linear approximation: $\Gamma Y^{(i+1)} = \Gamma X^{(i-1)} \oplus \Gamma X^{(i)}$, for $i = 2$ and 3
- Go through all possible cases (1. $\Gamma Y^{(1)} = 0$, 2. $\Gamma Y^{(1)} \neq 0, \Gamma Y^{(2)} = 0 \ldots$)

Practical Security against LC

With the previous lemma, straightforward to prove:

Theorem

For 2-cell GF-NLFSR cipher with bijective SPN round function and linear branch number $\mathcal{B} = 5$, we have

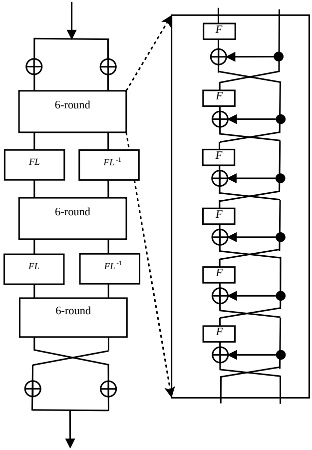
1. $\mathcal{L}^{(8)} \geq 7$,
2. $\mathcal{L}^{(12)} \geq 11$,
3. $\mathcal{L}^{(16)} \geq 15$,

where $\mathcal{L}^{(r)}$ is the minimum number of linear active S-boxes over r rounds.

Camellia

- Jointly developed by NTT and Mitsubishi Electric Corporation
- 18-round Feistel structure for 128-bit key and 24 rounds for 192-bit and 256-bit keys,
- Additional input/output whitenings and logical functions, FL-function and FL^{-1}-function, inserted every 6 rounds
- Bijective SPN F-function
- S-function: 8 S-boxes in parallel
- P-function: bytewise exclusive-ORs
- $\mathcal{B} = 5$; $p_s, q_s = 2^{-6}$

p-Camellia: "*Parallelizable*" Camellia



- Replace Feistel network with 2-cell GF-NLFSR
- Other components such as number of rounds, S-function, P-function and the key schedule etc remain unchanged

DC of p-Camellia

- p: Maximum differential characteristic probabilities reduced to 16-round
- Over 16 rounds $\Rightarrow$ four 4-round blocks
- Recall: $\mathcal{B} = 5$, $p_s = 2^{-6}$
- By previous results, minimum number of differential active S-boxes $= 4 \times 5 + 2 = 22$
- $\Rightarrow p \leq (2^{-6})^{22} = 2^{-132} < 2^{-128}$
- $\Rightarrow$ Secure against DC

LC of p-Camellia

- q: Maximum linear characteristic probabilities reduced to 16-round
- By previous results, minimum number of linear active S-boxes is 15
- $\Rightarrow q \leq (2^{-6})^{15} = 2^{-90}$
- $\Rightarrow$ Attacker needs to collect at least 2^{90} chosen/known plaintexts to mount an attack, which is not feasible in practice
- $\Rightarrow$ Secure against LC

Other Attacks on p-Camellia

- **Boomerang attack**: Can be shown that for 16 rounds, probability of finding a boomerang distinguisher $\leq 2^{-180}$
  $\Rightarrow$ Secure against boomerang attack
- **Impossible differential attack**: Maximum length of impossible differential distinguisher is 4
  $\Rightarrow$ Full cipher secure against impossible differential attack
- **Integral attack**: Maximum length of integral distinguisher is 4 and attacker can extend by at most 3 rounds
  $\Rightarrow$ Full cipher secure against impossible differential attack

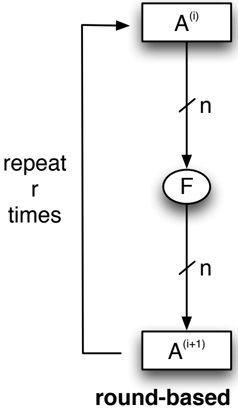
Other Attacks on p-Camellia

- **Slide attack**: FL- and FL^{-1}-functions provide non-regularity across rounds, and different subkeys used for every round
  $\Rightarrow$ Unlikely to work

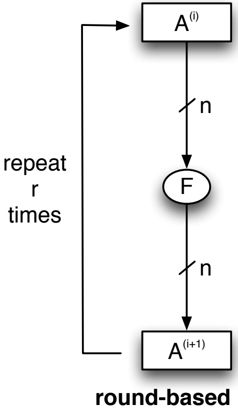
- **Higher order differential attack**: Algebraic degree reaches maximum degree of 127 after 6th round
  $\Rightarrow$ Unlikely to work

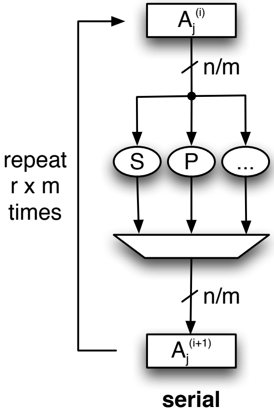
- **Interpolation attack**: After passing through many S-boxes and P-functions, cipher becomes a complex function which is a sum of many multi-variate monomials over $GF(2^8)$
  $\Rightarrow$ Unlikely to work

HW Implementation Strategies

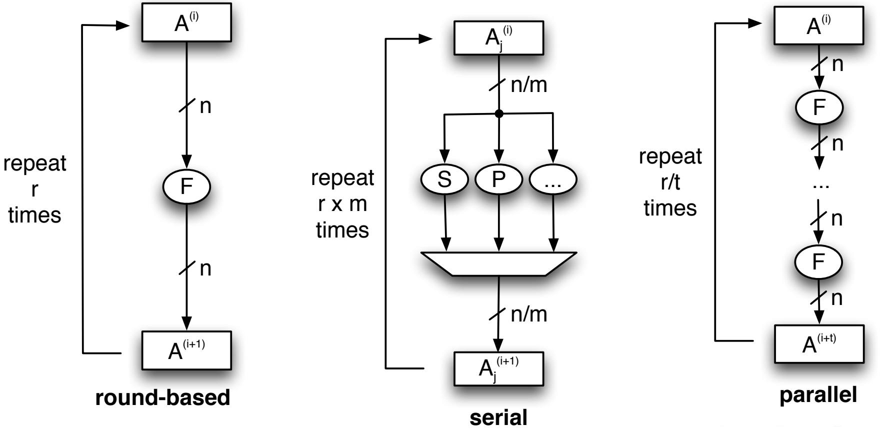


HW Implementation Strategies

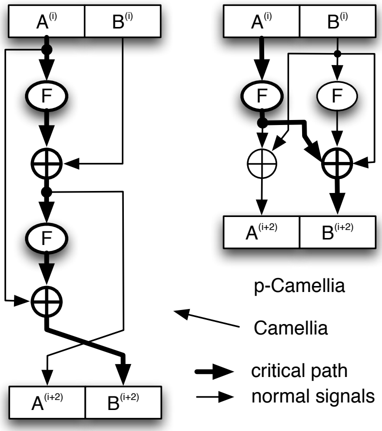




HW Implementation Strategies

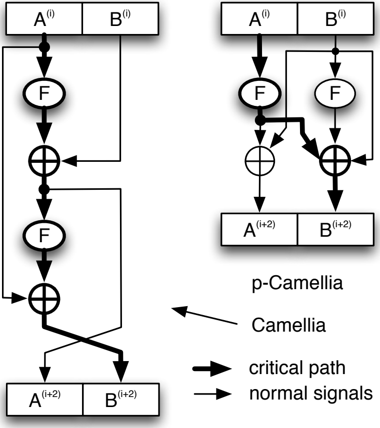


Implementation Advantages of p-Camellia



- *serialized*: no disadvantage
- *round-based*: no disadvantage

Implementation Advantages of p-Camellia



- *serialized*: no disadvantage
- *round-based*: no disadvantage
- *parallelized*: critical path is halved
  - $\longrightarrow$ double Max. Freq.
  - $\longrightarrow$ lower fan-out
  - $\longrightarrow$ lower gate count
  - $\longrightarrow$ lower power consumption
- if fully pipelined $\longrightarrow$ delay is halved

SMS4

- Underlying block cipher used in WAPI standard (Chinese national WLAN standard)
- 128-bit key, 32-round generalized Feistel structure
- Each round transforms four 32-bit words X_i, $i = 0, 1, 2, 3$:

$$(X_0, X_1, X_2, X_3, rk) \mapsto (X_1, X_2, X_3, X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)),$$

where rk denotes the round key

- Non-linear function T: 32-bit subkey addition, S-box Substitution (layer of four 8-bit S-boxes), a 32-bit linear transformation L
- $\mathcal{B} = 5$; $p_s, q_s = 2^{-6}$
- Key schedule has similar structure to main cipher with slight differences

p-SMS4: "*Parallelizable*" SMS4

- Replace generalized Feistel network with 4-cell GF-NLFSR
- Modify key schedule to have same structure as the main cipher: also parallelizable in hardware
- Other components such as number of rounds, S-function, P-function etc remain unchanged

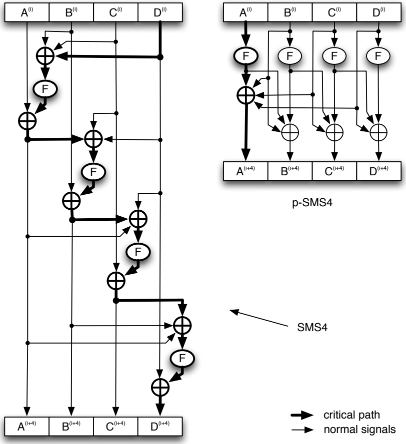
Security of p-SMS4 against block cipher attacks

- Follows similar analysis to p-Camellia
- E.g. Can be shown differential characteristic probability over 29 rounds $\leq 2^{-108}$
- $\Rightarrow$ Attacker needs to collect at least 2^{108} chosen plaintext-ciphertext pairs
- For random input differences, only 2^{-32} of the time do we need 8 rounds to ensure at least 5 active S-boxes
- Similar to SMS4, no bound for characteristic linear probability of p-SMS4 provided in this paper
- But the bound has been derived! (upcoming extended version)

Security of p-SMS4 against block cipher attacks

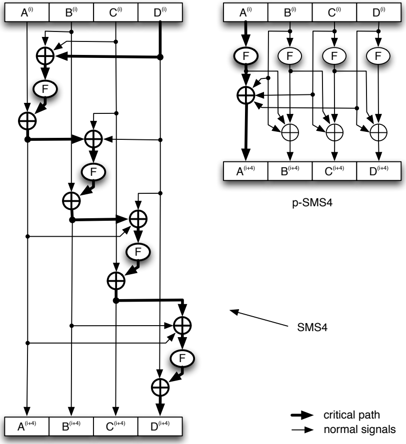
- Similar to p-Camellia, we show that p-SMS4 is secure against boomerang, impossible differential, integral, slide, XSL, higher order differential and interpolation attacks.
- Differential probability for the key schedule is at most 2^{-90}.
  $\longrightarrow$ related key differential attack is not feasible (at least 2^{90} related keys required).

Implementation Advantages of p-SMS4



- *serialized*: no disadvantage
- *round-based*: no disadvantage

Implementation Advantages of p-SMS4



- *serialized*: no disadvantage
- *round-based*: no disadvantage
- *parallelized*: critical path is $\frac{1}{4}$
  - $\rightarrow$ 4x Max. Freq.
  - $\rightarrow$ lower fan-out
  - $\rightarrow$ lower gate count
  - $\rightarrow$ lower power consumption
- if fully pipelined $\rightarrow$ delay is $\frac{1}{4}$

Conclusion

- Proposed the use of n-cell GF-NLFSR structure to parallelize (Generalized) Feistel structures
- Used two examples, p-Camellia and p-SMS4, and showed that they offer sufficient security against various known existing attacks
- Hardware implementations have n times higher maximum frequency, while having lower area and power demands
- $\Rightarrow$ n-cell GF-NLFSRs are particularly well suited for high throughput applications

Thank you!