Parallelisable variants of Camellia and SMS4 block cipher: p-Camellia and p-SMS4

Huihui Yap* and Khoongming Khoo

DSO National Laboratories,
20 Science Park Drive, 118230, Singapore
and
Division of Mathematical Sciences,
School of Physical and Mathematical Sciences,
Nanyang Technological University,
21 Nanyang Link, 637371, Singapore
E-mail: yhuihui@dso.org.sg
E-mail: kkhoongm@dso.org.sg
*Corresponding author

Axel Poschmann

Division of Mathematical Sciences,
School of Physical and Mathematical Sciences,
Nanyang Technological University,
21 Nanyang Link, 637371, Singapore
E-mail: aposchmann@ntu.edu.sg

Abstract: We propose two parallelisable variants of Camellia and SMS4 block ciphers based on the *n*-cell GF-NLFSR. The *n*-cell generalised Feistel-non-linear feedback shift register (GF-NLFSR) structure (Choy et al., 2009a) is a generalised unbalanced Feistel network that can be considered as a generalisation of the outer function *FO* of the KASUMI block cipher. An advantage of this cipher over other *n*-cell generalised Feistel networks, e.g., SMS4 (Diffe and Ledin, 2008) and Camellia (Aokiet al., 2001), is that it is parallelisable for up to *n* rounds. In hardware implementations, the benefits translate to speeding up encryption by up to *n* times while consuming similar area and significantly less power. At the same time, *n*-cell GF-NLFSR structures offer similar proofs of security against differential cryptanalysis as conventional *n*-cell Feistel structures. In this paper, we prove security against differential, linear and boomerang attacks. We also show that the selected number of rounds are conservative enough to provide high security margin against other known attacks such as integral, impossible differential, higher order differential, interpolation, slide, XSL and related-key differential attacks.

Keywords: generalised unbalanced Feistel network; GF-NLFSR; Camellia; SMS4.

Reference to this paper should be made as follows: Yap, H., Khoo, K. and Poschmann, A. (2013) 'Parallelisable variants of Camellia and SMS4 block cipher: p-Camellia and p-SMS4', *Int. J. Applied Cryptography*, Vol. 3, No. 1, pp.1–20.

Biographical notes: Huihui Yap received her BSc (First Class Honours) and Master in Mathematics from the National University of Singapore. She is currently a Researcher at DSO National Laboratories and a part-time PhD student (Mathematics) at Nanyang Technological University, both in Singapore. Her current research interest is on applied cryptography.

Khoongming Khoo received his BS (Hons.) in Mathematics from the National University of Singapore, and his PhD in Combinatorics and Optimisation from the University of Waterloo, Canada. He is currently a Researcher at DSO National Laboratories and an Adjunct Associate Professor at Nanyang Technological University, both in Singapore. His current research interest is on applied cryptography.

Axel Poschmann is an Assistant Professor at Nanyang Technological University (NTU), Singapore. In 2009, he received his PhD in Electrical Engineering from Ruhr University Bochum, Germany, where he also graduated as an IT Security Engineer (2005); both under the supervision of Christof Paar. In 2008, he received his Master in Business Studies from the University Hagen, Germany. From 2009 to 2011, he worked as a Postdoctoral Research Fellow with the Coding and Cryptography Research Group at NTU. He is the Editor of the IACR book reviews, Co-editor of the ISO standard 29192-2 on lightweight block ciphers, and one of the designers of the award-winning block cipher PRESENT. His primary research interests include lightweight cryptography and side channel aspects for pervasive devices.

1 Introduction

1.1 Background and motivation

Two very important security properties of block cipher structures are low differential and linear probability bounds for protection against differential and linear cryptanalysis. Choy et al. (2009a) had proven that the 'true' differential/linear probabilities of any n rounds of the n-cell GF-NLFSR structure is p^2 if the differential/linear probability of the non-linear function of each round is p. However, this result is applicable only if we use a non-linear function with good provable differential/linear probability. One option is to use an S-box. However, if the non-linear function takes in 32-bit input, an S-box of this size would be infeasible to implement in terms of logic gates in hardware or as a look-up-table in memory. Other options would be to build a substitution-diffusion-substitution (SDS) structure (Park et al., 2003), use a Feistel structure (http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf) or even a nested Feistel structure for the non-linear function (http://www.etsi.org/website/document/algorithms/ts_135202v070000p.pdf) because there are provable bounds for the differential and linear probabilities of these structures.

However, these non-linear functions are too complex, and cannot be implemented efficiently with respect to either space or speed. Therefore, the substitution-then-diffusion structure is usually implemented for the non-linear functions. These structures are commonly called substitution permutation networks (SPN) in the literature. Numerous examples of implementations where the SPN structure is used for the non-linear functions of Feistel and generalised Feistel structures exist. They include DES (National Bureau of Standards, 1977), Camellia (Aoki et al., 2001), SMS4 (Diffe and Ledin, 2008) and Clefia (Shirai et al., 2007), to name a few. Motivated by these considerations, we would like to investigate the practical differential and linear probability bounds of the n-cell GF-NLFSR structure when the non-linear function is a SPN structure.

As applications, we would like to parallelise some of the abovementioned ciphers, where we replace the (generalised) Feistel structures by the parallelisable GF-NLFSR structures, while keeping the internal components like S-boxes and linear diffusion to be the same. This would make encryption speed faster by up to n times. Two candidates which we find promising for parallelising are the Camellia and SMS4 ciphers.

1.2 Related works

In order to analyse the resistance of a block cipher against differential and linear cryptanalysis, we would like to establish a lower bound for the number of active S-boxes (S-boxes which contribute to the differential/linear probability) in any differential/linear characteristic path over a fixed number of rounds. Using such bounds, the cipher designer can choose a large enough number of rounds so that there are too many active S-boxes for differential/linear cryptanalysis to be successful.

Kanda (2001) has proven that for a Feistel cipher with an SPN round function having branch number $\mathcal{B}$ (a measure of dispersion, please refer to Section 2 for the exact definition), the number of active S-boxes in any differential and linear characteristic path over every $4r$ rounds is at least $r\mathcal{B}+\left\lfloor \frac{r}{2} \right\rfloor$. Based on this lower bound, the authors of Aoki et al. (2001) designed the block cipher Camellia, which has practical provable security against differential and linear cryptanalysis.

1.3 Our contribution

In Section 3, we provide a neat and concise proof of the result that for a $2nr$-round parallelisable n-cell GF-NLFSR structure with an SPN round function having branch number $\mathcal{B}$, the number of active S-boxes in any differential characteristic path is at least $r\mathcal{B}+\left\lfloor \frac{r}{2} \right\rfloor$. The result holds for any $n \geq 2$ in general, and we expect the result to be useful in the design and analysis of block cipher structures. For the case of a 2-cell GF-NLFSR structure, we have $r\mathcal{B}+\left\lfloor \frac{r}{2} \right\rfloor$ active S-boxes over every $4r$ rounds, which is the same as Kanda's (2001) result for a conventional 2-cell Feistel structure. Motivated by this observation, we propose in Section 4 a parallelisable version of Camellia, p-Camellia, where we change the conventional Feistel structure to a 2-cell GF-NLFSR structure but keep all other components such as S-boxes and linear diffusion maps to be the same. We also prove the security of p-Camellia against linear and boomerang attacks, and that the selected number of rounds are conservative enough to provide high security margin against other known attacks such as integral, impossible differential, higher order differential, interpolation and slide attacks.

In addition, we assess the advantages of hardware implementations. For this reason, we briefly introduce design strategies for hardware implementations. We then show that especially for applications with high throughput requirements, a 2-cell GF-NLFSR such as p-Camellia offers significant advantages over a conventional 2-cell Feistel structure such as Camellia. In particular, we show that an implementation of p-Camellia that processes two rounds in parallel has a maximum frequency that is nearly twice as high as it would be for Camellia while having similar area demands and significantly less power demands. We also show that for fully pipelined implementations a conventional 2-cell Feistel structure requires twice as many pipeline stages, and hence twice as many clock cycles delay, to achieve the same frequency as it is the case for a 2-cell GF-NLFSR.

In Section 5, we also apply a 4-cell GF-NLFSR structure to form a parallelisable version of SMS4 called p-SMS4. We change the generalised Feistel structure in both the main cipher and key schedule of SMS4 to a 4-cell

GF-NLFSR structure but keep all other components such as S-boxes and linear diffusion maps to be the same. We first prove that p-SMS4 is secure against differential and linear cryptanalysis. Biryukov et al. (2009) showed a powerful related-key differential attack on AES-256 which can recover the secret key with complexity 2^{131} using 2^{35} related keys. We give a proof through the p-SMS4 key schedule that p-SMS4 is resistant against this attack. We also prove the security of p-Camellia against boomerang attack, and that the selected number of rounds are conservative enough to provide high security margin against other known attacks such as integral, impossible differential, higher order differential, interpolation, slide and XSL attacks.

A 4-cell GF-NLFSR structure offers also implementation advantages for round-based and parallelised hardware architectures. We show that a 4-cell GF-NLFSR structure, implemented in an architecture that processes four rounds in one clock cycle, has a significantly shorter critical path, and hence a higher maximum frequency, than a conventional 4-cell Feistel structure. In parallelised implementations, this advantage increases to a nearly four times higher maximum frequency while having similar area demands and significantly less power demands. In general, the advantage is dependent on the number of branches, hence an *n*-cell GF-NLFSR has an advantage of a nearly n times higher maximum frequency.

This paper is an extended version of Yap et al. (2010). We added an explanation of the duality between differential and linear cryptanalysis for the p-Camellia and p-SMS4 structures in Section 3.2, and corrected a slight notational error in the proof of protection against linear cryptanalysis for p-Camellia in Yap et al. (2010). In addition, a proof for protection against linear cryptanalysis for p-SMS4 was given. We also did a hardware implementation of p-Camellia and p-SMS4 and presented the speed-up over Camellia and SMS4 respectively in this extended paper. Finally, we added test vectors for p-Camellia and p-SMS4.

2 Definitions and preliminaries

In this section, we will list some definitions and summarise the results of Kanda (2001). He has proven the upper bounds of the maximum differential and linear characteristic probabilities of Feistel ciphers with bijective SPN round functions. More explicitly, the round function *F*-function comprises the key addition layer, the S-function and the *P*-function. Here, we neglect the effect of the round key since by assumption, the round key, which is used within one round, consists of independent and uniformly random bits, and is bitwise XORed with data. The *S*-function is a non-linear transformation layer with m parallel d-bit bijective S-boxes whereas the *P*-function is a linear transformation layer. In particular, we have

$$S:\left(GF(2^d)^m\right)\to\left(GF(2^d)^m\right),\ X=(x_1,\cdots,x_m)$$
$$\mapsto Z=S(X)=\left(s_1(x_1),\cdots,s_m(x_m)\right),$$

$$P:\left(GF(2^d)^m\right)\to\left(GF(2^d)^m\right),\ Z=(z_1,\cdots,z_m)$$
$$\mapsto Y=P(Z)=(y_1,\cdots,y_m),$$

$$F:\left(GF(2^d)^m\right)\to\left(GF(2^d)^m\right),\ X\mapsto Y$$
$$=F(X)=P\left(S(X)\right).$$

Definition 1: 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:

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

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

Definition 2: The maximum differential and linear probabilities of S-boxes are defined as:

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

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

This means that p_s, q_s are the upper bounds of the maximum differential and linear probabilities for all S-boxes.

Definition 3: Let $X = (x_1, x_2, \cdots, x_m) \in GF(2^d)^m$. Then the Hamming weight of X is denoted by $H_w(X) = \#\{i \mid x_i \neq 0\}$.

Definition 4 (Rijmen et al., 1996): The branch number $\mathcal{B}$ of linear transformation θ is defined as follows:

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

Consider Feistel ciphers with bijective SPN round functions as described previously. As mentioned in Kanda (2001), for the differential case, $\mathcal{B}$ is taken to be the *differential* branch number, i.e., $\mathcal{B}=\min_{\Delta X\neq 0}(H_w(\Delta X)+H_w(\Delta Y))$, where ΔX is an input difference into the *S*-function and ΔY is an output difference of the *P*-function. On the other hand, for the linear case, $\mathcal{B}$ is taken to be the linear branch number, i.e., $\mathcal{B}=\min_{\Gamma Y\neq 0}(H_w(P^*(\Gamma Y))+H_w(\Gamma Y))$, where ΓY is an output mask value of the *P*-function and P^* is a diffusion function of mask values concerning the *P*-function. Throughout this paper, $\mathcal{B}$ is used to denote differential or linear branch number, depending on the context.

Definition 5: 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 1: Let $\mathcal{D}^{(r)}$ and $\mathcal{L}^{(r)}$ be the minimum number of all differential and linear active S-boxes for a 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 $p_s^{L^{(r)}}$, respectively.

Note that Theorem 1 applies to any block cipher in general.

Theorem 2 (Kanda, 2001): 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 $r\mathcal{B} + \lfloor \frac{r}{2} \rfloor$.

3 Practical security evaluation of GF-NLFSR against differential and linear cryptanalysis

GF-NLFSR was proposed by Choy et al. (2009a). It is an n-cell extension of the outer function *FO* of the KASUMI block cipher which is a 2-cell structure.

Throughout this paper, we consider GF-NLFSR block ciphers with SPN (S-P) round function, as described in Section 1.2. In this paper, we assume that both the *S*-function and *P*-function are bijective.

With reference to Figure 1, let $X^{(i)}$ and $Y^{(i)}$ be the input and output data to the i^{th} round function respectively. Then the GF-NLFSR block cipher can be defined as

$$X^{(i+n)} = Y^{(i)} \oplus X^{(i+1)} \oplus X^{(i+2)} \oplus \cdots \oplus X^{(i+n-1)}, \quad \text{for } i = 1, 2, \cdots, \tag{1}$$

3.1 Differential cryptanalysis

We now investigate the minimum number of differential active S-boxes for GF-NLFSR block cipher. From equation (1), it can be shown almost immediately that there must be at least two differential active S-boxes over $(n + 1)$-round of n-cell GF-NLFSR cipher.

Proposition 1: The minimum number of differential active S-boxes for $(n + 1)$-round n-cell GF-NLFSR cipher with bijective SPN round function satisfies $\mathcal{D}^{(n+1)} \geq 2$.

Proof: Without loss of generality, we assume that the $n + 1$ consecutive rounds run from the first round to the $(n + 1)^{\text{th}}$ round. Since the SPN round function is bijective, $\Delta Y(1) = 0$ if and only if $\Delta X(1) = 0$. From equation (1), we have

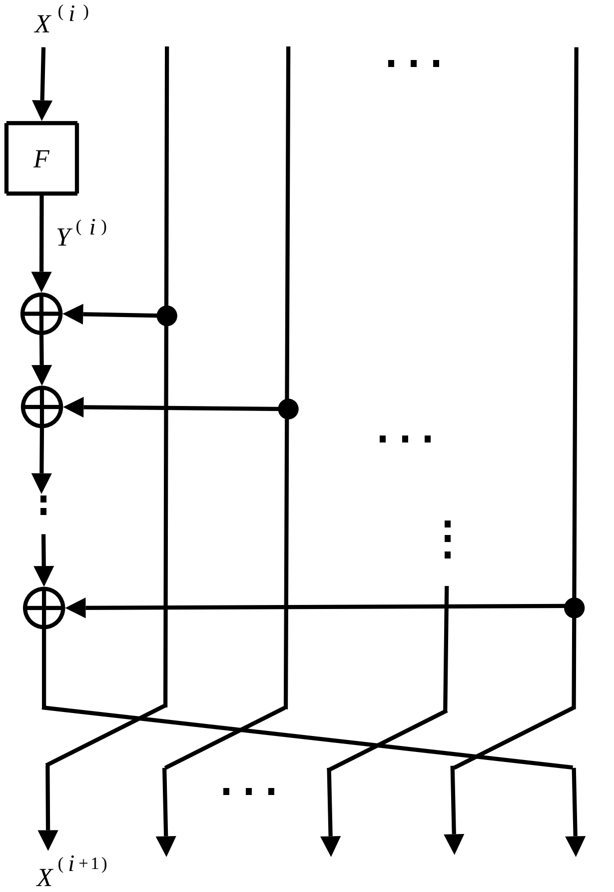
$$\Delta X^{(n+1)} = \Delta Y^{(1)} \oplus \Delta X^{(2)} \oplus \Delta X^{(3)} \oplus \cdots \oplus \Delta X^{(n)}, \tag{2}$$

from which it follows that there must exist at least two non-zero terms in equation (2) in order for equation (2) to hold. Therefore,

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

□

Figure 1 i^{th} round of GF-NLFSR



Lemma 1: Let $X = (x_1, x_2, \cdots, x_m)$ and $X' = (x_1', x_2', \cdots, x_m') \in GF(2^d)^m$. Then

$$H_w(X \oplus X') \leq H_w(X) + H_w(X')$$

Proof:

$$\begin{aligned} & H_w(X \oplus X') \\ & = \#\{s \mid x_s \neq 0 \text{ and } x_s' = 0\} + \#\{t \mid x_t = 0 \text{ and } x_t' \neq 0\} \\ & + \#\{u \mid x_u \neq 0 \text{ and } x_u' \neq 0 \text{ and } x_u \neq x_u'\} \\ & \leq H_w(X) + \#\{t \mid x_t = 0 \text{ and } x_t' \neq 0\} \\ & \leq H_w(X) + H_w(X') \end{aligned}$$

□

Lemma 2 is a straightforward generalisation of Lemma 1.

Lemma 2: Let $X_1, X_2, \cdots, X_k \in GF(2^d)^m$. Then

$$H_w(X_1 \oplus X_2 \oplus \cdots \oplus X_k) \leq H_w(X_1) + H_w(X_2) + \cdots + H_w(X_k).$$

As stated in Theorem 1, to investigate the upper bound of the maximum differential characteristic probability of the GF-NLFSR cipher, we need to find a lower bound for $\mathcal{D}^{(r)}$, the number of differential active S-boxes for r consecutive rounds of the cipher. Then the differential characteristic probability of the r-round GF-NLFSR cipher is at most $p_s^{\mathcal{D}^{(r)}}$.

Lemma 3: For n-cell GF-NLFSR cipher, the minimum number of differential active S-boxes in any $2n$ consecutive rounds satisfies $\mathcal{D}^{(2n)} \geq \mathcal{B}$.

Proof: Without loss of generality, we assume that the $2n$ consecutive rounds run from the first round to the $2n^{\text{th}}$ round. For $j = 1, \cdots, n$, note that 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

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

□

Remark 1: From the above proof, we see that with probability $1 - \frac{1}{M}$, where M is the size of each cell, i.e., most of the time, we have $\Delta X^{(1)} \neq 0$. In that case, we are able to achieve at least $\mathcal{B}$ number of differential active S-boxes over $(n + 1)$ rounds of n-cell GF-NLFSR cipher.

As a consequence of Lemma 3 and using a similar approach as Kanda (2001), we have the following result.

Theorem 3: The minimum number of differential active S-boxes for $2nr$-round n-cell GF-NLFSR cipher with bijective SPN round function satisfies

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

In particular, when $n = 2$, the minimum number of differential active S-boxes for $4r$-round 2-cell GF-NLFSR cipher with bijective SPN round function is at least $r\mathcal{B} + \left\lfloor \frac{r}{2} \right\rfloor$. Hence, we see that 2-cell GF-NLFSR cipher with bijective SPN round function has similar practical security against differential cryptanalysis as Feistel ciphers with bijective SPN round functions. Moreover, 2-cell GF-NLFSR has an added advantage that it realises parallel computation of round functions, thus providing strong motivation for parallelising ciphers with SPN round functions, as described in Section 4.

3.2 Linear cryptanalysis

For the purpose of parallelising Camellia and SMS4, we shall investigate the practical security of 2-cell and 4-cell GF-NLFSR cipher against linear cryptanalysis. Again from Theorem 1, to investigate the upper bound of the maximum linear characteristic probability of the GF-NLFSR cipher, we need to find a lower bound for $\mathcal{L}^{(r)}$, the number of linear active S-boxes for r consecutive rounds of the cipher. Then the linear characteristic probability of the r-round cipher is at most $q_s^{\mathcal{L}^{(r)}}$. We first consider the 2-cell GF-NLFSR cipher, followed by the 4-cell GF-NLFSR cipher.

3.2.1 Duality between differential characteristic and linear approximation

As discussed in Section 3 of Matsui (1995), when analysing mask values in linear cryptanalysis, we need to consider the duality between differential characteristic and linear approximation, where each XOR is replaced by a joint and each joint is replaced by an XOR. Hence, in the case of 2-cell GF-NLFSR cipher, with reference to Figure 2, we have

$$\Gamma X^{(i+2)} = \Gamma Y^{(i)} \oplus \Gamma Y^{(i+1)}, \text{ for } i \geq 1, \tag{3}$$

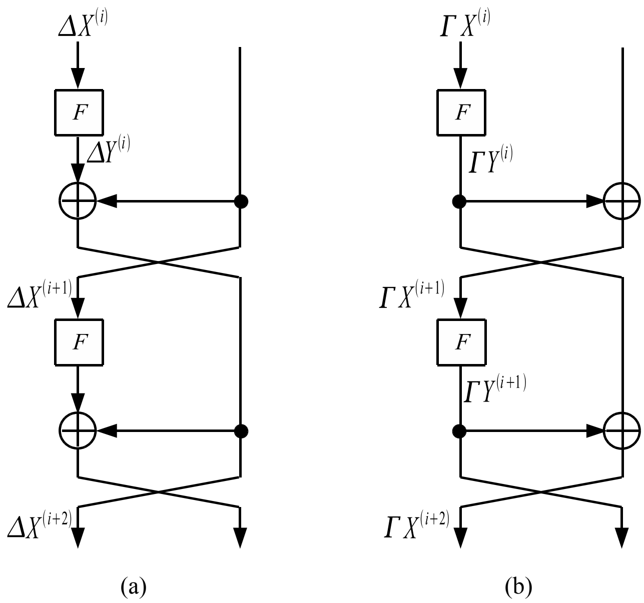
where the input and output mask values to the i^{th} round F function are denoted by $\Gamma X^{(i)}$ and $\Gamma Y^{(i)}$, respectively.

Similarly, for 4-cell GF-NLFSR cipher, with reference to Figure 5, we have

$$\Gamma X^{(i+4)} = \Gamma Y^{(i)} \oplus \Gamma Y^{(i+1)} \oplus \Gamma Y^{(i+2)} \oplus \Gamma Y^{(i+3)}. \tag{4}$$

Lemma 4: 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 four consecutive rounds satisfies $\mathcal{L}^{(4)} \geq 3$.

Figure 2 (a) 2-cell GF-NLFSR cipher, (b) dual of 2-cell GF-NLFSR cipher



Proof: Let the input and output mask values to the i^{th} round F function be $\Gamma X^{(i)}$ and $\Gamma Y^{(i)}$, respectively. Note that since the F function is bijective, $\Gamma X^{(i)} = 0$ if and only if $\Gamma Y^{(i)} = 0$. Without loss of generality, we assume that the four consecutive rounds run from the first round to the fourth round. Thus, the minimum number of linear active S-boxes over four consecutive rounds is given by

$$\mathcal{L}^{(4)} = H_w(\Gamma Y^{(1)}) + H_w(\Gamma Y^{(2)}) + H_w(\Gamma Y^{(3)}) + H_w(\Gamma Y^{(4)}).$$

As discussed in the previous section, we have, from equation (3),

$$\Gamma X^{(i+1)} = \Gamma Y^{(i-1)} \oplus \Gamma Y^{(i)},$$

for i = 2 and 3. We consider all cases as follows, where $\mathcal{L}_i^{(r)}$ denotes the number of linear active S-boxes over r rounds for case i:

Case 1 $\Gamma X^{(1)} = 0$

This implies that $\Gamma X^{(2)} \neq 0$ and $\Gamma X^{(3)} = \Gamma Y^{(2)}$. Hence, $\mathcal{L}_1^{(3)} \geq H_w(\Gamma X^{(2)}) + H_w(\Gamma X^{(3)}) = H_w(\Gamma X^{(2)}) + H_w(\Gamma Y^{(2)}) \geq \mathcal{B} = 5 \geq 3.$ Thus, $\mathcal{L}_1^{(4)} \geq \mathcal{L}_1^{(3)} \geq 3.$

Case 2 $\Gamma X^{(1)} \neq 0$ and $\Gamma X^{(2)} = 0$

This implies that $\Gamma X^{(3)} = \Gamma Y^{(1)}$. Hence, $\mathcal{L}_2^{(3)} \geq H_w(\Gamma X^{(1)}) + H_w(\Gamma X^{(3)}) + H_w(\Gamma X^{(1)}) + H_w(\Gamma Y^{(1)}) \geq \mathcal{B} = 5 \geq 3.$ Thus, $\mathcal{L}_2^{(4)} \geq \mathcal{L}_2^{(3)} \geq 3.$

Case 3 $\Gamma X^{(1)} \neq 0$, $\Gamma X^{(2)} \neq 0$ and $\Gamma X^{(3)} = 0$

This implies that $\Gamma X^{(4)} = \Gamma Y^{(2)}$. Hence, $\mathcal{L}_2^{(4)} \geq H_w(\Gamma X^{(1)}) + H_w(\Gamma X^{(2)}) + H_w(\Gamma X^{(4)}) = H_w(\Gamma X^{(1)}) + H_w(\Gamma X^{(2)}) + H_w(\Gamma Y^{(2)}) \geq 1 + \mathcal{B} = 6 \geq 3.$

Case 4 $\Gamma X^{(1)} \neq 0$, $\Gamma X^{(2)} \neq 0$, $\Gamma X^{(3)} \neq 0$ and $\Gamma X^{(4)} = 0$

Then we obtain $\mathcal{L}_4^{(4)} \geq H_w(\Gamma X^{(1)}) + H_w(\Gamma X^{(2)}) + H_w(\Gamma X^{(3)}) \geq 1 + 1 + 1 = 3.$

Case 5 $\Gamma X^{(1)} \neq 0$, $\Gamma X^{(2)} \neq 0$, $\Gamma X^{(2)} \neq 0$ and $\Gamma X^{(4)} \neq 0$

Then we obtain $\mathcal{L}_5^{(4)} = H_w(\Gamma X^{(1)}) + H_w(\Gamma X^{(2)}) + H_w(\Gamma X^{(3)}) + H_w(\Gamma X^{(3)}) \geq 1 + 1 + 1 + 1 = 4 \geq 3.$

Therefore, $\mathcal{L}^{(4)} \geq 3$. □

Theorem 4: 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 $\mathcal{L}^{(16)} \geq 15.$

Proof: Without loss of generality, we begin from the first round.

1 From the proof of Lemma 4, over 8 rounds, we only need to check the case for $\Gamma X^{(1)} \neq 0$, $\Gamma X^{(2)} \neq 0$, $\Gamma X^{(3)} \neq 0$ and $\Gamma X^{(4)} = 0$. (In all remaining cases, there will be at least 7 linear active S-boxes over 8 rounds.) However, $\Gamma X^{(3)} \neq 0$ and $\Gamma X^{(4)} = 0$ correspond to Case 1 of Lemma 4 for the four consecutive rounds that begin from the 4th round and end after the 7th round. Hence, there will be at least 3 + 5 = 8 linear active S-boxes. Therefore, $\mathcal{L}^{(8)} \geq 7$.

2 From (i), over 12 rounds, we only need to consider the case for $\Gamma X^{(i)} \neq 0$ for i = 1, ···, 7 and $\Gamma X^{(8)} = 0$. Following a similar argument to (i), we are definitely ensured of at least 7 + 5 = 12 linear active S-boxes. Hence, $\mathcal{L}^{(12)} \geq 11$.

3 The proof is similar to that of (i) and (ii).

We conclude this section with the study of minimum number of active S-boxes for 4-cell GF-NLFSR.

Proposition 1: Assume that the linear branch number $\mathcal{B} = 5$. Then the minimum number of linear active S-boxes for 5-round 4-cell GF-NLFSR cipher with bijective SPN round function satisfies $\mathcal{L}^{(5)} \geq 2$.

Proof: Let $\Gamma X^{(i)}$ and $\Gamma Y^{(i)}$ be the input and output mask to the i^{th} round function respectively. Since the round function is bijective, $\Gamma X^{(i)} = 0$ if and only if $\Gamma Y^{(i)} = 0$. It is evident from equation (4) that there cannot exist exactly one non-zero input mask for five consecutive rounds. The result now follows easily. □

Theorem 5: Assume that the linear branch number $\mathcal{B} = 5$. Then the minimum number of linear active S-boxes for 10-round 4-cell GF-NLFSR cipher with bijective SPN round function satisfies $\mathcal{L}^{(10)} \geq \mathcal{B} + 1$.

Proof: With no loss of generality, assume that the 10 rounds run consecutively from the first round to the tenth round. Let $\Gamma X^{(i)}$ and $\Gamma Y^{(i)}$ be the input and output mask to the i^{th} round function respectively. Recall that due to the duality between differential characteristic and linear approximation, equation (4) holds. Let $\mathcal{M} = \{\Gamma X^{(1)}, \Gamma X^{(2)}, \Gamma X^{(3)}, \Gamma X^{(4)}\}$. We consider all the following cases, where $\mathcal{L}_j^{(r)}$ denotes the number of linear active S-boxes for r rounds for case j.

Case 1 There is exactly one non-zero input mask in set $\mathcal{M}$, i.e., $\Gamma X^{(i)} \neq 0$ for some i = 1, 2, 3 or 4. Then $\Gamma X^{(5)} = \Gamma Y^{(i)} \neq 0$. Since for four consecutive rounds, the input masks cannot be zero at the same time, we obtain

$$\begin{aligned}\mathcal{L}_1^{(9)} &= H_w(\Gamma X^{(i)}) + H_w(\Gamma X^{(5)}) \\ &\quad + H_w(\Gamma X^{(6)}) + \cdots + H_w(\Gamma X^{(9)}) \\ &\geq H_w(\Gamma X^{(i)}) + H_w(\Gamma Y^{(i)}) + 1 \\ &\geq \mathcal{B} + 1.\end{aligned}$$

Case 2 All input masks in $\mathcal{M}$ are non-zero.

By Proposition 1, we obtain

$$\begin{aligned}\mathcal{L}_2^{(9)} &= H_w(\Gamma X^{(1)}) + \cdots + H_w(\Gamma X^{(4)}) + H_w(\Gamma X^{(5)}) \\ &\quad + \cdots + H_w(\Gamma X^{(9)}) \\ &\geq 4 + 2 \\ &= 6 \\ &\geq \mathcal{B} + 1.\end{aligned}$$

Case 3 There are exactly three non-zero input masks in $\mathcal{M}$.

Let $\mathcal{S} = \{\Gamma X^{(5)}, \Gamma X^{(6)}, \Gamma X^{(7)}, \Gamma X^{(8)}\}$. If there are at least three non-zero input masks in $\mathcal{S}$, then we are done. Also, since the input masks for four consecutive rounds cannot be zero at the same time, at least one input mask in $\mathcal{S}$ is non-zero. This implies that we only need to check the following:

1 There is exactly one non-zero input difference in $\mathcal{S}$.

Then $\Gamma X^{(9)} = \Gamma Y^{(j)}$ for j = 5, 6, 7 or 8. Hence

$$\mathcal{L}_3^{(9)} \geq 3 + H_w(\Gamma X^{(j)}) + H_w(\Gamma X^{(9)}) \geq \mathcal{B} + 3.$$

2 There are exactly two non-zero input masks in $\mathcal{S}$.

- Suppose $\Gamma X^{(5)} = 0$ and $\Gamma X^{(6)} \neq 0$. Then $\Gamma Y^{(1)} \oplus \Gamma Y^{(2)} \oplus \Gamma Y^{(3)} \oplus \Gamma Y^{(4)} = 0$ and it follows that $\Gamma X^{(6)} = \Gamma Y^{(1)} \neq 0$. Hence, we are ensured of at least $\mathcal{B}+2$ active S-boxes.
- Suppose $\Gamma X^{(6)} = 0$ and $\Gamma X^{(7)} \neq 0$. Then $\Gamma Y^{(2)} \oplus \Gamma Y^{(3)} \oplus \Gamma Y^{(4)} \oplus \Gamma Y^{(5)} = 0$ and it follows that $\Gamma X^{(7)} = \Gamma Y^{(2)} \neq 0$. Hence, we are ensured of at least $\mathcal{B}+2$ active S-boxes.
- Suppose $\Gamma X^{(6)} = \Gamma X^{(7)} = 0$, $\Gamma X^{(5)} \neq 0$ and $\Gamma X^{(8)} \neq 0$. Then it can be deduced easily that $\Gamma X^{(8)} = \Gamma Y^{(3)} \neq 0$, and there must be at least $\mathcal{B}+2$ active S-boxes.
- Suppose $\Gamma X^{(7)} = \Gamma X^{(8)} = 0$, $\Gamma X^{(5)} \neq 0$ and $\Gamma X^{(6)} \neq 0$. It follows directly that $\Gamma X^{(9)} = \Gamma Y^{(4)}$. If $\Gamma X^{(9)} \neq 0$, then we are done. Otherwise $\Gamma X^{(4)} = 0$ which implies that $\Gamma X^{(3)} \neq 0$. However, $0 = \Gamma X^{(8)} = \Gamma Y^{(3)} \neq 0$, which is a contradiction.

Case 4 There are exactly two non-zero input masks in $\mathcal{M}$.

1 Suppose $\Gamma X^{(5)} = 0$. Then $\Gamma X^{(6)} = \Gamma Y^{(1)}$.

- If $\Gamma X^{(1)} \neq 0$, then $\mathcal{L}_4^{(6)} \geq H_w(\Gamma X^{(1)}) + H_w(\Gamma Y^{(1)}) + 1 \geq \mathcal{B} + 1$.
- If $\Gamma X^{(1)} = 0$ and $\Gamma X^{(2)} \neq 0$, then $\Gamma X^{(7)} = \Gamma Y^{(2)}$ and so we obtain,

$$\mathcal{L}_4^{(7)} \geq H_w(\Gamma X^{(2)}) + H_w(\Gamma Y^{(2)}) + 1 \geq \mathcal{B} + 1.$$

- If $\Gamma X^{(1)} = 0$ and $\Gamma X^{(2)} = 0$, then $\Gamma X^{(3)} \neq 0$ and $\Gamma X^{(4)} \neq 0$. Hence, $\Gamma X^{(8)} = \Gamma Y^{(3)}$, from which

$$\mathcal{L}_4^{(8)} \geq H_w(\Gamma X^{(3)}) + H_w(\Gamma X^{(4)}) + H_w(\Gamma X^{(8)}) \geq \mathcal{B} + 1,$$

follows.

2 Suppose $\Gamma X^{(5)} \neq 0$ and $\Gamma X^{(6)} = 0$. It follows that $\Gamma X^{(7)} = \Gamma Y^{(2)}$.

- If $\Gamma X^{(2)} \neq 0$, then $\mathcal{L}_4^{(7)} \geq H_w(\Gamma X^{(2)}) + H_w(\Gamma Y^{(2)}) + 1 \geq \mathcal{B} + 1$.
- If $\Gamma X^{(2)} = 0$ and $\Gamma X^{(3)} \neq 0$, then $\Gamma X^{(8)} = \Gamma Y^{(3)}$. This implies that

$$\mathcal{L}_4^{(8)} \geq H_w(\Gamma X^{(3)}) + H_w(\Gamma Y^{(3)}) + 1 \geq \mathcal{B} + 1.$$

- If $\Gamma X^{(2)} = 0$ and $\Gamma X^{(3)} = 0$, then $\Gamma X^{(1)} \neq 0$ and $\Gamma X^{(4)} \neq 0$. This implies that $\Gamma X^{(9)} = \Gamma Y^{(4)}$, and so

$$\mathcal{L}_4^{(9)} \geq H_w(\Gamma X^{(4)}) + H_w(\Gamma X^{(9)}) + H_w(\Gamma X^{(1)}) \geq \mathcal{B} + 1.$$

3 Suppose $\Gamma X^{(5)} \neq 0$, $\Gamma X^{(6)} \neq 0$ and $\Gamma X^{(7)} = 0$. Then $\Gamma X^{(8)} = \Gamma Y^{(3)}$.

- If $\Gamma X^{(3)} \neq 0$, then $\mathcal{L}_4^{(8)} \geq H_w(\Gamma X^{(3)}) + H_w(\Gamma Y^{(3)}) + 1 \geq \mathcal{B} + 1$.
- If $\Gamma X^{(3)} = 0$ and $\Gamma X^{(4)} \neq 0$, then $\Gamma X^{(9)} = \Gamma Y^{(4)}$. This implies that

$$\mathcal{L}_4^{(9)} \geq H_w(\Gamma X^{(4)}) + H_w(\Gamma Y^{(4)}) + 1 \geq \mathcal{B} + 1.$$

- If $\Gamma X^{(3)} = 0$ and $\Gamma X^{(4)} = 0$, then $\Gamma X^{(1)} \neq 0$ and $\Gamma X^{(2)} \neq 0$. This implies that $\Gamma X^{(10)} = \Gamma Y^{(5)} \neq 0$. So

$$\mathcal{L}_4^{(10)} \geq H_w(\Gamma X^{(5)}) + H_w(\Gamma X^{(10)}) + H_w(\Gamma X^{(1)}) + H_w(\Gamma X^{(2)}) + H_w(\Gamma X^{(6)}) \geq \mathcal{B} + 3.$$

4 Suppose $\Gamma X^{(5)} \neq 0$, $\Gamma X^{(6)} \neq 0$ and $\Gamma X^{(7)} \neq 0$. If $\Gamma X^{(8)} \neq 0$ or $\Gamma X^{(9)} \neq 0$, then there will be at least 6 linear active S-boxes and we are done. Otherwise $\Gamma X^{(8)} = \Gamma X^{(9)} = 0$ and $\Gamma X^{(10)} = \Gamma Y^{(5)} \neq 0$ and we obtain

$$\mathcal{L}_4^{(10)} \geq H_w(\Gamma X^{(5)}) + H_w(\Gamma X^{(10)}) + H_w(\Gamma X^{(6)}) + H_w(\Gamma X^{(7)}) \geq \mathcal{B} + 2.$$

Hence considering all cases, we conclude that $\mathcal{L}^{(10)} \geq \mathcal{B} + 1$. □

Corollary 1: The minimum number of linear active S-boxes for 9-round 4-cell GF-NLFSR cipher with bijective SPN round function satisfies $\mathcal{L}^{(9)} \geq 4$.

Proof: The result follows easily from the proof of Theorem 5. □

4 Application 1: parallelising Camellia

4.1 Brief description of Camellia

Camellia was jointly developed by NTT and Mitsubishi Electric Corporation. According to Aoki et al. (2001), Camellia uses an 18-round Feistel structure for 128-bit key, and a 24-round Feistel structure for 192-bit and 256-bit keys, with additional input/output whitenings and logical functions called the *FL*-function and FL^{-1}-function inserted every 6 rounds. Its *F*-function uses the substitution-permutation network (SPN) structure, whereby the non-linear layer comprises eight S-boxes in parallel while the linear layer can be represented using only byte-wise exclusive-ORs. Note that the *F*-function is bijective.

For security against differential and linear cryptanalysis, the branch number of the linear layer should be optimal, i.e., branch number = 5. In addition, the S-boxes adopt functions which are affine equivalent to the inversion function in $GF(2^8)$ which achieves the best known of the maximum differential and linear probabilities 2^{-6} (Aoki et al., 2001).

The key schedule of Camellia is slightly different for the 128-bit key version and the 192-bit/256-bit key version. Despite the slight differences, the key schedule is relatively simple and consists of two main steps. One (or two) 128-bit subkey materials are first derived from the secret key via some Feistel network. The round keys are then generated by rotating the secret key itself and the derived subkeys by various amounts.

For more details of the structure of Camellia, readers are referred to Aoki et al. (2000).

4.2 Parallelising Camellia: p-Camellia

In this section, we propose another version of the existing Camellia block cipher, which we call p-Camellia (*'parallelisable' Camellia*). As described previously, Camellia uses a Feistel network structure. For the encryption procedure of p-Camellia, we shall replace the Feistel network with the 2-cell GF-NLFSR block cipher structure instead, as depicted in Figure 6 of Appendix. Other components such as number of rounds, S-function, P-function and the key schedule for the different key versions, etc. remain unchanged. In addition, similar to Camellia, there are input/output whitenings which are represented by the XOR symbols at the beginning/end of p-Camellia cipher in Figure 6.

4.3 Differential and linear cryptanalysis of p-Camellia

Following the same approach in Aoki et al. (2000), denote the maximum differential and linear characteristic probabilities of p-Camellia reduced to 16-round by p and q respectively. Recall that since both p-Camellia and Camellia use the same F-function, in the case of p-Camellia, the maximum differential and linear probability of the S-boxes are 2^{-6}. From Aoki et al. (2000), the differential branch numbers is equal to 5. By considering the P^*-function of Camellia as in Kanda (2001), the linear branch number is verified to be 5.

Over 16 rounds, there are four 4-round blocks. By virtue of Theorem 3, where n = 2 and r = 4, we have

$$p \le (2^{-6})^{4\times 5+2} = 2^{-132} < 2^{-128}.$$

By Theorem 4, we obtain $q \le (2^{-6})^{15} = 2^{-90}$. This implies that an attacker needs to collect at least 2^{90} chosen/known plaintexts to mount an attack, which is not feasible in practice.

This implies that there is no effective differential or linear characteristic for p-Camellia reduced to more than 15 rounds. In other words, p-Camellia offers sufficient security against differential and linear attack.

4.4 Other attacks on p-Camellia

In this section, we briefly examine the protection of p-Camellia against various known attacks. Since p-Camellia uses the same components as Camellia, we expect that p-Camellia offers similar level of protection against most of the attacks, as compared to Camellia.

4.4.1 Boomerang attack

To perform a boomerang attack, the cipher is split into two shorter ciphers E_0 and E_1 such that the differential probability of each part is known to be large. Suppose an adversary split 16 rounds into E_0 and E_1 with r and $16 - r$ rounds, respectively. By Theorem 3, the characteristic differential probability of each sub-ciphers would be bounded by $p_0 \le (2^{-30})^{\lfloor r/4 \rfloor}$ and $p_1 \le (2^{-30})^{\lfloor (16-r)/4 \rfloor}$. (Note that we ignore the last term in the upper bound of Theorem 3 for ease of calculation.) It can be easily verified that $\lfloor r/4 \rfloor + \lfloor (16-r)/4 \rfloor \ge 3$ for $r = 1, \ldots, 15$. Consequently,

$$p_0^2 \times p_1^2 \le 2^{-60\times 3} = 2^{-180} < 2^{-128},$$

and thus p-Camellia is secure against boomerang attack.

4.4.2 Impossible differential attack

Impossible differential attack is a chosen plaintext attack and is an extension of differential cryptanalysis. The main idea of this attack is to construct an impossible differential characteristic which is then used to filter wrong key guesses. Employing similar techniques as Wei et al. (2010), we can prove the following result.

Proposition 2: Let e_1 denote a subblock which is non-zero in the first byte position and zero in the remaining byte positions. For 2-cell GF-NLFSR cipher with bijective SPN round function and differential branch number $\mathcal{B} \ge 3$, there is at least one 5-round impossible differential, namely of the form $(e_1, 0) \not\to_5 (\beta, \beta)$, where β is a non-zero fixed difference.

(Note that here we only consider $\mathcal{B} \ge 3$ since linear transformation layers with $\mathcal{B} = 2$ are unlikely to be used as they do not aid in the protection of the cipher against differential attack.)

Proof: Suppose for a contradiction that $(e_1, 0) \to_5 (\beta, \beta)$ is possible. In the direction of encryption, after 3 rounds, we have $(e_1, 0) \to (PS(e_1), PS(e_1) \oplus PSPS(e_1))$. On the other hand, decrypting two rounds, we obtain $(S^{-1}P^{-1}(\beta), 0) \leftarrow (\beta, \beta)$. Hence,

$$
\begin{aligned}
&PS(e_1) \otimes PSPS(e_1) = 0, \\
&P\big(S(e_1) \oplus SPS(e_1)\big) = 0, \qquad (5) \\
&S(e_1) \oplus SPS(e_1) = 0.
\end{aligned}
$$

However,

$$H_w\big(SPS(e_1) \oplus S(e_1)\big) \geq (\mathcal{B} - 1) - 1 = \mathcal{B} - 2 \geq 3 - 2 = 1,$$

which is a contradiction with equation (5). □

Since for p-Camellia, $\mathcal{B} = 5$, by Proposition 2, there is at least a 5-round impossible differential in p-Camellia. We have not found impossible differentials with more than 5 rounds. As explained in Aoki et al. (2001), we expect that the presence of the *FL*- and FL^{-1} functions will greatly increase the difficulty of performing impossible differential attack on p-Camellia since the functions change the differential paths depending on key values.

4.4.3 *Integral attack*

In an integral attack, the attacker studies the propagation of multisets of chosen plaintexts of which part is held constant, and another part varies through all possibilities (also said to be *active*) through the cipher. There is a 4-round integral distinguisher of 2-cell GF-NLFSR (Choy et al., 2009a), namely $(A, C) \rightarrow (S_0, S_1)$, where C is constant, A is active and $S_0 \oplus S_1$ is active. We have not found integral distinguishers with more than 4 rounds. An adversary can extend an integral attack distingusher by at most three rounds. That means he would need to extend the integral attack distinguisher from 4 to 18 – 3 = 15 rounds which seems unlikely.

4.4.4 *Slide attack*

The slide attack works on ciphers with cyclical structures over a few rounds. According to Aoki et al. (2001), the *FL*- and FL^{-1}-functions are inserted between every 6 rounds to provide non-regularity across rounds. In addition, different subkeys are used for every round, making slide attack unlikely.

We now proceed to examine the protection of p-Camellia against higher order differential attack and interpolation attack. We will adopt a similar approach as Aoki et al. (2001), which is somewhat heuristic but adequate for us to have a comprehensive and insightful discussion.

4.4.5 *Higher order differential attack*

Higher order differential attack was introduced by Knudsen (1995). This attack works especially well on block ciphers with components of low algebraic degree such as the KN-cipher (Jakobsen and Knudsen, 1997), whereby the ciphers can be represented as Boolean polynomials of low degree in terms of the plaintext. The attack requires $O(2^{t+1})$ chosen plaintext when the cipher has degree t.

p-Camellia uses exactly the same S-boxes as Camellia and it was confirmed in Aoki et al. (2001) that the degree of the Boolean polynomial of every output bit of the S-boxes is 7 by finding Boolean polynomial for every outpit bit of the S-boxes. Hence, similar to Camellia, the degree of an intermediate bit in the encryption process should increase as the data passes through many S-boxes. Indeed, let (α_i, β_i) be the input to the $(i + 1)^{\text{th}}$ round of p-Camellia. Suppose $\deg(\alpha_0) = \deg(\beta_0) = 1$. After the first round, $\deg(\alpha_1) = \deg(\beta_0) = 1$ while $\deg(\alpha_1) = \deg(F(\alpha_0) \oplus \beta_0) = 7$. Continuing this process, we see that the degrees of α_i and β_i for $i = 0, 1, 2, \cdots$, increases as follows: (1, 1), (1, 7), (7, 7), (7, 49), (49, 49), (49, 127), (127, 127), ⋯.

That is, the degrees increase exponentially as the number of rounds increase and reach the maximum degree of 127 after the 6th round, implying that it is highly unlikely that higher order differential attack will work.

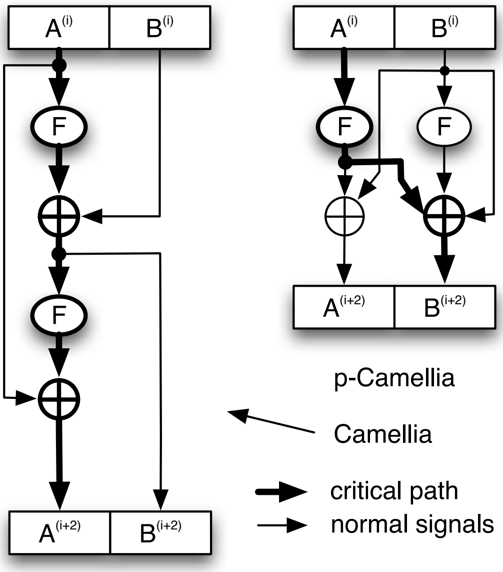
4.4.6 *Interpolation attack*

The interpolation attack (Jakobsen and Knudsen, 2001) works on block ciphers that can be expressed as an equation in $GF(2^d)$ with few monomials. p-Camellia uses the same components as Camellia and it was shown in Aoki et al. (2001) that as the data passes through many S-boxes and the P-function, the cipher became a complex function which is a sum of many multivariate monomials over $GF(2^8)$. Hence, we also expect p-Camellia to be secure against interpolation attack.

4.5 *Implementation advantages*

Before we discuss the implementation advantages of p-Camellia we briefly introduce hardware implementation strategies for block ciphers that consist of a round-function that is iterated several times. While software implementations have to process single operations in a serial manner, hardware implementations offer more flexibility for parallelisation. Generally speaking, there exist three major architecture strategies for the implementation of block ciphers: *serialised*, *round-based*, and *parallelised*. In a *serialised* architecture, only a fraction of a single round is processed in one clock cycle. These lightweight implementations allow reduction in area and power consumption at the cost of a rather long processing time. If a complete round is performed in one clock cycle, we have a *round-based* architecture. This implementation strategy usually offers the best time-area product and throughput per area ratio. A *parallelised* architecture processes more than one round per clock cycle, leading to a rather long critical path. A longer critical path leads to a lower maximum frequency but also requires the gates to drive a higher load (fanout), which results in larger gates with a higher power consumption. By inserting intermediate registers (a technique called *pipelining*), it is possible to split the critical path into fractions, thus increasing the maximum frequency. Once the pipeline is filled, a complete encryption can be performed in one clock cycle with such an architecture. Consequently, this implementation strategy yields the highest throughput at the cost of high area demands. Furthermore, since the pipeline has to be filled, each pipelining stage introduces a delay of one clock cycle.

Figure 3 Possible hardware architecture of two rounds of (a) Camellia and (b) p-Camellia



(a) (b)

From a lightweight perspective, i.e., if we consider serialised architectures, it is no wonder that area, power and timing demands stay the same for Camellia and p-Camellia, since no operation was introduced or removed. Also, a round-based p-Camellia implementation is as efficient as a round-based Camellia implementation. However, if we consider applications that require high throughput, p-Camellia has significant advantages. If we consider an architecture that implements two rounds in one clock cycle (see Figure 3), Camellia's critical path involves two *F*-functions and two 2-input XOR gates, compared to only one *F*-function and one 3-input XOR gate for p-Camellia. Since Camellia inserts every six rounds the FL and FL^{-1} functions, it is advantageous to parallelise this fraction of Camellia/p-Camellia. In this case, the critical path of Camellia consists of six F-functions, six 2-input XOR gates and the delay of FL/FL^{-1} while p-Camellia's critical path only consists of three *F*-functions, three 3-input XOR gates, and the delay of FL/FL^{-1}. Given the fact that the *F*-function consists of a 2-input XOR gate (key addition), several combinatorial gates (S-box) and an extensive XOR network (P-function), the delay difference between a 2-input and a 3-input XOR gate is negligible. Hence, p-Camellia can achieve a maximum frequency that is nearly twice as high as it would be for Camellia while having similar or lower area and power demands. In case pipelining is applied, Camellia requires twice as much pipelining stages as p-Camellia to achieve the same maximum frequency, resulting in a delay that is twice as high.

To substantiate our claims, we have implemented the round function of Camellia and p-Camellia each with a 128-bit key in VHDL. We obtained area, timing and power figures for a 180 nm ASIC technology from UMC using Synopsys Design Vision for synthesis. Table 1 depicts a comparison of the hardware implementation results of the round function of Camellia and p-Camellia. This is a typical setup in a co-processor or instruction set extension scenario. As expected, the area requirements of 4877 GE for one instance of the round function are the same for Camellia and p-Camellia and double to 9,754 GE for two instances. Also the maximum frequency of 229.4 MHz is the same for Camellia and p-Camellia in the one round implementation. However, as depicted in Figure 3 the critical path for two consecutive instances of the round function of Camellia is nearly twice as long as for p-Camellia. Consequently, the maximum frequency achievable for Camellia drops to 51.4% while it only slightly decreases to 96.5% for p-Camellia. p-Camellia cannot achieve exactly twice the maximum frequency, because it XORs three summands, while Camellia only XORs two summands. The maximum throughput of a 1 round implementation is the same for Camellia and p-Camellia and achieves 29.4 Gbps (Giga bits per second). A two round Camellia implementation slightly increases the maximum throughput by a mere 2.7% to 30.2 Gbps, while p-Camellia boosts the maximum throughput to 56.6 Gbps – an increment of 92.9% compared to the 1 round Camellia implementation and still 87.8% higher than the 2 round Camellia implementation.

Table 1 Comparison of the implementation results of the round function of Camellia and p-Camellia on UMC *180 nm* ASIC technology

	Camellia			
	1 round		*2 round*	
	abs.	*%*	*abs.*	*%*
Area (GE)	4,877	100	9,754	200
power* (mW)	2.65	100	8.38	316.5
max freq. (MHz)	229.4	100	117.8	51.4
max T'put (Gbps)	29.4	100	103	30.2
	p-Camellia			
	1 round		*2 round*	
	abs.	*%*	*abs.*	*%*
Area (GE)	4,877	100	9,754	200
power* (mW)	2.65	100	196.2	5.2
max freq. (MHz)	229.4	100	221.2	96.5
max T'put (Gbps)	29.4	100	56.6	192.9

Note: *At a frequency of 100 MHz and a supply voltage of 1.8 V.

For all architectures, we simulated the power consumption at a frequency of 100 MHz and a supply voltage of 1.8 Volt. 1 round of Camellia and p-Camellia require both 2.65 mW. While the power consumption for the 2 rounds implementation of Camellia increases more than 3 times (+216%) to 8.38 mW, it less than doubles for the 2 rounds implementation of p-Camellia (+96%) to 5.2 mW compared to the 1 round implementations. These figures highlight the advantages of p-Camellia over Camellia from a power perspective.

5 Application 2: parallelising SMS4

5.1 Brief description of SMS4

According to Diffe and Ledin (2008), SMS4 takes in a 128-bit key and uses a 32-round generalised Feistel structure to transform the plaintext to the ciphertext. Each round of the generalised Feistel transformation transforms four 32-bit words X_i, $i = 0, 1, 2, 3$, as follows:

$$\begin{aligned}&(X_0, X_1, X_2, X_3, r_k) \mapsto \\ &(X_1, X_2, X_3, X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus r_k)),\end{aligned} \tag{6}$$

where r_k denotes the round key. In each round, the non-linear function T does the following operations in sequence: 32-bit subkey addition, S-box substitution (layer of four 8-bit S-boxes) and lastly, a 32-bit linear transformation L.

It is well-known that the S-boxes adopt functions affine equivalent to the inversion function in $GF(2^8)$ (Ji and Hu, 2007; Choy et al., 2009c), which achieves the best known maximum differential and linear probabilities of 2^{-6}. Furthermore, it can be verified that the branch number of the linear transformation L is $\mathcal{L}_d = 5$. This gives optimal spreading effect which increases the number of active S-boxes for protection against differential and linear cryptanalysis.

The key schedule of SMS4 XORs the secret key MK with a constant FK and passes it through a nearly-identical 32-round structure as the main SMS4 cipher. The only difference is that the 32-bit linear transformation L is replaced by a simpler linear transformation L', which can be verified to have branch number $\mathcal{L}'_d = 4$. The 32-bit non-linear output of the i^{th} round of the key schedule is taken to be the i^{th} round subkey of the main cipher. For more details, please refer to Diffe and Ledin (2008).

5.2 Parallelising SMS4: p-SMS4

In this section, we propose another version of the existing SMS4 block cipher, which we call p-SMS4 (*'parallelisable' SMS4*). As described previously, SMS4 uses a generalised Feistel network structure described by equation (6). For the encryption procedure of p-SMS4, we shall replace the generalised Feistel network with the 4-cell GF-NLFSR block cipher structure described by:

$$\begin{aligned}&(X_0, X_1, X_2, X_3, r_k) \mapsto \\ &(X_1, X_2, X_3, X_1 \oplus X_2 \oplus X_3 \oplus T(X_0 \oplus r_k)).\end{aligned} \tag{7}$$

Other components such as number of rounds and the T-function, which consists of four S-boxes and a L-function, remain the same as SMS4. One round of p-SMS4 corresponds to a 4-cell version of the structure in Figure 1, where the non-linear function $F(\cdot)$ is the T-function used in SMS4.

The key schedule of p-SMS4 XORs the secret key MK with a constant FK and passes it through an identical 32-round structure as the main cipher of p-SMS4 described by equation (7). The constant FK, S-box and the linear transformation L' of the key schedule remain the same as SMS4. We need the key schedule to have the same structure as the main cipher so that it is also parallelisable in hardware, and thus can be made 'on-the-fly'.

5.3 Differential and linear cryptanalysis of p-SMS4

Su et al. proved bounds for the differential characteristic probability of the SMS4 cipher in Su et al. (2010). One of the results they proved was that in every 7 rounds of the SMS4 cipher, there are at least 5 active S-boxes. However, there are currently no known bounds on the linear characteristic probability of SMS4 to the best of our knowledge.

Similarly for the p-SMS4 cipher, we can easily compute the differential characteristic bound by Theorem 3. Denote the maximum differential probability of p-SMS4 reduced to 29-round by p (we assume a minus-3 round attack where the attacker guesses three subkeys with complexity 296).

Recall that both p-SMS4 and SMS4 use the same T-function. In the case of p-SMS4, the maximum differential probability of the S-boxes is 2^{-6} and $\mathcal{L}_d = 5$. By virtue of Theorem 3 with $n = 4$ and $r = 5$, the first 24 rounds has $5 \times 3 + \lfloor 3/2 \rfloor = 16$ active S-boxes. Over the next 5 rounds, we have 2 active S-boxes by

Proposition 1: Therefore, the differential characteristic probability over 29 rounds satisfies:

$$p \le (2^{-6})^{16} \times (2^{-6})^2 = 2^{-108}.$$

This implies that an attacker needs to collect at least 2^{108} chosen plaintext-ciphertext pairs to launch an attack. This is not feasible in practice. Moreover by Remark 1, for random input differences, we have at least 5 active S-boxes every 5 rounds with probability $1 - 2^{-32}$. Only 2^{-32} of the time do we need 8 rounds to ensure at least 5 active S-boxes. Thus, we expect the bound for the differential characteristic probability to be even lower. In summary, we have shown that p-SMS4 offers sufficient security against differential cryptanalysis.

Denote the maximum linear probability of p-SMS4 reduced to 28-round by q. Recall that the maximum linear probability of the S-boxes is 2^{-6} and the linear branch number is 5. By Theorem 5 and Corollary 1, we deduce that there must be at least 16 linear active S-boxes. Hence, $q \le (2^{-6})^{16} = 2^{-96}$. This implies that an attacker needs to collect at least 2^{96} chosen/known plaintexts to mount a linear attack, which is not feasible in practice.

This implies that there is no effective differential or linear characteristic for p-SMS4 reduced to more than 29 rounds. In other words, p-SMS4 offers sufficient security against differential and linear attack.

5.4 Related-key differential attack on p-SMS4

Related-key differential attacks have been shown to have the devastating effect of recovering the secret key of AES-256 with a complexity of 2^{131} using 2^{35} related keys in Biryukov et al. (2009). In related-key differential attack, there are non-zero differential inputs into both the cipher and the key schedule. The adversary tries to find a differential characteristic path in the key schedule with probability pk and a differential characteristic path in the main cipher with probability $p_{c|k}$ that holds, on the condition that the key schedule differential path is true. The attacker can then launch the attack with complexity $O(1 / (p_k \times p_{c|k}))$ where he can tweak the secret key $1 / p_k$ times to get that many related keys. In AES-256, we have $p_k = 2-35$ and $p_{c|k} = 2^{-93}$.

Because the p-SMS4 key schedule uses a 4-cell GF-NLFSR structure, we can try to bound the probability p_k of a differential characteristic path in the key schedule by Theorem 3. However, Theorem 3 cannot be directly applied to the main cipher to derive the differential characteristic probability $p_{c|k}$ because there are subkey differential inputs into every round.

We use the fact that the key schedule uses the inversion S-box with differential probability 2^{-6} and that the linear transform L' has branch number $\mathcal{L}'_d = 4$. By Theorem 3 with $n = 4$ and $r = 4$, every 24 rounds of the key schedule has $4 \times 3 + \lfloor 3/2 \rfloor = 13$ active S-boxes. With a computation similar to Section 5.3, we have another 2 active S-boxes over the next 5 rounds giving:

$$p_k \le (2^{-6})^{13} \times (2^{-6})^2 = 2^{-90}.$$

over 29 rounds of the key schedule. That means the complexity of any minus-3 round related-key differential attack is at least $O(2^{90})$ and uses at least 2^{90} related keys, which is not feasible in practice. Again, by a similar explanation as in Section 5.3 based on Remark 1, most of the time we have 5 active S-boxes per 5 rounds and we expect p_k to be lower and the attack complexity to be higher.

In Biryukov and Khovratovich (2009), a related-key boomerang attack on AES-256 with a complexity of 2^{119} using 4 related keys is presented but it assumes a more powerful adverserial model. In a similar way, we can show through the p-SMS4 key schedule differential structure that related-key boomerang attack is infeasible.

5.5 Other attacks on p-SMS4

5.5.1 Boomerang attack

Suppose an adversary performs a minus-3 round attack on 29 rounds of p-SMS4. He would need to split 29 rounds into two sub-ciphers E_0, E_1 with r and $29 - r$ rounds respectively, where $r = 1, \cdots, 28$. By Proposition 1 and Theorem 3, $p_0 \le (2^{-6})^{5\times\lfloor \frac{r}{8} \rfloor + 2\times\lfloor \frac{r \bmod 8}{5} \rfloor}$ and $p_1 \le (2^{-6})^{5\times\lfloor \frac{29-r}{8} \rfloor + 2\times\lfloor \frac{(29-r) \bmod 8}{5} \rfloor}$. (Note that we ignore the last term in the upper bound of Theorem 3 for ease of calculation.) For $r = 1, \cdots, 28$, let $n_8 = \lfloor \frac{r}{8} \rfloor + \lfloor \frac{29-r}{8} \rfloor$ and $n_5 = \lfloor \frac{r \bmod 8}{5} \rfloor + \lfloor \frac{(29-r) \bmod 8}{5}. \rfloor$ It can be easily checked that there are only three combinations of values that n_8 and n_5 can take, as summarised in the Table 2.

Now $p_0 \times p_1 \le (2^{-6})^{5n_8 + 2n_5}$. This implies that

$$p_0^2 \times p_1^2 \le (2^{-12})^{5n_s + 2n_5}.$$

The upper bounds of $p_0^2 \times p_1^2$ for each combination of n_8 and n_5 are also given in Table 2. From Table 2, we see that $p_0^2 \times p_1^2 < 2^{-128}$. Hence, p-SMS4 is secure against boomerang attack.

Table 2 Values of n_8, n_5 and upper bounds of $p_0^2 \times p_1^2$ for $r = 1, \cdots, 28$

n_8	n_5	r	$p_0^2 \times p_1^2$
3	0	1, ···, 4, 9, ···, 12, 17, ···, 20, 25, ···, 28	$\le (2^{-12})^{15} = 2^{-180}$
3	1	5, 8, 13, 16, 21, 24	$\le (2^{-12})^{15+2} = 2^{-204}$
2	2	6, 7, 14, 15, 22, 23	$\le (2^{-12})^{10+4} = 2^{-168}$

5.5.2 Impossible differential attack

According to Choy et al. (2009a), Li et al. (2009) and Wu et al. (2009), there is at least one 18-round impossible differential distinguisher in the 4-cell GF-NLFSR, which results in a 25-round impossible differential attack with complexity 2^{123} and uses 2^{115} chosen plaintext encryptions. An identical attack is applicable to 25-round p-SMS4 with the same complexity. However, that attack is unlikely to work on the full p-SMS4 cipher, which has 32 rounds.

5.5.3 Integral attack

According to Choy et al. (2009a) and Li et al. (2009), there is at least one 16-round integral attack distinguisher in the 4-cell GF-NLFSR starting with one active 32-bit word. A naive key guessing attack can extend this distinguisher by at most 3 rounds at the end (guessing more rounds of keys may make the complexity too close to 2^{128}). An adversary may extend the attack by 4 rounds in front, starting with three active words and using the method of Hwang et al. (2002). Using these means, we expect a 4 + 16 + 3 = 23 round attack on p-SMS4 and the full 32 rounds will be secure against integral attack.

5.5.4 Slide attack

The slide attack works on ciphers with cyclical structures over a few rounds. However, the subkeys used in every round are non-linearly derived from the previous subkey. Thus, the subkeys are all distinct and there is no simple linear relation between them, making slide attack unlikely.

5.5.5 XSL attack

Ji and Hu (2007) showed that the eprint XSL attack on SMS4 embedded in $GF(2^8)$ can be applied with complexity 277. A similar analysis can be applied on p-SMS4 to show that the complexity of the eprint XSL attack on p-SMS4 embedded in $GF(2^8)$ is also 277. However, it was shown by Choy et al. (2009c) that Ji and Hu's analysis might be too optimistic and the actual complexity of the compact XSL attack on embedded SMS4 is at least $2^{216.58}$. We can use an analysis identical to the ones used in Choy et al. (2009c) to show that the complexity of the compact XSL attack on p-SMS4 is also at least $2^{216.58}$.

Using a similar approach as Aoki et al. (2001), we discuss the protection of p-SMS4 against higher order differential attack and interpolation attack in the remaining of this section.

5.5.6 Higher order differential attack

As mentioned previously, higher order differential attack is generally applicable to ciphers that can be represented as Boolean polynomials of low degree in terms of the plaintext. The attack requires $O(2^{t+1})$ chosen plaintext when the cipher has degree t.

p-SMS4 uses exactly the same S-boxes as SMS4 where the degree of the Boolean polynomial of every output bit of the S-boxes is 7. Making the assumption that when we compose two *randomly chosen* S-boxes F, G of degree t_1, t_2, $F \circ G$ should have degree $t_1 t_2$. We expect the degree of an intermediate bit in the encryption process to increase exponentially as the data passes through many S-boxes.

Indeed, by the 4th round, every output bit will have degree 7. By the 8th round, every output bit will have degree $7^2 = 49$. By the 12th round, every output bit will have degree $\min(7^3, 127) = 127$ in terms of the plaintext bits. Therefore, p-SMS4 is secure against higher order differential attack.

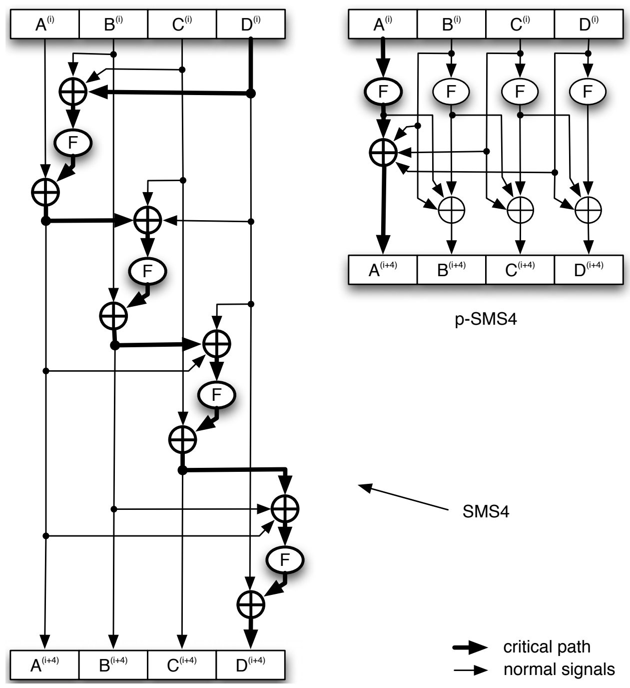
5.5.7 Interpolation attack

The interpolation attack works on block ciphers that can be expressed as an equation in $GF(2^d)$ with few monomials. p-SMS4 uses the same components as SMS4 and as the data passes through many S-boxes and L-functions, the cipher will became a complex function which is a sum of exponentially many multivariate monomials over $GF(2^8)$. Hence, we expect p-SMS4 to be secure against interpolation attack.

5.6 Implementation advantages

Similar to p-Camellia, we will assess the implementation advantages of p-SMS4 over SMS4 with respect to serialised, round-based and parallelised architectures. In case of SMS4, the XOR sum of three branches forms the input to the F-function and its output is XORed to the last branch while p-SMS4 uses one branch as the input for the F-function and XORs its output to the remaining three branches. This difference allows more flexible implementations of p-SMS4 compared to SMS4, because the XOR sum of four signals can be achieved by either using three 2-input XOR gates or combining a 3-input XOR gate with a 2-input XOR gate. The first option is faster (0.33 ns vs. 0.45 ns) while the second option requires less area (256 GE vs. 235 GE), which is an advantage for lightweight implementations. Beside this flexibility, p-SMS4 has similar characteristics as SMS4 for a serialised implementation. The critical path of a round-based p-SMS4 implementation is shorter than that of SMS4, since it consists of the F-function and a 2-input XOR gate compared to a 3-input XOR gate, the F-function and a 2-input XOR gate for SMS4.

Figure 4 Possible hardware architecture of four rounds of (a) SMS4 and (b) p-SMS4



(a) (b)

For parallelised implementations p-SMS4 offers even greater advantages. If we consider an implementation that processes four rounds in one clock cycle (see Figure 4), the critical path of p-SMS consists only of the F-function and two 2-input XOR gates while SMS4's critical path consists of four F-functions, four 2-input XOR gates and four 3-input XOR gates. Hence, the maximum frequency and thus the maximum throughput that can be achieved with p-SMS4 using such an architecture is around four times higher while the area and power consumption are similar or lower compared to a corresponding SMS4 implementation. A similar frequency can be achieved for SMS4 by inserting three pipelining stages, which significantly increases the area and power consumption and introduces a delay of three clock cycles.

To substantiate our claims, we have implemented the round function of SMS4 and p-SMS4 in VHDL. We obtained area, timing and power figures for a 180 nm ASIC technology from UMC using Synopsys design vision for synthesis. Table 3 depicts a comparison of the hardware implementation results of the round function of SMS4 and p-SMS4. This is a typical setup in a co-processor or instruction set extension scenario. As expected, the area requirements of 2,924 GE for one instance of the round function are the same for SMS3 and p-SMS4 and nearly quadruple to 11,546 GE and 11,574 GE for four instances. The 1 round implementation of p-SMS4 achieves a slightly higher maximum frequency of 290.7 MHz compared to SMS4 with 288.2 MHz. However, as depicted in Figure 4 the critical path for four consecutive instances of the round function of SMS4 is nearly four times as long as for p-SMS4. Consequently, the maximum frequency achievable for SMS4 drops to 25.4% while it only slightly decreases to 92.8% for p-SMS4. The maximum throughput of a 1 round implementation is the about same for SMS4 and p-SMS4 and achieves 36.9 Gbps and 37.2 Gbps, respectively. A four round SMS4 implementation slightly increases the maximum throughput by a mere 1.4% to 37.4 Gbps, while p-SMS4 boosts the maximum throughput to 136.9 Gbps – an increment of 271.1% compared to the 1 round SMS4 implementation and still 266% higher than the 4 round SMS4 implementation.

Table 3 Comparison of the implementation results of the round function of SMS4 and p-SMS4 on UMC *180 nm* ASIC technology

	SMS4			
	1 round		*4 round*	
	abs.	*%*	*abs.*	*%*
Area (GE)	2,924	100	11,546	394.9
power* (mW)	1.81	100	11.38	627.5
max freq. (MHz)	288.2	100	73.1	25.4
max T'put (Gbps)	36.9	100	37.4	101.4
	p-SMS4			
	1 round		*4 round*	
	abs.	*%*	*abs.*	*%*
Area (GE)	2,924	100	11,574	395.9
power* (mW)	1.39	76.8	5.9	322.3
max freq. (MHz)	290.7	100.9	267.4	92.8
max T'put (Gbps)	37.2	100.9	136.9	371.1

Note: *At a frequency of 100 MHz and a supply voltage of 1.8 V.

For all architectures, we simulated the power consumption at a frequency of 100 MHz and a supply voltage of 1.8 V. 1 round of SMS4 requires 1.81 mW and a similar p-SMS4 implementation requires 1.39 mW. While the power consumption for the 4 rounds implementation of SMS4 increases more than 6 times (+528%) to 11.38 mW, it less than quadruples for the 4 rounds implementation of p-SMS4 (+222%) to 5.85 mW compared to the 1 round implementations. These figures highlight the advantages of p-SMS4 over SMS4 from a power perspective.

From these estimates it becomes clear that the implementation advantages of our newly proposed parallelisable Feistel-structure becomes even larger with a growing number of branches. In fact, an n-cell GF-NLFSR can be implemented using n rounds in parallel while having nearly the same critical path as for a single round implementation. This translates to an about n times higher maximum frequency while the area and power consumption are similar then for a conventional Feistel structure.

6 Conclusions

In this paper, we proposed the use of n-cell GF-NLFSR structure to parallelise (generalised) Feistel structures. We used two examples, p-Camellia and p-SMS4, and showed that they offer sufficient security against various known existing attacks. At the same time, as compared to their conventional Feistel structure counterparts Camellia and SMS4, their hardware implementations achieve a maximum frequency that is about n times higher, where n is the number of Feistel branches, while having similar area demands and significantly less power demands. These estimates indicate that of n-cell GF-NLFSRs are particularly well suited for applications that require a high throughput.

Acknowledgements

The research was supported in part by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

References

'SKIPJACK and KEA Algorithm Specifications', available at http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf (accessed on 14 May 2010).

'Universal Mobile Telecommunications System (UMTS); 'Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification', available at http://www.etsi.org/website/document/algorithms/ts_135202v070000p.pdf (accessed on 14 May 2010).

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. and Tokita, T. (2000) 'Specification of Camellia – a 128-bit block cipher', available at http://info.isl.ntt.co.jp/camellia/ (accessed on 14 May 2010).

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. and Tokita, T. (2001) 'Camellia: a 128-bit block cipher suitable for multiple platforms, design and analysis', *SAC 2000, LNCS*, pp.39–56, Springer-Verlag.

Biryukov, A. and Khovratovich, D. (2009) 'Related-key cryptanalysis of the full AES-192 and AES-256', IACR eprint server, 2009/317, June, available at http://eprint.iacr.org/2009/317 (accessed on 14 May 2010).

Biryukov, A., Khovratovich, D. and Nikolic, I. (2009) 'Distinguisher and related-key attack on the full AES-256 (extended version)', IACR eprint server, 2009/241, June, http://eprint.iacr.org/2009/241 (accessed on 14 May 2010).

Choy, J., Chew, G., Khoo, K. and Yap, H. (2009a) 'Cryptographic properties and application of a generalized unbalanced Feistel network structure (revised version)', Cryptology Eprint Archive, Report 2009/178, July, (Revision of Choy et al., 2009b).

Choy, J., Chew, G., Khoo, K. and Yap, H. (2009b) 'Cryptographic properties and application of a generalized unbalanced Feistel network structure', *ACISP 2009, LNCS*, Vol. 5594, pp.73–89, Springer-Verlag.

Choy, J., Yap, H. and Khoo, K. (2009c) 'An analysis of the compact XSL attack on BES and embedded SMS4', to appear in *Proceedings of CANS 2009*, Springer-Verlag.

Diffe, W. and Ledin, G. (2008) 'SMS4 encryption algorithm for wireless networks', Cryptology ePrint Archive: Report 329.

Hwang, K., Lee, W., Lee, S., Lee, S. and Lim, J. (2002) 'Saturation attacks on reduced round skipjack', *FSE 2002, LNCS*, Vol. 2365, pp.100–111, Springer-Verlag.

Jakobsen, T. and Knudsen, L.R. (1997) 'The interpolation attack on block ciphers', *LNCS, FSE 1997*, Vol. 1267, pp.28–40, Springer-Verlag.

Jakobsen, T. and Knudsen, L.R. (2001) 'Attacks on block ciphers of low algebraic degree', *Journal of Cryptology*, Vol. 14, No. 3, pp.197–210, Springer.

Ji, W. and Hu, L. (2007) 'New description of SMS4 by an embedding over $GF(2^8)$', *LNCS, Indocrypt 2007*, Vol. 4859, pp.238–251, Springer-Verlag.

Kanda, M. (2001) 'Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function', *SAC 2000, LNCS*, Vol. 2012, pp.324–338, Springer-Verlag.

Knudsen, L.R. (1995) 'Truncated and higher order differentials', *LNCS, FSE 1994*, Vol. 1008, pp.196–211, Springer-Verlag.

Li, R., Sun, B. and Li, C. (2009) 'Distinguishing attack on a kind of generalized unbalanced Feistel network', Cryptology Eprint Archive, Report 2009/360, July.

Matsui, M. (1995) 'On correlation between the order of S-boxes and the strength of DES', *Eurocrypt 1994, LNCS*, Vol. 950, pp.366–375.

National Bureau of Standards (1977) 'Data encryption standard', FIPS-Pub. 46, National Bureau of Standards, US Department of Commerce, Washington DC, January.

Park, S., Sung, S., Lee, S. and Lim, J. (2003) 'Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES', *FSE 2003, LNCS*, Vol. 2887, pp.247–260, Springer-Verlag.

Rijmen, V., Daemon, J., Preneel, B., Bosselaers, A. and Win, E.D. (1996) 'The cipher SHARK', *Fast Software Encryption – Third International Workshop, LNCS*, Vol. 1039, pp.99–111, Springer.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S. and Iwata, T. (2007) 'The 128-bit blockcipher CLEFIA (extended abstract)', *FSE 2007, LNCS*, Vol. 4593, pp.181–195, Springer-Verlag.

Su, B., Wu, W. and Zhang, W. (2010) 'Differential cryptanalysis of SMS4 block cipher', Cryptology Eprint Archive, Report 2010/062, February.

Wei, Y., Li, P., Sun, B. and Li, C. (2010) 'Impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions', *ACNS 2010, LNCS*, Vol. 6123, pp.105–122, Springer.

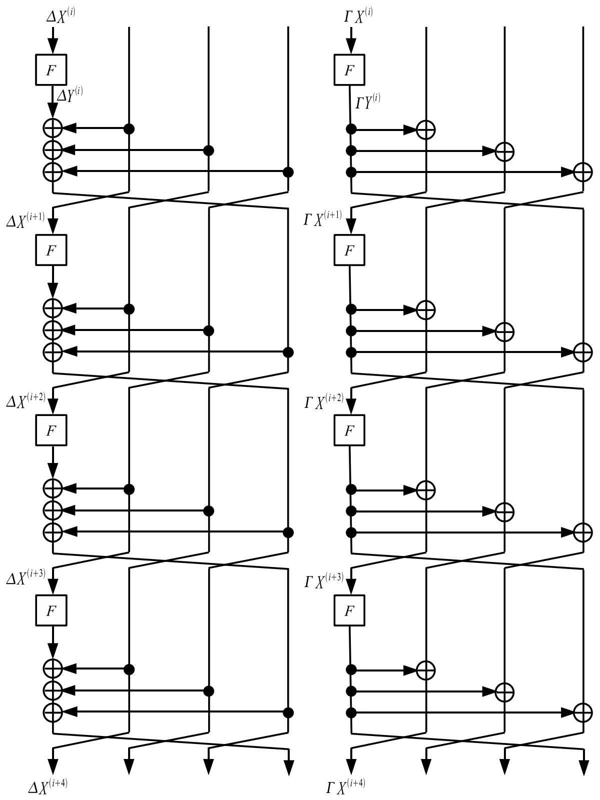
Wu, W., Zhang, L., Zhang, L. and Zhang, W. (2009) 'Security analysis of the GF-NLFSR structure and four-cell block cipher', Cryptology Eprint Archive, Report 2009/346, July.

Yap, H., Khoo, K. and Poschmann, A. (2010) 'Parallelizing the Camellia and SMS4 block ciphers', *Africacrypt 2010, LNCS*, Vol. 6055, pp.387–406, Springer.

Appendix A

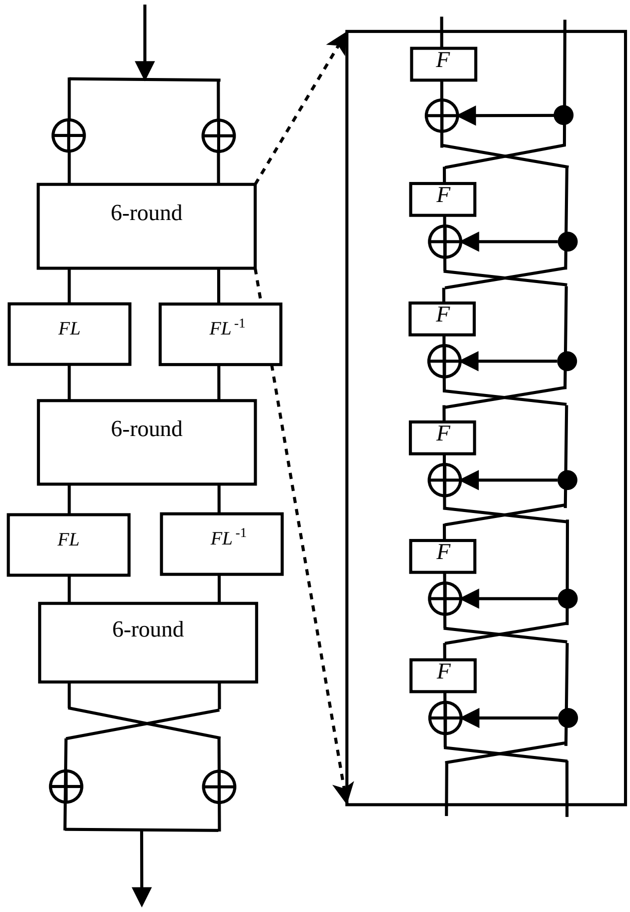
A.1 Figures

Figure 5 (a) 4-cell GF-NLFSR cipher (b) Dual of 4-cell GF-NLFSR cipher



(a) (b)

Figure 6 p-Camellia block cipher structure



A.2 Test vectors

Here, we provide test vectors for p-Camellia with 128, 192, and 256 bit keys (Tables 4 to 6) and for p-SMS4 with a 128 bit key (Table 7). We stick to the test vector format of the corresponding original ciphers, Camellia and SMS4.

Table 4 Test vector for p-Camellia-128

Plaintext			0123456789abcdef	fedcba9876543210
Key			0123456789abcdef	fedcba9876543210
Ciphertext			defcf36c09623e05	018e2cbe8f56b8d5
Operation		*Round key*	*Output*	
Pre-whitening	k_{w1}	0123456789abcdef	0000000000000000	0000000000000000
	k_{w2}	fedcba9876543210		
Round 1	k_1	eea36580448142e6	0000000000000000	9b8d4b3590733c4d
Round 2	k_2	6f90d050fe0bbe7d	9b8d4b3590733c4d	980912c9086ee08f
Round 3	k_3	a2b3c4d5e6f7ff6e	980912c9086ee08f	414509b219335b44
Round 4	k_4	5d4c3b2a19080091	414509b219335b44	da0823938d86088a
Round 5	k_5	b2c02240a17337c8	da0823938d86088a	11b9c2d3140d6f0d
Round 6	k_6	68287f05df3ef751	11b9c2d3140d6f0d	f8e2ea3adda357d9
FL	k_{l1}	112050b99be43414	ae543cec364dee2f	074935c3d3a31cdf
FL^{-1}	k_{l2}	3f82ef9f7ba8d960		
Round 7	k_7	79bdffdb97530eca	074935c3d3a31cdf	d7bc446d2558b71f
Round 8	K_8	8642002468acf135	d7bc446d2558b71f	35a14189576f51e2
Round 9	k_9	285ccdf21a0a1fc1	35a14189576f51e2	6fcd64be097d4302
Round 10	k_{10}	00123456789abcde	6fcd64be097d4302	2bcf3494f5cc36f9
Round 11	k_{11}	66f90d050fe0bbe7	2bcf3494f5cc36f9	e1376d1f82a7d0db
Round 12	k_{12}	deea36580448142e	e1376d1f82a7d0db	ac3b5fa60d77ff6a
FL	k_{l3}	97530eca86420024	67f4a5f18081c8ce	d1c4a05d8c7ebf40
FL^{-1}	k_{l4}	68acf13579bdffdb		
Round 13	k_{13}	1d950c840048d159	d1c4a05d8c7ebf40	b8013fe2ccca5214
Round 14	k_{14}	e26af37bffb72ea6	b8013fe2ccca5214	3a02d81ca092f03e
Round 15	k_{15}	3f82ef9f7ba8d960	3a02d81ca092f03e	c356213d32c0c94e
Round 16	k_{16}	112050b99be43414	c356213d32c0c94e	2c5c47a3889f8ffa
Round 17	k_{17}	19080091a2b3c4d5	2c5c47a3889f8ffa	a0fd1b76e77ec7d0
Round 18	k_{18}	e6f7ff6e5d4c3b2a	a0fd1b76e77ec7d0	01c2043dbba21c45
Post-whitening	k_{w3}	df3ef751b2c02240	defcf36c09623e05	018e2cbe8f56b8d5
	k_{w4}	a17337c868287f05		

Table 5 Test vector for p-Camellia-192

Plaintext			0123456789abcdef	fedcba9876543210
Key		0123456789abcdef	fedcba9876543210	0011223344556677
Ciphertext			e35d78a07ceaceb6	da16c6636d9fc622
Operation		*Round key*	*Output*	
Pre-whitening	k_{w1}	0123456789abcdef	0000000000000000	0000000000000000
	k_{w2}	fedcba9876543210		
Round 1	k_1	946e4e08d66a0dd8	0000000000000000	171c7c6793de1963
Round 2	k_2	fd823d9ed6fd541a	171c7c6793de1963	72129f29ca6a2a80
Round 3	k_3	9119a22ab33bfff7	72129f29ca6a2a80	198bacc0cfb1d383
Round 4	k_4	6ee65dd54cc40008	198bacc0cfb1d383	8ba65aa81ab1ac52
Round 5	k_5	0c2459e9c0530c7c	8ba65aa81ab1ac52	d183a232aaa243f0
Round 6	$k6$	4b7c30e3beef03a9	d183a232aaa243f0	22f03f1035031522
FL	k_{l1}	d115599dfffbb773	2e7855c108a043d1	17f762be38c75166
FL^{-1}	k_{l2}	2eeaa6620004488c		
Round 7	k_7	359a83763f608f67	17f762be38c75166	f257afda34b38387
Round 8	k_8	b5bf5506a51b9382	f257afda34b38387	9e77985b6aca9bf3
Round 9	$k9$	79bdffdb97530eca	9e77985b6aca9bf3	0e613abf6d8ad439
Round 10	k_{10}	8642002468acf135	0e613abf6d8ad439	f58170c3dd427d63
Round 11	k_{11}	7014c31f12df0c38	f58170c3dd427d63	46379e50f9619c03
Round 12	k_{12}	efbbc0ea4309167a	46379e50f9619c03	84c3e9dc6d38db5d
FL	k_{l3}	ffedcba987654321	b1585573752a8803	f97916036d18f359
FL^{-1}	k_{l4}	00123456789abcde		
Round 13	k_{13}	7ffeeddccbbaa998	f97916036d18f359	12bd5761b07ff06e
Round 14	k_{14}	8001122334455667	12bd5761b07ff06e	8f5546bf37cd2a29
Round 15	k_{15}	8fd823d9ed6fd541	8f5546bf37cd2a29	b5070bb89e052ac6
Round 16	k_{16}	a946e4e08d66a0dd	b5070bb89e052ac6	53206e03fd9f1484
Round 17	k_{17}	97530eca86420024	53206e03fd9f1484	8c49ce7921328baa
Round 18	k_{18}	68acf13579bdffdb	8c49ce7921328baa	f923d08f8c97d101
FL	k_{l5}	12df0c38efbbc0ea	63f21d8321a093da	05b403908e97d521
FL^{-1}	k_{l6}	4309167a7014c31f		
Round 19	k_{19}	2eeaa6620004488c	05b403908e97d521	366e2dce4fd51db0
Round 20	k_{20}	d115599dfffbb773	366e2dce4fd51db0	b7a24c53ed656ca6
Round 21	k_{21}	1871df7781d48612	b7a24c53ed656ca6	18b77e6662209c0a
Round 22	k_{22}	2cf4e029863e25be	18b77e6662209c0a	c2fbdf4b21c3b0df
Round 23	k_{23}	19080091a2b3c4d5	c2fbdf4b21c3b0df	dcfab8a27350ad5c
Round 24	k_{24}	e6f7ff6e5d4c3b2a	dcfab8a27350ad5c	495032975beea583
Post-whitening	k_{w3}	aa0d4a3727046b35	e35d78a07ceaceb6	da16c6636d9fc622
	k_{w4}	06ec7ec11ecf6b7e		

Table 6 Test vector for p-Camellia-256

Plaintext			0123456789abcdef	fedcba9876543210
Key			0123456789abcdef	fedcba9876543210
			0011223344556677	8899aabbccddeeff
Ciphertext			15e3eef9b879ebcd	d8204f9436564e0c
Operation		*Round key*	*Output*	
Pre-whitening	k_{w1}	0123456789abcdef	0000000000000000	0000000000000000
	k_{w2}	fedcba9876543210		
Round 1	k_1	8a5189e3b3d105c5	0000000000000000	487d45ecf3404dc7
Round 2	k_2	1daae720c89263ca	487d45ecf3404dc7	e66963613ebf68c7
Round 3	k_3	9119a22ab33bc44c	e66963613ebf68c7	6b1f28f6f41644cd
Round 4	k_4	d55de66ef77f8008	6b1f28f6f41644cd	c2c6cb8ca0535412
Round 5	k_5	671465d1b2160e57	c2c6cb8ca0535412	09e62c405dc5b786
Round 6	k_6	bcd4f117fd2b818f	09e62c405dc5b786	ae86bd493cdca41d
FL	k_{l1}	d115599de2266aae	f609c3ee5fcda78	6525a51d498f80735
FL^{-1}	k_{l2}	f3377bbfc004488c		
Round 7	k_7	ecf44171476ab9c8	525a51d498f80735	4cd907551429dc24
Round 8	k_8	322498f2a2946278	4cd907551429dc24	b313976933fd7a24
Round 9	k_9	79bdffdb97530eca	b313976933fd7a24	d4cd98ff068beac2
Round 10	k_{10}	8642002468acf135	d4cd98ff068beac2	7058010931524a06
Round 11	k_{11}	6c858395ef353c45	7058010931524a06	68acfb7d01e73e3c
Round 12	k_{12}	ff4ae063d9c51974	68acfb7d01e73e3c	6c7c32deb7811418
FL	k_{l3}	ffedcba987654321	bf531012d0bea86e	93e78e00b7851c18
FL^{-1}	k_{l4}	00123456789abcde		
Round 13	k_{13}	78899aabbccddeef	93e78e00b7851c18	15c67729db978ee7
Round 14	k_{14}	f001122334455667	15c67729db978ee7	474795e9e443e49b
Round 15	k_{15}	51daae720c89263c	474795e9e443e49b	af3bb8f76290ced6
Round 16	k_{16}	a8a5189e3b3d105c	af3bb8f76290ced6	762f5f82c62e0f8b
Round 17	k_{17}	97530eca86420024	762f5f82c62e0f8b	cb67a0a09434a577
Round 18	k_{18}	68acf13579bdffdb	cb67a0a09434a577	58a9b0d80095ffb8
FL	k_{l5}	ef353c45ff4ae063	341945d7027ee576	343c4f65209ded70
FL^{-1}	k_{l6}	d9c519746c858395		
Round 19	k_{19}	f3377bbfc004488c	343c4f65209ded70	1c0f7737506e358c
Round 20	k_{20}	d115599de2266aae	1c0f7737506e358c	612a4c06b75fa8e1
Round 21	$k_2 1$	788bfe95c0c7b38a	612a4c06b75fa8e1	a1972fbb555d9a6c
Round 22	k_{22}	32e8d90b072bde6a	a1972fbb555d9a6c	9f58893990e4fe98
Round 23	k_{23}	19080091a2b3c4d5	9f58893990e4fe98	5ac2c14145c62a45
Round 24	$k_2 4$	e6f7ff6e5d4c3b2a	5ac2c14145c62a45	2406abd17c883225
Post-whitening	k_{w3}	31e54528c4f1d9e8	15e3eef9b879ebcd	d8204f9436564e0c
	k_{w4}	82e28ed573906449		

Table 7 Test vector for p-SMS4

Plaintext	0123456789abcdef	fedcba9876543210
Key	0123456789abcdef	fedcba9876543210
Ciphertext	b1bc0608ef02423c	c3fbd3daab51b248
Operation	*Round key*	*Output*
Round 0	rk[0] = 91daf39c	X[0] = de546515
Round 1	rk[1] = c064f752	X[1] = 37df26d1
Round 2	rk[2] = 94e493e3	X[2] = a4ec9909
Round 3	rk[3] = de78427b	X[3] = 52425f79
Round 4	rk[4] = 2db76314	X[4] = d24a93d6
Round 5	rk[5] = 73451fb4	X[5] = f5f06a45
Round 6	rk[6] = 06daf312	X[6] = 6b38d201
Round 7	rk[7] = 86788fc8	X[7] = dfa666eb
Round 8	rk[8] = 5b2a143a	X[8] = 023d696e
Round 9	rk[9] = be03897b	X[9] = 6e33c8db
Round 10	rk[10] = 0f3b7112	X[10] = 68adf8a8
Round 11	rk[11] = 0062e41b	X[11] = a80ce0c1
Round 12	rk[12] = eef9fa01	X[12] = 868f5476
Round 13	rk[13] = 62678f1b	X[13] = 6e6ff87b
Round 14	rk[14] = a62c3624	X[14] = 1f7a4d1d
Round 15	rk[15] = e276a56a	X[15] = 57cf029d
Round 16	rk[16] = a1e07f93	X[16] = 336dce80
Round 17	rk[17] = cd493f68	X[17] = 052af90a
Round 18	rk[18] = 25935606	X[18] = fd43fa3b
Round 19	rk[19] = cc82ba7f	X[19] = b4f7dbaf
Round 20	rk[20] = 97ddff3e	X[20] = 053c1645
Round 21	rk[21] = f19615bf	X[21] = c28b9543
Round 22	rk[22] = af40d76d	X[22] = eb913b2a
Round 23	rk[23] = 371225f4	X[23] = 42f09763
Round 24	rk[24] = 56f5df7d	X[24] = 938296fd
Round 25	rk[25] = e18e3f68	X[25] = 57f0a98c
Round 26	rk[26] = 51de4d8e	X[26] = fa771ab4
Round 27	rk[27] = 3e8cf9ba	X[27] = 08b74c18
Round 28	rk[28] = 863f59db	X[28] = ab51b248
Round 29	rk[29] = cf23b8c6	X[29] = c3fbd3da
Round 30	rk[30] = b3cd61a9	X[30] = ef02423c
Round 31	rk[31] = 657ab0ae	X[31] = b1bc0608