SSM: Scalable Substitution Matrix Cipher

Dang Hai Van

Faculty of Information Technology
University of Science, VNU-HCM
dhvan@fit.hcmuns.edu.vn

Nguyen Thanh Binh

Faculty of Mathematics and Informatics
University of Science, VNU-HCM
ntbinh@mathdep.hcmuns.edu.vn

Tran Minh Triet

Faculty of Information Technology
University of Science, VNU-HCM
tmtriet@fit.hcmuns.edu.vn

Tran Ngoc Bao

Faculty of Mathematics and Informatics
University of Pedagogy, VNU-HCM
baotn@math.hcmup.edu.vn

We present Scalable Substitution Matrix Cipher (SSM). As a direct instance of the Substitution Permutation Network scheme, SSM is constructed by multiple rounds of transformations, each of which consists of a fixed non-linear substitution layer and a scalable keyed linear permutation layer. With the scalability of the permutation layer, SSM provides capabilities to extend block length and key length infinitely. This resolves the limitation of most secured block ciphers that support only several legal key/block lengths. As the security of SSM against differential and linear cryptanalysis is proved independently of specific values of key length and block length, for any key length and block length of SSM, SSM is expected to behave as good as can be expected from a block cipher with the same key length and block length.

Keywords: scalability, block cipher, substitution permutation network, matrix cipher, SSM

1. Introduction

Nowadays, there is an increasing need for new secure cryptographic algorithms to be used in various applications, such as e-commerce, smartcards, distributed computing... Therefore, governments and organizations have sought public submissions and evaluation to standardize new secure cryptographic primitives. Among new algorithms are symmetric block ciphers, the essential component in digital infrustrature and secure protocols.

Since mid-1990s, a lot of new block ciphers have been proposed, such as Rijndael [1], Khazad [2], Anubis[3], Camellia[4], ARIA [5], Hierocrypt [6,7]... However, most of new block ciphers support only several legel key lengths and block lengths. For example, Rijndael supports keys (resp. blocks) of 128, 192, or 256 bits. Thus, the scalability of these ciphers are limited to a predefined set of key sizes (resp. block sizes), and the maximum size of a key (resp. a block) is upper bounded. Hense new algorithms supporting larger keys and larger blocks should be devised to substitute these ciphers when current shorted-keyed algorithms become no longer practically secure in the future. Consequently, a secure cryptosystem that supports unlimited key size and block size is practically necessary as it can be used even when longer-keyed algorithm is required. This is the first objective of our proposal of a secure scalable block cipher, entitled Scalable Substitution Matrix cipher (SSM).

In fact, several symmetric ciphers based on matrix multiplcation have been proposed to achieve this property, such as Hill cipher [8] or its variants [9–11]. Unfortunately, these ciphers are completely linear and the security of these cipher achieve only by means of increasing significantly key length, thus inefficient in practical applications. A secure cipher

cannot be constructed with only matrix multiplication. However, as matrix multiplication provides diffusion, it is a useful cryptographic component to be used with non-linear transformations. Thus in this paper, we take another approach to construct a scalable secure cipher by integrating non-linear and linear components. SSM consists of multiple rounds of transformations, each of which includes a fixed non-linear byte substitution and a key-dependent matrix multiplication. Hence SSM follows the block cipher scheme Substitution - Permutation Network (SPN) [12], proposed by J.B. Kam and G.I. Davida.

Most secure block ciphers following SPN use high diffusion mappings as permutation layers, such as maximum diffusion layers constructed by MDS-code in Shark [13], Square [14], Rijndael, GrandCru [15], Khazad,Anubis... As it is highly cost to construct such maximum diffusion layer, the diffusion layer is usually fixed thus key independent. In this paper, we aim to illustrate that a transformation that does not necessarily provide maximum diffusion can be used to construct secure ciphers. We propose a simple yet efficient method to construct a linear mapping with branch number [1] of 3 or 4 to be used in SSM.

The paper is organized as follows. In section 2, we review related works and analyse our approach to construct SSM. Our method to construct a linear mapping with branch number of no less a specific threshold β(in this paper, we consider $\beta = 3$ or 4) to be used in SSM is presented and analysed in section 3. In section 4, we describe SSM in details. Security analysis against differential and linear cryptanalysis is discussed in section 5. Performance analysis of SSM is illustrated in section 6, then conclusions and future works in section 7.

2. Background and related works

Firstly we review Hill cipher and its variants to analyse their advantages and limitations. We then present briefly Substitution-Permutation Network, the cipher scheme we use to construct SSM. Finally, we analyse current approach to use maximum diffusion mappings as permutation layers and propose our idea to use easy-to-find mappings with less diffusion capability to construct secure ciphers.

2.1. *Matrix cipher and scalability*

Scalibility is the property of most public key cryptosystems, such as RSA [16], Diffie-Hellman [17]... However, several symmetric key crytosystems also have this characteristic, such as Hill cipher [8] and some of its variants [9–11].

In Hill cipher, each letter is treated as a number in $\mathbb{Z}_{26}$. A block of n letters is processed as a vector of n dimensions, and multiplied by a $n \times n$ matrix, modulo 26. In order to decrypt, this permutation matrix must be invertible in $\mathbb{Z}_{26}^n$ and is considered as the cipher key. Hill cipher is completely linear thus vulnerable to known plaintext attack.

From this classical cryptosystem, several modifications have been proposed to strengthen the security of Hill cipher.

- In [9], Saeednia proposed to use a pre-shared invertible matrix to protect permutation matrix. This proposal turns out to be a key exchange protocol rather than a modified cipher.
- In [10,11], Sastry and Shankar suggested to use bit-transpositions to provide confusion and multiple rounds of encryption to improve the security. However, all these variants are totally constructed by linear cryptographic components.

We also follow the usage of matrix multiplication to construct a scalable diffusion layer. However we mix this layer with non-linear byte substitution to create a secure cipher with scalability.

2.2. *Substitution-Permutation Network*

C. Shannon proposed to use confusion and diffusion as two properties of operations of a secure cipher [18]. His proposal is considered as the general strategy to construct modern secure block ciphers. Together with Feistel network [19], Substitution-permutation-network (SPN) [12], proposed by J.B. Kam and G.I. Davida, is one of the most popular block cipher schemes that have greate influence to modern block ciphers.

A cipher that follows SPN scheme consists of multiple rounds of transformation, each of which consists of a substitution layer and a permutation layer to provide confusion and diffusion respectively. In the construction of SSM, we follow strictly the structure

of SPN. The substitution layer is implemented as a fixed key-independent byte substitution while the permutation layer is constructed by matrix multiplication.

2.3. *Diffusion layer and Branch Number*

Definition 1. Branch Number [1], denoted by B, of a linear transformation F is defined as follows:

$$B(F)=\min\{wt(a)+wt(F(a)), a\in\mathrm{dom}(F)\backslash\{0\}\} \quad (1)$$

where wt is Hamming weight (the number of non-zero elements in a given vector).

If F is defined over n-dimensional space, $B(F)$ is upper bounded by $n+1$. F is considered as maximum diffusion layer [13] if $B(F)=n+1$. Maximum diffusion layers are common cryptographic components in many modern secure ciphers [1–3,13,14]. However, as it is highly cost to construct such optimum diffusion layer, this component is usually fixed and key-independent. Thus another key-dependent component is required in each round of transformations. In this paper, we propose a scheme to combine key-dependent component and diffusion layer into a keyed-diffusion layer. To achieve this, we use matrix multiplication corresponding to branch number of 3 or 4 and the matrix is the cipher key.

3. Generating invertible matrix with certain diffusion capability

In this section, we propose two specific strategies to generate an $n\times n$ matrix with branch number of no less the β for $beta = 3$ and 4 respectively. Then we use the criterion proposed in Theorem 2 of [20] to ensure generated matrix be invertible in $\mathbb{Z}_{256}^n$. We use these 2 types of matrices in permutation layer of SSM (cf. Sec. 4.3)

Definition 2. Given a matrix $M_{n\times n}$. M satisfies constraint Φ_k iff for any k-tuple of columns, there exists d_1 rows ($d_1 \geq d-k$) of M such that there exists only one non-zero element in each of these d_1 rows.

Theorem 3.1. *Given d ($2\leq d\leq n-1$) and a matrix $M_{n\times n}$ satisfies Φ_k for $k=1,...,d-1$. Then for any column vector $X=(x_1,...,x_2)^T\neq 0$, we have:*

$$\min\left\{wt(X)+wt(MX^T)\right\}\geq d \quad (2)$$

Proof. Let $Q=MX^T=(q_1,...,q_n)^T$ where $q_i=\sum_{j=1}^{n} m_{ij}x_j$. As X is a non-zero vector, $wt(X)=k\geq 1$. Suppose that

$$\begin{cases} x_{i_1},...,x_{i_k}\neq 0 \\ x_i=0,\forall i\notin\{i_1,...,i_k\}=I \end{cases} \quad (3)$$

We have

$$\begin{aligned} q_l=\sum_{i=1}^{n} m_{li}x_i &= \sum_{i\in\{i_1,...,i_k\}} m_{li}x_i+\sum_{i\notin\{i_1,...,i_k\}} m_{li}x_i \\ &=\sum_{i\in I} m_{li}x_i+0=\sum_{i\in I} m_{li}x_i \end{aligned} \quad (4)$$

There are $d_1\geq(d-k)$ rows, denoted by $L=\{l_1,...,l_{d_1}\}$ so that for each row l_i ($i=1,...,d_1$) there is exactly one non-zero element, denoted by m_{li_t}, hence:

$$\begin{aligned} q_l&=\sum_{i\in I} m_{li}x_i \\ &=m_{li_1}x_{i_1}+m_{li_2}x_{i_2}+...+m_{li_t}x_{i_t}+...+m_{li_k}x_{i_k} \\ &=0+0+...+m_{li_t}x_{i_t}+0+...=m_{li_t}x_{i_t}\neq 0 \end{aligned} \quad (5)$$

Therefore Q has $d_1\geq(d-k)$ non-zero elements.

$$\begin{aligned} \Rightarrow wt(X)+wt(MX^T)&=k+d_1 \\ &\geq k+(d-k)=d \end{aligned} \quad (6)$$

. □

Theorem 3.2. *If $M_{n\times n}$ ($n\geq 3$) satisfies the following conditions:*

(i) $M_{ij}\neq 0$, if $(i-j) \bmod n\leq 1$
(ii) $M_{ij}=0$, if $(i<j)\wedge((i-j) \bmod n>1)$

then
(P) : for any k-tuple of columns ($k\in\{1,2\}$), there exist $d_1\geq(3-k)$ rows so that in each of these d_1 rows, there is exactly one non-zero element.

Proof. To prove (P), we need to prove the two following statements:
(P_1) If $k=1$, for any 1-tuple of column, there are at least 2 rows such that each row has only one non-zero element in this column.
(P_2) If $k=2$, for any 2-tuple of column, there is at least 1 row such that this row has only one non-zero element in these columns.

Because M satisfies (i), we have (P_1). We prove that (P_2) is also true.

Table 1. Form of matrix satisfying conditions of Theorem 3.2.

$\neq 0$	0	0	0	0	0	0	$\neq 0$
$\neq 0$	$\neq 0$	0	0	0	0	0	0
	$\neq 0$	$\neq 0$	0	0	0	0	0
		$\neq 0$	$\neq 0$	0	0	0	0
			$\neq 0$	$\neq 0$	0	0	0
				$\neq 0$	$\neq 0$	0	0
					$\neq 0$	$\neq 0$	0
						$\neq 0$	$\neq 0$

- Case 1:

$$\begin{cases} m_{00} \neq 0 \\ m_{0j} = 0, \text{for } 1 \leq j < n-1 \\ m_{10} \neq 0 \\ m_{1(n-1)} = 0 \end{cases} \quad (7)$$

$\Rightarrow (P_2)$ is true for every 2-tuple of columns $(0, j), \text{for } 1 \leq j < n$ (*1)

- Case 2:

$$\begin{cases} m_{ii} \neq 0, \text{for } 1 \leq i \leq n-1 \\ m_{ij} = 0, \text{for } 1 \leq i < j < n \end{cases} \quad (8)$$

$\Rightarrow (P_2)$ is true for every 2-tuple of columns $(i, j), \text{for } 1 \leq i \leq j < n$ (*2)

From (*1) and (*2), we conclude that (P_2) is true for every 2-tuple of columns. □

Given a matrix M that satisfies the conditions in Theorem 3.3. From Theorem 3.1 and 3.2, we infer that for any column vector $X = (x_0, ..., x_{n-1})^T \neq 0$, $\min\left\{wt(X) + wt(MX^T)\right\} \geq 3$

Theorem 3.3. *If $M_{n\times n}$ $(n \geq 5)$ satisfies the following conditions:*

(i) $M_{ij} \neq 0, \text{if } (i-j) \bmod n \leq 2$
(ii) $M_{ij} = 0, \text{if } (i < j) \wedge ((i-j) \bmod n > 2)$
(iii) $M_{i(i-3)} = 0, \text{for } 3 \leq i < n$
(iv) $M_{(n-1)0} = 0$

then
(R) : *for any k-tuple of columns $(k \in \{1, 2, 3\})$, there exist $d_1 \geq (4-k)$ rows so that in each of these d_1 rows, there is exactly one non-zero element.*

Proof. To prove (R), we need to prove the three following statements:
(R_1) If $k = 1$, for any 1-tuple of column, there are at least 3 rows such that each row has only one non-zero element in this column.
(R_2) If $k = 2$, for any 2-tuple of columns, there are at least 2 rows such that each row has only one non-zero element in these columns.
(R_3) If $k = 3$, for any 3-tuple of columns,there is at least 1 row such that this row has only one non-zero element in these columns.

Table 2. Form of matrix satisfying conditions of Theorem 3.3.

$\neq 0$	0	0	0	0	0	$\neq 0$	$\neq 0$
$\neq 0$	$\neq 0$	0	0	0	0	0	$\neq 0$
$\neq 0$	$\neq 0$	$\neq 0$	0	0	0	0	0
0	$\neq 0$	$\neq 0$	$\neq 0$	0	0	0	0
	0	$\neq 0$	$\neq 0$	$\neq 0$	0	0	0
		0	$\neq 0$	$\neq 0$	$\neq 0$	0	0
			0	$\neq 0$	$\neq 0$	$\neq 0$	0
				0	$\neq 0$	$\neq 0$	$\neq 0$
					0	$\neq 0$	$\neq 0$
0						0	$\neq 0$

Because M satisfies (i), we have (R_1). We prove that (R_2) and (R_3) are also true.

- Case 1:

$$\begin{cases} m_{00} \neq 0, m_{0j} = 0, \forall 1 \leq j < n-3 \\ m_{20} \neq 0, m_{2(n-2)} = m_{2(n-1)} = 0 \end{cases} \quad (9)$$

$\Rightarrow (R_2)$ is true for every 2-tuple of columns $(0, j)$, for $1 \leq j < n$ (**1)

- Case 2:

$$\begin{cases} m_{11} \neq 0, m_{1j} = 0, \forall 2 \leq j < n-2 \\ m_{21} \neq 0, m_{2(n-1)} = 0 \end{cases} \quad (10)$$

$\Rightarrow (R_2)$ is true for every 2-tuple of columns $(1, j)$, for $2 \leq j < n$ (**2)

- Case 3:

$$m_{ii} \neq 0, m_{ij} = 0, \text{ for } 2 \leq i < j \leq n-1 \quad (11)$$

$\Rightarrow (R_2)$ is true for every 2-tuple of columns (i, j), for $2 \leq i < j \leq n-1$ (**3)

From (**1), (**2), and (**3), we conclude that (R_2) is true for every 2-tuple of columns.

In order to prove (R_3), we have to prove that for any 3-tuple of columns (i_1, i_2, i_3),there is at least 1 row such that this row has only one non-zero element in these columns.

- Case 1:

$$\begin{cases} m_{00} \neq 0 \\ m_{01} = 0 \\ m_{0i_3} = 0, \text{for } 2 \leq i_3 \leq n-3 \end{cases} \quad (12)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{0, 1, i_3\}$, for $2 \leq i_3 \leq n-3$

- Case 2:

$$\begin{cases} m_{30} = 0 \\ m_{31} \neq 0 \\ m_{3i_3} = 0, \text{for } i_3 \in \{n-2, n-1\} \end{cases} \quad (13)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{0, 1, i_3\}$, for $i_3 \in \{n-2, n-1\}$

- Case 3:

$$\begin{cases} m_{10} \neq 0, \\ m_{12} = 0, \\ m_{1i_3} = 0, \text{for } 3 \leq i_3 \leq n-2 \end{cases} \quad (14)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{0, 2, i_3\}$, for $3 \leq i_3 \leq n-2$

- Case 4:

$$\begin{cases} m_{30} = 0, \\ m_{32} \neq 0, \\ m_{3(n-1)} = 0 \end{cases} \quad (15)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{0,2,n-1\}$

- Case 5:

$$\begin{cases} m_{20} \neq 0, \\ m_{2i_2} = 0, \text{for } 3 \leq i_2 \leq n-2 \\ m_{2(n-1)} = 0, \text{for } 4 \leq i_3 \leq n-1 \end{cases} \quad (16)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{0, i_2, i_3\}$ for $3 \leq i_2 < i_3 \leq n-1$

- Case 6:

$$\begin{cases} m_{11} \neq 0, \\ m_{12} = 0, \\ m_{1i_3} = 0, \text{for } 3 \leq i_3 \leq n-2 \end{cases} \quad (17)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{1, 2, i_3\}$ for $3 \leq i_3 \leq n-2$

- Case 7:

$$\begin{cases} m_{41} = 0, \\ m_{42} \neq 0, \\ m_{4(n-1)} = 0 \end{cases} \quad (18)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{1, 2,n-1\}$ for $3 \leq i_3 \leq n-2$

- Case 8:

$$\begin{cases} m_{11} = 0, \\ m_{1i_2} \neq 0, \text{for } 3 \leq i_2 \leq n-2 \\ m_{1i_3} = 0, \text{for } 4 \leq i_3 \leq n-2 \end{cases} \quad (19)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{1, i_2, i_3\}$ for $3 \leq i_2 < i_3 \leq n-2$

- Case 9:

$$\begin{cases} m_{21} = 0, \\ m_{2i_2} \neq 0, \text{for} 3 \leq i_2 \leq n-2 \\ m_{2(n-1)} = 0 \end{cases} \quad (20)$$

$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{1,i_2,n-1\}$ for $3 \leq i_2 \leq n-2$

- Case 10:

$$m_{i_1 i_1} \neq 0, m_{i_1 i_2} = 0, m_{i_1 i_3} = 0 \quad (21)$$

for $2 \leq i_1 < i_2 < i_3 \leq n-1$
$\Rightarrow (R_3)$ is true for every 3-tuple of columns $\{i_1, i_2, i_3\}$ for $2 \leq i_1 < i_2 < i_3 \leq n-1$

We now can conclude that (R_3) is true for every 3-tuple of columns. □

Given a matrix M that satisfies the conditions in Theorem 3.3. From Theorem 3.1 and 3.3, we infer that for any column vector $X = (x_0, ..., x_{n-1})^T \neq 0$, $\min\left\{wt(X) + wt(MX^T)\right\} \geq 4$

Theorem 3.4 (20-Theorem 2). *.Given a square matrix $A = (a_{ij})_{n \times n}$ over $\mathbb{K}(\mathbb{K} = \mathbb{N}, \mathbb{Z})$ such that each row and each column of A has only one odd number, we have*

- $\forall n \in \mathbb{N}^+, \det(A) \equiv 1 \pmod 2$
- $\forall n \in \mathbb{N}^+, a_{ij} \in \mathbb{Z}_{2p}$*, where p is a prime number,* $\det(A) \neq 0 \pmod{2p}$

From Theorem 3.4, we have:

$$\det(A) \equiv 1 (\text{mod} 2) \Rightarrow \det(A) \equiv 1 (\text{mod} 2^8) \quad (22)$$

$\Rightarrow \det(A)$ is odd $\Rightarrow \det(A) \in \mathbb{Z}_{2^8}^*$. Therefore A is a non-singular modular matrix (modular 2^8).

4. Specification of proposed cipher

4.1. *Structure of SSM*

SSM is a byte-oriented block cipher. In SSM, plaintext block of a fixed length (n bytes) is transformed into a corresponding ciphertext block (n bytes) using a given key k. This cipher key k is an invertible matrix $M_{n \times n}$ constructed using the strategy proposed in Theorem 3.2 or 3.3. The encryption process consists of multiple rounds of transformations. The number of rounds, denoted by Nr, is defined as follow:

$$Nr = 2 \left\lceil \frac{2n}{3\beta} \right\rceil + 2 \quad (23)$$

The round transformation of round r, denoted by ζ^r, consists of two main steps:

- Key-independent nonlinear substitution (denoted by φ): each byte of the state is substituted using a fixed non-linear S-box (cf. Sec. 4.2).
- Keyed linear transformation (denoted by λ): the whole state is linearly mixed using a $n \times n$ matrix derived from the cipher key k (cf. Sec. 4.2).

Figure 1 illustrates the structure of one round of SSM. As $\zeta^r[k] = \lambda[k] \circ \varphi$, we have:

$$SSM\,[k] = \zeta^{Nr-1}[k] \circ \ldots \circ \zeta^1[k] \circ \zeta^0[k] \qquad (24)$$

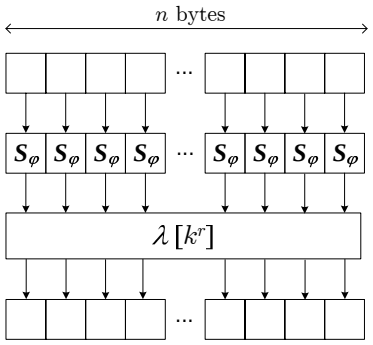

Fig. 1. Structure of one round of SSM

4.2. *Key-independent non-linear substitution φ*

In [1,21], the non-linear S-box of Rijndael is analysed to provide optimum cryptographic properties, such as maximum prop ratio [22] and maximum input-output correlation [22]. However, Rijndael S-box still has undesired property of simple description in GF(2^8) [13]. Its algebraic expression is sparse with only 9 terms, which leads to the concern of algebraic attacks [21,23] and interpolation attacks [24]. Hence, we use the improved S-box, called Gray S-box [25], in the key-independent non-linear substitution of SSM. Gray S-box inherits all good cryptographic properties of Rijndael S-box, including maximum prop ratio of 2^{-6} and maximum input-output correlation of 2^{-3}. Furthermore, the algebraic expression of Gray S-box achives sthe maximum number of terms (255).

In SSM, all operations of φ are processed in $GF(2)[x]/\langle\mu(x)\rangle$ where $\mu\,(x) = x^8 + x^4 + x^3 + x + 1$. Every block byte x is substituted using a fixed S-box constructed as follows:

(1) Apply the affine mapping over GF $(2)^8$ on the binary representation $(x_0, x_1, ..., x_7)$ of x. The result, denoted by $y = (y_0, y_1, ..., y_7)$, is defined as follows:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,1 \end{pmatrix} \times \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \qquad (25)$$

(2) Take the inverse mapping $z = y^{-1} \in GF(2)[x]/\langle\mu(x)\rangle$ with the extension $0^{-1} = 0$

(3) Apply the affine mapping over GF $(2)^8$ on the binary representation $(z_0, z_1, ..., z_7)$ of z. The result, denoted by $t = (t_0, t_1, ..., t_7)$, is defined as follows:

$$\begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,0\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,1\,1 \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \qquad (26)$$

The inverse mapping, denoted by φ^{-1}, use the inverse substitution table S-box S_φ^{-1} to substitute each byte of a state.

4.3. *Keyed linear transformation λ*

Keyed linear transformation *lambda* operates on the whole state. The state is considered as an n-byte column vector and multiplied (modulo 256) an $n \times n$ matrix M. In SSM, M is the cipher key. It should be noticed that this transformation is defined over $\mathbb{Z}_{256}^n$ instead of GF(2^8) as in the non-linear step.

5. Security strength against Differential and Linear Cryptanalysis

5.1. *Differential and Linear Cryptanalysis*

Differential cryptanalysis(DC) attacks [26] are possible if there are predictable difference propagations over T rounds (typically $T = Nr-1$ or $T = Nr-2$)

that have a prop ratio [22] (the relative amount of all input pairs that for the given input difference give rise to the output difference) significantly larger than 2^{1-m} if m is the block length (in bits).

Linear cryptanalysis(LC) attacks [27] are possible if there are predictable input-output correlations over T rounds (typically $T = Nr - 1$ or $T = Nr - 2$) significantly larger than $2^{-m/2}$ if m is the block length (in bits).

To prove the security of SSM against DC and LC, we adopt the approach used by J. Daemen and V. Rijmen in [1,22] with a single differential trail or a single linear trail. The proof is presented as follows:

- Determine the minimum number of active S-boxes [1] in any trail over multiple of two rounds. (cf. Sec. 5.2),
- Determine the upper bound of prop ratio of a differential trail and the upper bound of correlation of a linear trail over multiple of two rounds (cf. Sec. 5.3).

For DC, the active S-boxes in a round are determined by the nonzero bytes in the difference of the states at the input of a round. Let the pattern that specifies the positions of the active S-boxes be denoted by the term (*difference*) activity pattern and let the *(difference) element weight* be the number of active S-boxes in a pattern.

For LC, the active S-boxes in a round are determined by the nonzero bytes in the *selection vectors* at the input of a round. Let the pattern that specifies the positions of the active S-boxes be denoted by the term *(correlation) activity pattern* and let the *(correlation) element weight* $wt(a)$ be the number of active S-boxes in a pattern a.

5.2. *Number of Active S-boxes in 2r rounds*

Theorem 5.1. *Any trail over $2r$ rounds ($r > 0$) of SSM has at least $r \times \beta$ active S-boxes.*

Proof. Let $a^{(0)}$ be the activity pattern at the input of round 0, $a^{(i+1)}$ be the activity pattern at the output of round i.

As β is the branch number of λ, in round i for $0 \leq i < 2r$, the number of active S-boxes in $a^{(i)}$ and $a^{(i+1)}$ is lower bounded by β. To determine the number of active S-boxes over $2r$ rounds of SSM, we consider each group of two consecutive rounds:

$$\sum_{i=0}^{2r-1} wt\left(a^{(i)}\right) = \sum_{i=0}^{r-1} \left(wt\left(a^{(2i)}\right) + wt\left(a^{(2i+1)}\right)\right) \geq \sum_{i=0}^{r-1} \beta = r \times \beta$$

□

5.3. *Weight of differential and linear trails*

Theorem 5.2. *The maximum prop ratio of any trail over $2r$ rounds ($r > 0$) of SSM is upper bounded by $2^{-6\times r\times\beta}$.*

Proof. J. Daemen proved that the prop ratio of a differential trail can be approximated by the product of the prop ratios of its active S-boxes [22]. Basing on the fact that S-box used in SSM has the maximum prop ratio 2^{-6} and Theorem 5.1, we conclude that the prop ratio of a differential trail over $2r$ rounds of SSM is upper bounded by $2^{-6\times r\times\beta}$. □

Analogously, using the fact that the correlation of a linear trail can be approximated by the product of input-output correlations of its active S-boxes [22], we have the similar result for the upper bound of the maximum input-output correlation of any linear trail over $2r$ rounds of SSM. Basing on the fact that S-box used in SSM has the maximum input-output correlation 2^{-3} and Theorem 5.1, we have:

Theorem 5.3. *The maximum input-output correlation of any trail over $2r$ rounds ($r > 0$) of SSM is upper bounded by $2^{-3\times r\times\beta}$.*

Let $r_0 = \left\lceil \frac{2n}{3\beta} \right\rceil$. From Theorem 5.2 we conclude that the maximum prop ratio of any trail over $2r_0$ rounds of SSM is upper bounded by 2^{-8n}. This ensures the resistance of SSM against DC. From Theorem 5.3 we conclude that the maximum input-output correlation of any trail over $2r_0$ rounds of SSM is upper bounded by 2^{-4n}. This ensures the resistance of SSM against LC. Taking into account 2 rounds as the common security margin [28], the number of rounds Nr is $2r_0 + 2$ (cf. Eq. (23)).

6. Experimental Results

First we analyse the effect of increasing block size n on the number of rounds Nr for $\beta = 3$ and $\beta = 4$. Fig. 2 illustrates number of rounds Nr as a function

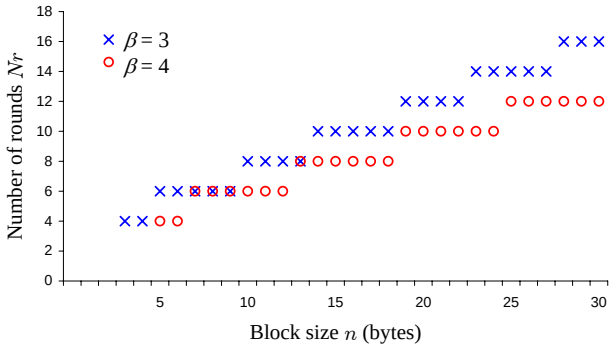

Fig. 2. Number of rounds Nr as a function of block size n for $\beta = 3$ and $\beta = 4$.

of block size n for $\beta = 3$ and $\beta = 4$. For SSM with $\beta = 4$, as the matrix multiplication has more diffusion capability thus SSM with $\beta = 4$ uses less rounds of transformations than SSM with $\beta = 3$.

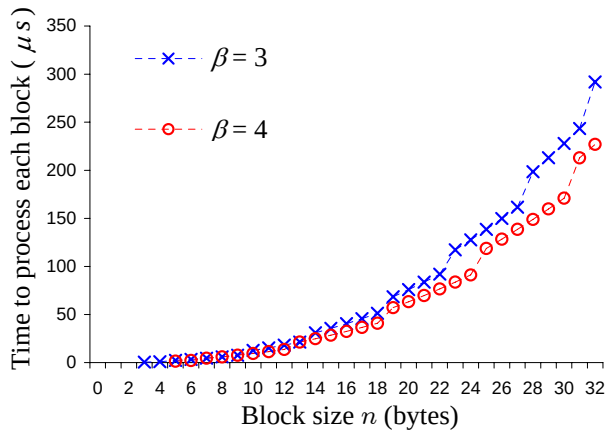

Fig. 3. Time to process each block (n bytes) in microseconds

To analyse the performance of SSM, our experiment (cf. Fig. 3) illustrates time to process each block (n bytes) in microseconds. This experiment was performed on QuadCore 3.2GHz system. As the decryption process of SSM consists of the same number of substitutions and the same number of matrix multiplications, decryption speed is approximately the same as encryption speed.

7. Conclusions

In this article, we present our proposed scalable cipher SSM constructed by combining non-linear substitution and matrix multiplication. By using matrix multiplication as diffusion layer, SSM supports unlimited block length and key length. With non-linear substitution, SSM eliminates limitation of most matrix ciphers with only linear components. The security of SSM against differential and linear cryptanalysis is proved independently of specific key length and block length. This ensures the security of SSM for any specific key length and block length.

We also propose two strategies to construct easily an $n \times n$ matrix with branch number of no less than a threshold β for $beta = 3$ or 4. By applying the criterion proposed in Theorem 2 of [20], the generated matrix is invertible in $\mathbb{Z}_{256}^n$. Thus we can easily generate abundantly invertible matrices of any size with certain diffusion capability to use as cipher keys in SSM. This result supports our proposal to use diffusion layer that is not neccessary to provide maximum diffusion to create secure ciphers.

Our proposal of SSM and two strategies to construct matrices with certain diffusion capability open new problems to be explored. Currently we are studying other criteria and strategies to create diffusion layers with any given branch number. Besides, we will apply our proposed strategies to construct matrices into cipher schemes other than SPN to create nem secure ciphers. Futhermore, we also study specific criteria to generate optimum matrices to be used in specific hardware or system.

References

1. J. Daemen and V. Rijmen, "AES proposal: Rijndael." AES algorithm submission, 1999.
2. V. Rijmen and P.S.L.M. Barreto, "The Khazad legacy-level block cipher," 2000.
3. P.S.L.M. Baretto and V. Rijmen, "The Anubis block cipher," 2000.
4. D. Kwon, "Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis," Selected Areas in Cryptography, pp.39–56, Springer Berlin / Heidelberg, 2000.
5. D. Kwon, "New block cipher: ARIA," CISC 2003, LNCS, vol.2971, pp.432–445, Springer Berlin / Heidelberg, 2003.
6. Toshiba Corporation, "Specification on a block cipher: Hierocrypt-L1," 2000.
7. Toshiba Corporation, "Specification of Hierocrypt-3," 2000.
8. L.S. Hill, "Cryptography in an algebraic alphabet," The American Mathematical Monthly 36, pp.306–312, 1929.
9. S. Saeednia, "How to make the hill cipher secure," Cryptologia, vol.24(4), pp.353–370, 2000.
10. V. Sastry and N.R. Shankar, "Modified hill cipher with interlacing and iteration," Journal of Computer

Science, vol.3(11), pp.854–859, 2007.
11. V. Sastry and N.R. Shankar, "Modified hill cipher for a large block of plaintext with interlacing and iteration," Journal of Computer Science, vol.4(1), pp.15–20, 2008.
12. J. Kam and G. Davida, "Structured design of substitution-permutation encryption networks," IEEE Transactions on Computers, vol.C-28, no.10, pp.747–753, 1979.
13. J. Daemen, V. Rijmen, B. Preneel, A. Bosselaers, and E.D. Win, "The cipher SHARK," FSE 1996, LNCS, vol.1039, pp.99 – 111, 1996.
14. J. Daemen, L.R. Knudsen, and V. Rijmen, "The block cipher Square," Fast Software Encryption, LNCS, vol.1267, pp.149–165, 1997.
15. J. Borst, "The block cipher: GrandCru," 2000.
16. R. Rivest, A. Shamir, and L. Adleman., "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol.21(2), pp.120–126, 1978.
17. W. Diffie and M.E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol.IT-22, pp.644–654, 1976.
18. C.E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol.28(4), pp.656–715, 1949.
19. National Institute of Standards and Technology, "FIPS 46, Data Encryption Standard (DES)," 1977.
20. T.N. Bao, "On generating key-matrix for matrix cipher and applications," RIVF, 2008.
21. N. Ferguson, R. Schroeppel, and D. Whiting, "The inverse S-box, non-linear polynomial relations and cryptanalysis of block ciphers," AES-2004, LNCS, vol.3373, pp.170–188, 2004.
22. J. Daemen, Cipher and hash function design strategies based on linear and differential cryptanalysis, Ph.D. thesis, K.U.Leuven, 1995.
23. N.T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," ASIACRYPT 2002, LNCS, vol.2501, pp.267–287, 2002.
24. T. Jakobsen and L.R. Knudsen, "The interpolation attack on block ciphers," Fast Software Encryption, LNCS, vol.1267, pp.28–40, Springer-Verlag, 1997.
25. M.T. Tran, D.K. Bui, and A.D. Duong, "Gray s-box for advanced encryption standard," 2008 International Conference on Computational Intelligence and Security (CIS'08), 2008.
26. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," CRYPT0 90, LNCS, vol.537, pp.2–21, 1990.
27. M. Matsui, "Linear cryptanalysis method for DES cipher," EUROCRYPT 93, LNCS, vol.765, pp.386–397, 1994.
28. L. Keliher, "Refined analysis of bounds related to linear and differential cryptanalysis for the AES," AES-2004, LNCS, vol.3373, pp.42–57, 2004.