A SCALABLE BLOCK CIPHER DESIGN USING FILTER BANKS OVER FINITE FIELDS

S. Saraireh and M. Benaisa
Electronic and Electrical Engineering Department, University of Sheffield, UK

ABSTRACT

A scalable block cipher based on a filter bank structure over $GF(2^3)$ is proposed. The filter bank structure is used to introduce the diffusion during the circular convolution process between the filters coefficients (which are generated from the key) and the plaintext. The confusion is achieved by the mixing between the analysis filter bank and a novel addition mod $2^n$ and XOR scheme. The proposed cipher is scalable in both block and key lengths. The cipher is shown to be secure against differential and linear cryptanalysis and of lesser complexity than the AES. The proposed cipher structure enables security versus complexity versus performance trade-offs to be made, an increasingly important aspect of security in communications systems.

Index Terms—Block Cipher, Filter Banks, Finite Fields, Scalability

1 INTRODUCTION

Increasingly, scalability is becoming an important driver for communication systems to enable reconfiguration to match a particular level of quality of service requirement. In these systems scalable security remains a major challenge. Scalability in cryptosystems enables an encryption scheme to be adjusted, in a specific application, in terms of security and performance requirements [1]. Scalability is considered as the most common drawback of existing block ciphers. The Rijndael AES [2] for example, although supports 3 key lengths still deals with a fixed number of block and key lengths and a specific number of rounds for these to achieve its level of security.

A key consideration in scalable cipher design is the tradeoff security versus complexity versus performance. This trade-off in turn depends, at the cipher design stage, on the diffusion-confusion rates trade offs that can be made without compromising security. Filter banks/wavelets over finite fields have been proposed for implementing error control coding systems [3] and cryptosystems [4-6]. The attractiveness of filter bank structures for implementing cryptography primitives can be related to the following desirable features:

a) Design simplicity, since based on the established design of digital filters; this also offers scope for high speed implementations in hardware and software and potentially lower resources in hardware.

b) Potential for high security with a lower number of rounds due to their intrinsic high diffusion rate if suitable confusion schemes can be added.

c) Encryption performed by the analysis filter bank over finite field, so the decryption process can be done by running the synthesis filter bank. The main operation for the decryption process, as shown in Fig. (2) is the circular convolution between the synthesis filter bank coefficients and the encrypted plaintext (ciphertext).

The user key determines the filters coefficients. These are generated from a random number (key). The most important property for such system is the perfect reconstruction property that the analysis and synthesis filter banks must satisfy together with the method used to generate these filters.

The implementation of the two bands filter bank is based on the implementation of two types building blocks $D(z)$ and $S(z)$ [7], where $D(z)$ is called the degree-one PU building block and it is represented mathematically as follow:

\[ D(z) = d(0) + z^{-1}d(1)I + z^{-1}I_{v}I_{v}^T + z^{-2}I_{v}I_{v}^T \]

where $I_{v} = v^T v \neq 0$, and $v = [a ~ b]^T$, which is a vector of length two and $I_{v}$ is always square, $I_{v}$ is nonzero when $a \neq b$ [7]. $S(z)$ is called a degree $2 \tau$ elementary building block and it is represented as follow [7]:

\[ S_{\tau, \gamma}(z) = \zeta(I + J) + z^{-\gamma}I + z^{-2\gamma} \zeta(I + J) \]

where $\zeta \neq 0$ is a scalar in $GF(2^n)$, $\tau$ is any positive integer,
I is the identity matrix and J is the exchange matrix. So, 
\[ I + J = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \] \[ \text{[7]}. \]

These building blocks are used to implement the polyphase matrix (E(z)) of the two bands filter bank, which is used to generate the filters for the filter bank system:
\[ H_s(z) = E_{\text{in}}(z^2) + z^{-1} E_{\text{in}}(z^2), \quad s = 0, 1 \] \[ \text{(3)} \]

The basic process of the finite field analysis and synthesis filter bank system is the convolution over \( GF(2^n) \). The convolution is a linear operation between the coefficients of the analysis filter bank and the plaintext. It is employed to introduce the high diffusion rate (permutation) for the cipher resulting in the plaintext transformed into a sequence similar to a white noise sequence [4]. The input block length (plaintext) is the same as the output block length (ciphertext) in the block cipher mode. Consequently, circular convolution is applied in this case.

The necessary nonlinearity (confusion) in the proposed cipher is achieved via the integer addition \( \mod 2^n \), XOR based S-box configuration shown in Fig.3 for encryption and Fig.4 for decryption where +/- Represents integer Add/Subst. \( \mod 2^n \), \( \oplus (\text{XOR}) \), \( <<< \text{left rotation} \) that depends on the s-box size.

This combination introduces a good diffusion and confusion rates [8] whilst enabling scalability with reduced complexity by changing the number of stages and the s-box size to match a required level of security at required levels of complexity. In Fig.1, the nonlinearity is introduced through the integer addition operation [9] due to the carry function [10]. Integer addition is used instead of XOR to increase the diffusion process, and improve nonlinearity [11]. To satisfy the perfect reconstruction in the decryption side the addition \( \mod 2^n \) is simply replaced by subtraction \( \mod 2^n \) with a small arrangement process as shown in Fig. (2). Also the proposed structure matches directly a scalable filter band structure and does not involve any feedback loop as in [4, 5]. This enables the overall cipher to be scalable without additional complexity.

The key schedule is scalable, based on the same addition \( \mod 2^n \) and XOR combination. The \( N \) bits key length is first divided into two halves \( (n = N/2) \). Each of the halves is then applied to one of the branches in Fig. (1). The rotation process depends on the length of the input data \( (n) \). It should be close to the center of the input value and relatively prime to it. The output is then applied to a random round constant to eliminate the similarity and avoid round and round transformations symmetry and guard against a slide attack.

3 SECURITY ANALYSIS

The most common used statistical tests to examine the diffusion property of an s-box are: avalanche criterion, strict avalanche criterion (SAC), and bit independent criterion (BIC). While the confusion property of an s-box can be examined by implementing the XOR distribution table and the linear approximation table (LAT). To study the randomness of the overall block cipher the avalanche weight distribution (AWD) can be carried out. AWD is considered as a simple and fast criterion to study the diffusion and confusion properties of a block cipher. AWD is based on the histogram of the Hamming weight of the avalanche vectors of several pairs of plaintexts. In order to satisfy the avalanche weight distribution, the histogram of the Hamming weight of the avalanche vectors should be a binomial distribution around \((m/2)\), where \( m \) is the length of the avalanche vector (block length). As mentioned earlier, the proposed s-box is scalable as it supports different s-box sizes with different number of stages. In this paper, the analysis is performed for a \( 16 \times 16 \) s-box with different number of stages; the input into each branch comprises 8 bits and the left rotation is 5 bits. The results obtained are shown in Tables (1–2).
In block ciphers, the differential branch number \( \beta_d \) is defined as:

\[
\beta_d = \min_{\Delta P \neq 0} (H(\Delta P) + H(f(\Delta P)))
\]

(4)

where \( \Delta P \) is an input difference into the block cipher and \( f(\Delta P) \) is an output difference from the block cipher. While \( H(\cdot) \) is the Hamming weight of the vector, which is equal to the number of nonzero characters in the vector [13].

The differential branch number for the cipher with 16 bytes key and block length is calculated by using eq. (4) with one nonzero byte input, in this case, the Hamming weight of the input difference is 1, and the Hamming weight of the output difference is 16 due to the convolution process, the branch number is therefore 17, which is the maximum value that the cipher can get, therefore, the cipher has an optimum diffusion layer.

The maximum differential characteristic probability for an \( r \)-round SPN cipher is upper bounded by \((p_1)^{r/2}\). The differential characteristic probability for one round of the proposed cipher would therefore be \((2^{-11.67805})^{1/17} = 2^{-198.52685}\) with seven stages s-box, and it is \((2^{-10.58962})^{1/17} = 2^{-188.5827}\) with eight stages s-box, while it is \((2^{-121.18722})^{1/17} = 2^{-198.52685}\) with nine stages s-box; thus requiring much more than the available \((2^{128})\) plaintext, and as a result secure against differential cryptanalysis with seven, eight or nine stages s-boxes.

To study the resistance of the proposed block cipher against linear cryptanalysis, the linear approximation tables (LATs) [14] of the s-boxes are implemented and the corresponding maximum linear probabilities \( (p_i)^{r/2} \) obtained are: \(2^{-7.12866}, 2^{-9.176978}, \) and \(2^{-10.58962}\) for seven, eight and nine stages s-boxes, respectively.

The linear branch number is the same as the differential branch number, so it is 17 for 16 bytes block and key length. The maximum linear characteristic probability for an \( r \)-round SPN cipher is again upper bounded by \((p_1)^{r/2}\).

The linear characteristic probability for one round block cipher is:

\[
(2^{-7.12866})^{1/17} = 2^{-121.18722}
\]

with a seven stages s-box, while it is \((2^{-9.176978})^{1/17} = 2^{-156.008626}\) with an eight stages s-box and it is \((2^{-10.58962})^{1/17} = 2^{-180.0232}\) with a nine stages s-box.

The linear characteristic probabilities for the proposed block cipher is therefore upper bounded by \((p_1)^{r/2}\).

To investigate the security of the proposed block cipher against the differential cryptanalysis [12], the maximum differential probability \( (p_i) \) of the s-box, which depends on the maximum value in the XOR distribution table is first evaluated; the maximum differential probability values are calculated as \(2^{-8.8707037}\) for a seven stages s-box, \(2^{-11.09311}\) for an eight stages s-box, and \(2^{-11.67805}\) for a nine stages s-box. The next step is to find the minimum number of differential active s-boxes of the cipher (differential branch number). A differential active s-box is defined as an s-box given a nonzero input difference [13]. If the s-box is bijective, then the s-boxes that give nonzero output difference are also considered as differential active s-boxes [13].

The relative error values obtained for the s-boxes with seven, eight and nine stages are very small; reflecting the high diffusion rate that the proposed s-boxes exhibit. The results show that, as expected, the number of stages is increased, the diffusion rate is increased, and the relative absolute error values are decreased, due to the additional processing that affects the input data.

The maximum values obtained in the XOR distribution tables \( (XOR_{\text{max}}) \) and the maximum values obtained in the linear approximation tables \( (LAT_{\text{max}}) \) are very low compared to the s-box dimension \((2^8 \times 2^8)\), resulting in very small maximum differential and linear probabilities. Note that, as the number of stages is increased, the values of \(XOR_{\text{max}}\) and \(LAT_{\text{max}}\) are decreased as expected, due to the additional nonlinear process that applies to the input data.

The AWD of the proposed block cipher was evaluated for different s-boxes and different block lengths using 100000 random plaintexts on one round of the proposed block cipher. The block lengths are 192, 128 and 160 bits for seven, eight and nine stages s-boxes. The obtained histograms of the Hamming weight (HW) of the avalanche vectors are binomial distributions around the values of the block lengths 96, 64 and 80, respectively.

Table (1): S-Boxes Diffusion Results

<table>
<thead>
<tr>
<th>S-Box</th>
<th>(\varepsilon_{\text{AVAL}})</th>
<th>(\varepsilon_{\text{BIC}})</th>
<th>(\varepsilon_{\text{SAC}})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seven Stage S-Box</td>
<td>0.0030</td>
<td>0.0206</td>
<td>0.0801</td>
</tr>
<tr>
<td>Eight Stage S-Box</td>
<td>0.0020</td>
<td>0.0165</td>
<td>0.0197</td>
</tr>
<tr>
<td>Nine Stage S-Box</td>
<td>0.0031</td>
<td>0.0148</td>
<td>0.0179</td>
</tr>
</tbody>
</table>

Table (2): S-Boxes Confusion Results

<table>
<thead>
<tr>
<th>S-box</th>
<th>(XOR_{\text{max}})</th>
<th>(LAT_{\text{max}})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seven Stage S-Box</td>
<td>140</td>
<td>2770</td>
</tr>
<tr>
<td>Eight Stage S-Box</td>
<td>30</td>
<td>1362</td>
</tr>
<tr>
<td>Nine Stage S-Box</td>
<td>20</td>
<td>814</td>
</tr>
</tbody>
</table>

The relative error values obtained for the s-boxes with seven, eight and nine stages are very small; reflecting the high diffusion rate that the proposed s-boxes exhibit. The results show that, as expected, the number of stages is increased, the diffusion rate is increased, and the relative absolute error values are decreased, due to the additional processing that affects the input data.
cipher with any of the above s-boxes are significantly larger than $2^{64} (2^{128/2})$, again requiring much more than the available $(2^{128})$ plaintexts. Although the above analysis was performed for a single round, it is important to note that, to increase the security margin and avoid key recovery attacks, it is essential to increase the number of rounds to at least two rounds.

### 4 SCALABILITY AND COMPLEXITY

Table (3) shows some results for different combinations of key and block sizes for the encryption process with a nine stages s-box. The results indicate that the cipher is scalable, and that optimum security at minimum complexity is obtained when the block size equal to the key size. The number of operations and amount of storage required for the algorithm although not perfect provide an indication about the potential implementation complexity of the cipher in software and hardware. Table (4) shows a complexity comparison between the proposed cipher and the AES cipher with the same key and block length in terms of table lookups and number of logical operations normalised per bit. It can be seen from the results obtained that the complexity of the filter bank block cipher is less than that of the AES [15] when the number of rounds is taken into account.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>80</td>
<td>4.25</td>
<td>2$^{232.9712}$</td>
<td>2$^{256.9171}$</td>
</tr>
<tr>
<td>80</td>
<td>128</td>
<td>5.75</td>
<td>2$^{232.9712}$</td>
<td>2$^{256.9171}$</td>
</tr>
<tr>
<td>128</td>
<td>128</td>
<td>5.75</td>
<td>2$^{560.0464}$</td>
<td>2$^{397.0537}$</td>
</tr>
<tr>
<td>128</td>
<td>192</td>
<td>7.75</td>
<td>2$^{560.0464}$</td>
<td>2$^{397.0537}$</td>
</tr>
<tr>
<td>176</td>
<td>176</td>
<td>7.25</td>
<td>2$^{487.1216}$</td>
<td>2$^{537.1903}$</td>
</tr>
<tr>
<td>176</td>
<td>192</td>
<td>7.75</td>
<td>2$^{487.1216}$</td>
<td>2$^{537.1903}$</td>
</tr>
</tbody>
</table>

Table (4): Complexity comparison.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>AES Filter bank Enc.</th>
<th>AES Filter bank Dec.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rounds</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>Block size (bits)</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Word size (bits)</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Key size (bits)</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Table lookups/Table size (bits)</td>
<td>160(8*32)</td>
<td>0</td>
</tr>
<tr>
<td>Shift/Rotation/multiplication</td>
<td>30</td>
<td>530</td>
</tr>
<tr>
<td>XOR, ADD, SUB.(bit size)</td>
<td>11 (128 bit), 120 (32 bit)</td>
<td>736</td>
</tr>
<tr>
<td>Total TLUs (8 bits)</td>
<td>160</td>
<td>0</td>
</tr>
<tr>
<td>Total logical Ops (8-bit)</td>
<td>656</td>
<td>736</td>
</tr>
<tr>
<td>TLUs per bit</td>
<td>1.25</td>
<td>0</td>
</tr>
<tr>
<td>Logical Ops per bit</td>
<td>5.125</td>
<td>5.75</td>
</tr>
</tbody>
</table>

### 5 CONCLUSIONS

A scalable filter bank block cipher structure has been developed and analyzed. The cipher satisfies the principles of security and is secure against linear and differential cryptanalysis. The complexity of the block cipher is comparable with the complexity of the AES with the same key and block length but requires fewer rounds. The cipher structure enables security versus complexity versus performance trade-offs to be made for a given application, an increasingly important requirement in current and future communication systems.

### 6 REFERENCES