Recursive Diffusion Layers for Block Ciphers and Hash Functions

Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala and Pouyan Sepehrdad

Isfahan University of Technology, Isfahan, Iran
Isfahan University, Isfahan, Iran
EPFL, Lausanne, Switzerland

Happy Persian New Year!

Outline

- Lightweight Algorithms and Diffusion Layers
- Designing A Recursive Diffusion Layer
- Designing A Diffusion Layer with One Linear Function
- Designing A Diffusion Layer with Two Linear Functions
- Conclusion

Lightweight Algorithms and Diffusion Layers

- Most block ciphers: A round consists of confusion and diffusion layers.
- The confusion layer: often uses small S-boxes.
- The diffusion layer: plays an efficacious role in providing resistance against DC and LC.
- Diffusion layers must
  - have large branch numbers.
  - be efficient, both the layer and its reverse.

Lightweight Algorithms and Diffusion Layers

- Lightweight block ciphers:
  - New ciphers appear everyday in the literature.
  - Compete over the throughput and GE.
  - Not providing the same level of security (LC, DC, AC).
  - Does the comparison make sense?

- Designing lightweight and efficient diffusion layers:
  - Efficient and perfect recursive Feistel-like diffusion layers.
  - We design one without any finite fields operations.
  - Only have “XOR”s and “Shift” or “Rotations”.
  - LED and PHOTON: a nice and efficient MDS diffusion layer.

Designing A Recursive Diffusion Layer

$$D : \begin{cases} y_0 = x_0 \oplus F_0(x_1, x_2, \ldots, x_{s-1}) \\ y_1 = x_1 \oplus F_1(x_2, x_3, \ldots, x_{s-1}, y_0) \\ \vdots \\ y_{s-1} = x_{s-1} \oplus F_{s-1}(y_0, y_1, \ldots, y_{s-2}) \end{cases}$$

- Maximal branch number
- Length of the input words be changeable
- Have a very simple inverse
- An efficient linear functions F.

Designing A Recursive Diffusion Layer

$$D : \begin{cases} y_0 = x_0 \oplus F_0(x_1, x_2, \ldots, x_{s-1}) \\ y_1 = x_1 \oplus F_1(x_2, x_3, \ldots, x_{s-1}, y_0) \\ \vdots \\ y_{s-1} = x_{s-1} \oplus F_{s-1}(y_0, y_1, \ldots, y_{s-2}) \end{cases}$$

$$D^{-1} : \begin{cases} x_{s-1} = y_{s-1} \oplus F_{s-1}(y_0, y_1, \ldots, y_{s-2}) \\ x_{s-2} = y_{s-2} \oplus F_{s-2}(x_{s-1}, y_0, \ldots, y_{s-3}) \\ \vdots \\ x_0 = y_0 \oplus F_0(x_1, x_2, \ldots, x_{s-1}) \end{cases}$$

Some Instances of Recursive Diffusion Layers

- Feistel with a linear F $$D : \begin{cases} y_0 = x_0 \oplus L(x_1) \\ y_1 = x_1 \oplus L(y_0) \end{cases}$$
- Salsa20 (non linear) $$D : \begin{cases} y_1 = x_1 \oplus ((x_0 + x_3) <<< 7) \\ y_2 = x_2 \oplus ((x_0 + y_1) <<< 9) \\ y_3 = x_3 \oplus ((y_1 + y_2) <<< 13) \\ y_0 = x_0 \oplus ((y_2 + y_3) <<< 18) \end{cases}$$
- PHOTON matrix $$\mathbf{B} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 1 & 4 \end{pmatrix} \Rightarrow \mathbf{B}^4 = \begin{pmatrix} 1 & 2 & 1 & 4 \\ 4 & 9 & 6 & 17 \\ 17 & 38 & 24 & 66 \\ 66 & 149 & 100 & 11 \end{pmatrix}$$

The Proposed Regular s n-bit Words Diffusion Layer

1: Input : s n-bit words $x_0, \ldots, x_{s-1}$
2: Output : s n-bit words $y_0, \ldots, x_{s-1}$
3: **for** $i = 0$ to $s - 1$ **do**
4: $\quad y_i = x_i$
5: **end for**
6: **for** $i = 0$ to $s - 1$ **do**
7: $$y_i = \bigoplus_{j=0}^{s-1} \alpha_{[(j-i) \mod s]} y_j \oplus L \left(\bigoplus_{j=0}^{s-1} \beta_{[(j-i) \mod s]} y_j \right)$$
8: **end for**

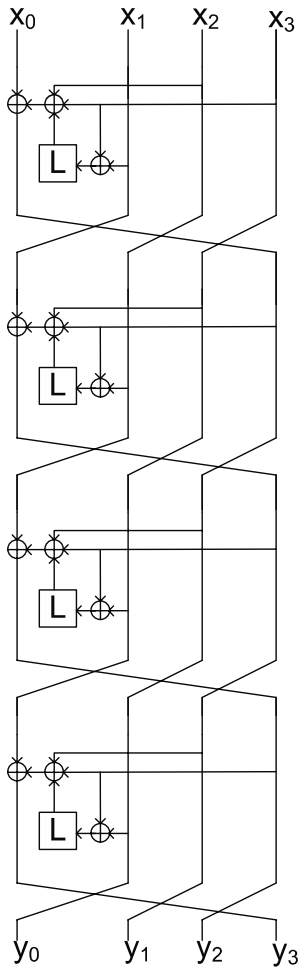
- In the main pseudo code: $F_i(x_1, x_2, \ldots, x_{s-1}) = F_0(x_1, x_2, \ldots, x_{s-1})$

$$F_i(x_1, x_2, \ldots, x_{s-1}) = \bigoplus_{j=1}^{s-1} \alpha_j x_j \oplus L \left(\bigoplus_{j=1}^{s-1} \beta_j x_j \right)$$

A Regular 4 × 4 In/Out Diffusion Layer with Perfect Diffusion

$$D:\begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases} \Rightarrow \quad D^{-1}:\begin{cases} x_3 = y_3 \oplus y_2 \oplus y_1 \oplus L(y_0 \oplus y_2) \\ x_2 = y_2 \oplus y_1 \oplus y_0 \oplus L(x_3 \oplus y_1) \\ x_1 = y_1 \oplus y_0 \oplus x_3 \oplus L(x_2 \oplus y_0) \\ x_0 = y_0 \oplus x_3 \oplus x_2 \oplus L(x_1 \oplus x_3) \end{cases}$$

A Regular 4 × 4 In/Out Diffusion Layer with Perfect Diffusion



Conditions on L: Maximal Branch Number

- Outputs based on inputs

$$D: \begin{cases} y_0 = x_0 \oplus L(x_1) \oplus x_2 \oplus x_3 \oplus L(x_3) \\ y_1 = x_0 \oplus L(x_0) \oplus x_1 \oplus L(x_1) \oplus L^2(x_1) \oplus x_2 \oplus L^2(x_3) \\ y_2 = L^2(x_0) \oplus x_1 \oplus L(x_1) \oplus L^3(x_1) \oplus x_2 \oplus L(x_2) \oplus x_3 \oplus L^2(x_3) \oplus L^3(x_3) \\ y_3 = x_0 \oplus L^2(x_0) \oplus L^3(x_0) \oplus L(x_1) \oplus L^2(x_1) \oplus L^3(x_1) \oplus L^4(x_1) \\ \qquad \oplus L(x_2) \oplus L^2(x_2) \oplus L^2(x_3) \oplus L^4(x_3) \end{cases}$$

- The linear functions must be invertible for maximal branch number:

$$\begin{cases} L(x) \\ x \oplus L(x) \\ x \oplus L^3(x) \\ x \oplus L^7(x) \end{cases}$$

$L(x) = (x \oplus (x \ll 3)) \gg 1$

Some Linear Functions

- Large number of linear functions satisfying the conditions, some are:

word size	Some linear functions L
4	$L(x) = (x \oplus x \ll 3) \oplus 1$
8	$L(x) = (x \oplus (x \,\&\, 0x2) \ll 1) \oplus 1$
16	$L(x) = (x \oplus x \ll 15) \oplus 1$
32	$L(x) = (x \oplus x \ll 31) \oplus 15$ or $L(x) = (x \oplus 24) \oplus (x \,\&\, 0xFF)$
64	$L(x) = (x \oplus x \ll 63) \oplus 1$ or $L(x) = (x \oplus 8) \oplus (x \,\&\, 0xFFFF)$

- Without any circular shift:

word size	Sample linear functions L
32	$L(x) = (x \ll 3) \oplus (x \gg 1)$
64	$L(x) = (x \ll 15) \oplus (x \gg 1)$

Replacement of Some Diffusion Layers

- MDS_H of Hierocrypt
  - Performance two times better
- Binary matrix of MMB
  - Branch number of the MMB diffusion layer increases to 5.
    - prevents the attacks [SAC'09] presented on this block cipher.
  - Performance is decreased by 10%.
- PHOTON
  - If L(x)=2x in GF(2^4) , the matrix is:

$$B=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&2&1&3\end{pmatrix}\Rightarrow B^4=\begin{pmatrix}1&2&1&3\\3&7&1&4\\4&11&3&13\\13&30&6&20\end{pmatrix}$$

All Other Regular Diffusion Layers

For s > 4, no diffusion layer was found with only one linear function.

All Other Regular Diffusion Layers

s	Diffusion Layer	Function that must be invertible
2	$D: \begin{cases} y_0 = x_0 \oplus L(x_1) \\ y_1 = x_1 \oplus L(y_0) \end{cases}$	$L(x)$ and $x \oplus L(x)$
3	$D: \begin{cases} y_0 = x_0 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$ and $x \oplus L^3(x)$
3	$D: \begin{cases} y_0 = x_0 \oplus x_1 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus x_2 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
3	$D: \begin{cases} y_0 = x_0 \oplus x_2 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_1 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
3	$D: \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_1 \oplus x_2) \\ y_1 = x_1 \oplus x_2 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(y_0 \oplus y_1) \end{cases}$	$L(x)$, $x \oplus L(x)$, and $x \oplus L^3(x)$
4	$D: \begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
4	$D: \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_2 \oplus x_3 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus y_0 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_0 \oplus y_1 \oplus L(y_0 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$ and $x \oplus L^7(x)$
4	$D: \begin{cases} y_0 = x_0 \oplus x_2 \oplus L(x_1 \oplus x_2 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus L(x_2 \oplus x_3 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus L(x_3 \oplus y_0 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus L(y_0 \oplus y_1 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$, $x \oplus L^7(x)$ and $x \oplus L^{15}(x)$
4	$D: \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_3 \oplus L(x_1 \oplus x_2 \oplus x_3) \\ y_1 = x_1 \oplus x_2 \oplus y_0 \oplus L(x_2 \oplus x_3 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus \oplus y_1 \oplus L(x_3 \oplus y_0 \oplus y_1) \\ y_3 = x_3 \oplus y_0 \oplus y_2 \oplus L(y_0 \oplus y_1 \oplus y_2) \end{cases}$	$L(x)$, $x \oplus L(x)$, $x \oplus L^3(x)$, $x \oplus L^7(x)$ and $x \oplus L^{15}(x)$

Non-regular Recursive Diffusion Layers

- In the non-regular diffusion layers: F_i's are different.
  - Use only one linear function.

1: Input : s n-bit words $x_0, \ldots, x_{s-1}$
2: Output : s n-bit words $y_0, \ldots, x_{s-1}$
3: **for** $i = 0$ to $s - 1$ **do**
4: $\quad y_i = x_i$
5: **end for**
6: **for** $i = 0$ to $s - 1$ **do**
7: $$\quad y_i = y_i \oplus \left(\bigoplus_{j=0, j\neq i}^{s-1} A_{i,j} y_j \right) \oplus L \left(\bigoplus_{j=0, j\neq i}^{s-1} B_{i,j} y_j \right)$$
8: **end for**

- The space for a complete search is 2^{2s^2} for an s input/output diffusion layer.

Non-regular Recursive Diffusion Layers

- After a complete search
  - For s = 3, the one with the least number of XORs:

$$\mathbf{D}: \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \\ y_1 = x_1 \oplus x_2 \oplus L(y_0 \oplus x_2) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \end{cases}$$

  - For s = 4, the one with the least number of XORs:

$$\mathbf{D}: \begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus y_0 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0) \end{cases}$$

- For s > 4, a complete search is too costly.

Regular Recursive Diffusion Layers with Two Linear Functions

1: Input : s n-bit words $x_0, \ldots, x_{s-1}$
2: Output : s n-bit words $y_0, \ldots, x_{s-1}$
3: **for** $i = 0$ to $s-1$ **do**
4: $\quad y_i = x_i$
5: **end for**
6: **for** $i = 0$ to $s-1$ **do**
7: $$y_i = \bigoplus_{j=0}^{s-1} \alpha_{[(j-i) \mod s]} y_j \oplus L_1 \left(\bigoplus_{j=0}^{s-1} \beta_{[(j-i) \mod s]} y_j \right) \oplus L_2 \left(\bigoplus_{j=0}^{s-1} \gamma_{[(j-i) \mod s]} y_j \right)$$
8: **end for**

- If L_1 and L_2 do not have any relation, the analysis is hard.

$$L_2(x) = L_1^2(x) \quad \text{or} \quad L_2(x) = L_1^{-1}(x)$$

Regular Diffusion Layer for s > 4

s	y_0 in a perfect diffusion Layer
5	$y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_4) \oplus L^2(x_1)$
5	$y_0 = L^{-1}(x_4) \oplus x_0 \oplus x_2 \oplus L(x_1 \oplus x_3 \oplus x_4)$
6	$y_0 = x_0 \oplus x_5 \oplus L(x_3 \oplus x_5) \oplus L^2(x_1 \oplus x_2 \oplus x_4)$
6	$y_0 = L^{-1}(x_2 \oplus x_5) \oplus x_0 \oplus x_3 \oplus L(x_1 \oplus x_3 \oplus x_4 \oplus x_5)$
7	$y_0 = x_0 \oplus x_2 \oplus x_4 \oplus L(x_3) \oplus L^2(x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6)$
7	$y_0 = L^{-1}(x_1 \oplus x_3 \oplus x_6) \oplus x_0 \oplus x_6 \oplus L(x_1 \oplus x_2 \oplus x_4 \oplus x_5)$
8	$y_0 = x_0 \oplus x_1 \oplus x_3 \oplus x_4 \oplus L(x_2 \oplus x_3 \oplus x_5) \oplus L^2(x_1 \oplus x_5 \oplus x_6 \oplus x_7)$
8	$y_0 = L^{-1}(x_3 \oplus x_4 \oplus x_7) \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_4 \oplus L(x_1 \oplus x_5 \oplus x_6 \oplus x_7)$

- The linear functions which must be invertible:

$$
\begin{array}{lll}
L(x) & I \oplus L(x) & I \oplus L^3(x) \\
I \oplus L^7(x) & I \oplus L^{15}(x) & I \oplus L^{31}(x) \\
I \oplus L^{63}(x) & I \oplus L^{127}(x) & I \oplus L^{255}(x) \\
I \oplus L^{511}(x) & I \oplus L^{1023}(x) & I \oplus L^{2047}
\end{array}
$$

Conclusion

- We introduced some efficient and perfect recursive diffusion layers.
- Found all regular s input/output recursive diffusion layers with $s < 8$ and one linear function.
- Found all non-regular s input/output recursive diffusion layers with
- $s < 5$ and one linear function.
- Found some efficient regular s input/output recursive diffusion layers with $s < 9$ and two linear function.
- A good candidate for designing new block ciphers or hash functions.


Questions?