Anna Grocholewska-Czuryło

Division of Information System Security
Poznań University of Technology
HaF - A new family of hash functions

Poznan University of Technology
Introduction

- Hash functions
- HAF – a family of parameterized hash functions
- Design principles
- Security considerations
Design Principles

- Parametrization
- Selectable message digest length
- Flexibility between security and performance
- Resistance to known attacks
- HAIFA iteration mode
General model of HaF

\[ m \]

1. Append padding bits

2. Append length string

\[ M = M_0 \| M_1 \| \ldots \| M_{k-1} \]

3. Formatted message

\[ H_0 = \| V \]

4. \( H_0 = \| V \)

5. \( M_i \)

6. \( \varphi \)

7. \( s \)

8. \( H_i \)

9. \( H_{i+1} \)

10. \( h(m) = H_k \)
Compression Function
Round Function

\[ N_i \xrightarrow{\ll} \text{lsb}_4(N) \xrightarrow{\text{Round } \# i} N_i^* \]

\[ H_i \xrightarrow{\text{16 steps}} F \xrightarrow{\text{16 steps}} H_i^* \]

16-bit values

\[ A_{15} \]
\[ A_2 \]
\[ A_1 \]
\[ A_0 \]
Step Function
Security Considerations
HaF S-boxes

- S-boxes based on inversion mapping with modifications to remove affine equivalence between component functions
- balancedness
- lowest possible value in XOR profile
- complex algebraic description
- No cycles
- Size: 16x16 bits
- S-box nonlinearity: 32510
- Degree: 15
Inverse mapping

- Irreducible polynomial to define Galois Field (in AES it is $11b$)
- Another polynomial as generator
- n-bit elements treated as polynomials:
  - $b_7b_6b_5b_4b_3b_2b_1b_0 ightarrow b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0$
An multiplicative inverse of polynomial \( g \) in \( \text{GF}(2^n) \) is such a polynomial \( h \) that \( gh = 01 \).

Element \( 00 \) doesn't have an inverse in \( \text{GF} \).
Inverse of \( 01 \) is \( 01 \).

Nonlinearity of such a mapping is \( 2^{n-1} - 2^{n/2} \)
- 112 for \( n=8 \), 32512 for \( n=16 \).

Inverse mapping is different for every irreducible polynomial. It doesn't depend on a selected generator polynomial.
Affine transform

- To avoid algebraic attack
- Must be a full permutation
- in AES:

$$b'_i = b_i \oplus b_{(i+4) \mod 8} \oplus b_{(i+5) \mod 8} \oplus b_{(i+6) \mod 8} \oplus b_{(i+7) \mod 8} \oplus c_i$$

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$
Removing cycles

- Each HaF S-box should be just one cycle

- Removal of cycles done in two steps:
  - Selecting such affine transformation so that the resulting S-box has only two cycles
  - Joining the two cycles while removing affine equivalence from the S-box
Removing affine equivalence

- All S-boxes based on inverse mapping have linear redundancy
- To remove: find two pairs of S-box elements that, when switched, remove this affine equivalence
- Marginal loss of nonlinearity - reduced by 2.
- Joining two cycles of an S-box into one.
How to check if affine equivalence exists in a S-box?

- Algebraic degree and nonlinearity remain unchanged by affine transform
- Absolute values of Walsh transform and autocorrelation function are both rearranged
Modified AES S-box example

- 63 7C 77 7B F2 6B 6F C5 30 01 67 2B D7 AB 76
- CA 82 C9 7D FA 59 47 F0 AD D4 A2 AF 9C A4 72 C0
- B7 FD 93 26 36 3F F7 CC 34 A5 E5 F1 71 D8 31 15
- 04 C7 23 C3 18 96 05 9A 07 12 80 E2 EB 27 B2 75
- 09 83 2C 1A 1B 6E 5A A0 52 3B D6 B3 29 E3 2F 84
- 53 D1 00 ED 20 FC B1 5B 6A CB BE 39 4A 4C 58 CF
- D0 EF AA FB 43 4D 33 85 45 F9 02 7F 50 3C 9F A8
- 51 A3 40 8F 92 9D 38 F5 BC B6 DA 21 10 FF F3 D2
- CD 0C 13 EC 5F 97 44 17 C4 A7 7E 3D 64 5D 19 73
- 60 81 4F DC 22 2A 90 88 46 EE B8 14 DE 5E 0B DB
- E0 32 3A 0A 49 06 24 5C C2 D3 AC 62 91 95 E4 79
- E7 C8 37 6D 8D D5 4E A9 6C 56 F4 EA 65 7A AE 08
- BA 78 25 2E 1C A6 B4 C6 E8 DD 74 1F 4B BD 8B 8A
- 70 3E B5 66 48 03 F6 0E 61 35 57 B9 86 C1 1D 9E
- E1 F8 98 11 69 D9 8E 94 9B 1E 87 E9 CE 55 28 DF
- 8C A1 89 0D BF E6 42 68 41 99 2D 0F B0 54 BB 16
Association with round key

The diagram illustrates a process involving inputs and outputs, with symbols indicating the flow of data. The elements labeled $x_{ij}$ and $v_{ij}$ suggest inputs, while the outputs are denoted by $k_{ij'}$ and $k_{ij''}$. The structure is organized in a grid-like fashion, typical of cryptographic or signal processing algorithms, with operations performed in each cell.
Conclusions 1

- AES-like S-boxes are an excellent base for generating cryptographically strong S-boxes for various purposes
- Affine equivalence can be removed at relatively low cost (reduced nonlienarity)
- Cycles can be removed without any influence to nonlinear properties
Conclusions 11

- Elaborated scheme of HaF hash function family

- Currently experimenting with fault attacks on HaF to verify advantages
Thank you..