Cryptographically optimal functions

Nadiia Ichanska
(3d year PhD at the Selmer Center)

University of Bergen

Norsk Kryptoseminar 2024
October 25, 2024

Boolean functions BF_n

- A **Boolean function** is a mapping $f : f0; 1g^n \; ! \; f0; 1g$.

Boolean functions BF_n

- A Boolean function is a mapping $f : \{0,1\}^n \to \{0,1\}$.
- BF_n denotes the set of n-variable Boolean functions

Boolean functions BF_n

- A Boolean function is a mapping $f : \{0,1\}^n \to \{0,1\}$.
- BF_n denotes the set of n-variable Boolean functions
- The total number of Boolean functions in n variables is 2^{2^n}.

Boolean functions BF_n

- A Boolean function is a mapping $f : \{0,1\}^n \to \{0,1\}$.
- BF_n denotes the set of n-variable Boolean functions
- The total number of Boolean functions in n variables is 2^{2^n}.

n	4	5	6	7	8
$\lvert BF_n \rvert$	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
	$6 \cdot 10^4$	$4 \cdot 10^9$	10^{19}	10^{38}	10^{77}

Example of the Boolean function

- $f : F_2^3 \; 7! \; F_2;$

Example of the Boolean function

- f : F_2^3 7! F_2;
- Truth table:

x_1	x_2	x_3	f (x)
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Example of the Boolean function

- $f : F_2^3 \; 7! \; F_2;$
- Truth table:

x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

- Algebraic normal form:

$$f(x_1; x_2; x_3) = \; x_1x_2x_3 \quad x_2x_3 \quad x_3$$

Nonlinearity of Boolean Functions

- The nonlinearity of f :

$$N_f = \min_{a \in F_2^2; b \in F_2} d(f; a \cdot x + b);$$

Nonlinearity of Boolean Functions

- The nonlinearity of f :

$$N_f = \min_{a2F_2^2;b2F_2} d(f; a\ x + b);$$

- Covering radius bound:

$$N_f \quad 2^{n\ 1} \quad 2^{n=2\ 1};$$

Nonlinearity of Boolean Functions

- The nonlinearity of f :

$$N_f = \min_{a2 F_2^2; b2 F_2} d(f; a\ x + b);$$

- Covering radius bound:

$$N_f \quad 2^{n\ 1} \quad 2^{n=2\ 1};$$

- High nonlinearity is desirable to resist linear attacks on symmetric ciphers;

Nonlinearity of Boolean Functions

- The nonlinearity of f :

$$N_f = \min_{a2F_2^2;b2F_2} d(f; a\ x + b);$$

- Covering radius bound:

$$N_f \quad 2^{n\ 1} \quad 2^{n=2\ 1};$$

- High nonlinearity is desirable to resist linear attacks on symmetric ciphers;
- When $N_f = 2^{n\ 1} \quad 2^{n=2\ 1}$; f is bent;

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions: a variant of the MISTY1 block cipher,

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:
  a variant of the MISTY1 block cipher,
  was standardized for use in the 3GPP mobile communication system;

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:
  a variant of the MISTY1 block cipher,
  was standardized for use in the 3GPP mobile communication system;
- Stream cipher design.

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:
  a variant of the MISTY1 block cipher,
  was standardized for use in the 3GPP mobile communication system;
- Stream cipher design.
  Part of the lter and combiner functions (for nonlinearity).

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:
  a variant of the MISTY1 block cipher,
  was standardized for use in the 3GPP mobile communication system;
- Stream cipher design.
  Part of the lter and combiner functions (for nonlinearity).
  Grain and Trivium,

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:
  a variant of the MISTY1 block cipher,
  was standardized for use in the 3GPP mobile communication system;
- Stream cipher design.
  Part of the lter and combiner functions (for nonlinearity).
  Grain and Trivium,
  is part of eSTREAM project,

Applications

- KN-Cipher , designed in 1989 by Kaisa Nyberg;
- KASUMI Cipher uses highly nonlinear functions:
  a variant of the MISTY1 block cipher,
  was standardized for use in the 3GPP mobile communication system;
- Stream cipher design.
  Part of the lter and combiner functions (for nonlinearity).

  Grain and Trivium,

  is part of eSTREAM project,
  utilized highly nonlinear Boolean functions inspired by the properties of bent functions.

Fundamental components of the symmetric cryptograph

- $(f_1(x);::::;f_m(x))$; where$f_1;::::;f_m : F_2^n$ 7! F_2 - coordinate functions;

Fundamental components of the symmetric cryptograph

- $F(x) = (f_1(x); : : : ; f_m(x))$ is Vectorial Boolean function ;

Fundamental components of the symmetric cryptograph

- $F(x) = (f_1(x); : : : ; f_m(x))$ is Vectorial Boolean function ;
- $F : F_2^n \; 7! \; F_2^m$ - $(n; m)$-function, or S-box;

Fundamental components of the symmetric cryptograph

- $F(x) = (f_1(x); : : : ; f_m(x))$ is Vectorial Boolean function ;
- $F : F_2^n \; 7! \; F_2^m$ - $(n; m)$-function, or S-box;
- Truth table ✓;

Fundamental components of the symmetric cryptograph

- $F(x) = (f_1(x); : : : ; f_m(x))$ is Vectorial Boolean function ;
- $F : F_2^n$ 7! F_2^m - $(n; m)$-function, or S-box;
- Truth table ✓;
- Algebraic normal form✓;

Fundamental components of the symmetric cryptograph

- $F(x) = (f_1(x); : : : ; f_m(x))$ is Vectorial Boolean function ;
- $F : F_2^n \; 7! \; F_2^m$ - $(n; m)$-function, or S-box;
- Truth table ✓;
- Algebraic normal form ✓;
- When $n = m$ any function F has a unique univariate representation :

Fundamental components of the symmetric cryptograph

- $F(x) = (f_1(x); : : : ; f_m(x))$ is Vectorial Boolean function ;
- $F : F_2^n \; 7! \; F_2^m$ - $(n; m)$-function, or S-box;
- Truth table ✓;
- Algebraic normal form ✓;
- When $n = m$ any function F has a unique univariate representation: $F(x) = \sum_{i=0}^{2^n - 1} a_i x^i; \; a_i \; 2 \; F_{2^n}:$

Nonliniearity and di erential uniformity

- $N_F = \min_{v \in F_2^m \setminus \{0\}} N_{v\ F} =$
  $\min_{a \in F_2^n; b \in F_2; v \in F_2^m \setminus \{0\}} d(v \quad F; a \quad x + b);$

Nonliniearity and di erential uniformity

- $N_F = \min_{v \in F_2^m \setminus \{0\}} N_{v\,F} = \min_{a \in F_2^n; b \in F_2; v \in F_2^m \setminus \{0\}} d(v \quad F; a \quad x + b);$
- The derivative of F in the directio$a \in F_2^n$ is $D_a F(x) = F(x) + F(x + a);$

Nonliniearity and di erential uniformity

- $N_F = \min_{v \in F_2^m \setminus \{0\}} N_{v\,F} = \min_{a \in F_2^n; b \in F_2; v \in F_2^m \setminus \{0\}} d(v \quad F; a \quad x + b);$
- The derivative of F in the directio$a \in F_2^n$ is $D_a F(x) = F(x) + F(x + a);$
- The di erential uniformity of $F : F_2^n \to F_2^n$ is

$$_F(a; b) = \max_{a;b \in F_{2^n}; a \neq 0} \max \; \#\{x \in F_{2^n} : D_F(a; x) = b\}$$

Nonliniearity and di erential uniformity

- $N_F = \min_{v \in F_2^m \setminus \{0\}} N_{v\,F} = \min_{a \in F_2^n; b \in F_2; v \in F_2^m \setminus \{0\}} d(v \quad F; a \quad x + b);$
- The derivative of F in the directio$a \in F_2^n$ is $D_a F(x) = F(x) + F(x + a);$
- The di erential uniformity of $F : F_2^n \to F_2^n$ is

$$_F(a; b) = \max_{a;b \in F_{2^n}; a \neq 0} \max \; \#\{x \in F_{2^n} : D_F(a; x) = b\}$$

- Cryptographically optimal functions has $_F = 2$, and are called almost perfect nonlinear (APN) .

- AES (Advanced Encryption Standard) :

  uses an 8-bit S-box for encryption,
  resistance to linear and di erential attacks

- AES (Advanced Encryption Standard) :

  uses an 8-bit S-box for encryption,
  resistance to linear and di erential attacks

- PRESENT:

  uses 4-bit S-boxes,
  a lightweight block cipher for resource-constrained devices,
  S-boxes designed to balance security and e ciency.

- AES (Advanced Encryption Standard) :

  uses an 8-bit S-box for encryption,
  resistance to linear and di erential attacks

- PRESENT:

  uses 4-bit S-boxes,
  a lightweight block cipher for resource-constrained devices,
  S-boxes designed to balance security and e ciency.

- Camellia:
  - A block cipher that combines security features from both AES and Japanese cryptographic standards.
  - Uses S-boxes with properties optimized for cryptographic strength.

Conclusion

- Vectorial Boolean Functions are fundamental in symmetric cryptography, particularly in the design of S-boxes.

Conclusion

- Vectorial Boolean Functions are fundamental in symmetric cryptography, particularly in the design of S-boxes.
- Provide essential properties nonlinearity and di erential uniformity , ensuring resistance against attacks.

Conclusion

- **Vectorial Boolean Functions** are fundamental in symmetric cryptography, particularly in the design of S-boxes.
- Provide essential properties: **nonlinearity** and **di erential uniformity**, ensuring resistance against attacks.
- In binary case, functions that exhibit high nonlinearity and low differential uniformity are **APN functions**.

Conclusion

- **Vectorial Boolean Functions** are fundamental in symmetric cryptography, particularly in the design of S-boxes.
- Provide essential properties: **nonlinearity** and **di erential uniformity**, ensuring resistance against attacks.
- In binary case, functions that exhibit high nonlinearity and low differential uniformity are **APN functions**.
- Algorithms for finding new instance are essential.

Conclusion

- **Vectorial Boolean Functions** are fundamental in symmetric cryptography, particularly in the design of S-boxes.
- Provide essential properties: **nonlinearity** and **di erential uniformity**, ensuring resistance against attacks.
- In binary case, functions that exhibit high nonlinearity and low differential uniformity are **APN functions**.
- Algorithms for finding new instance are essential.
- Continuous research aims to further optimize them for efficiency, security, and practical deployment in various cryptographic applications.