Symmetric Encryption Scheme adapted to Fully Homomorphic Encryption Scheme: New Criteria for Boolean functions

Pierrick MÉAUX

École normale supérieure, INRIA, CNRS, PSL

Télécom ParisTech — Paris, France
Friday March 17

Table of Contents

Summary

Outsourcing Computation

Alice

Limited storage
Limited power

Store ?
Compute ?

Outsourcing Computation

Alice

Limited storage
Limited power

Store ✓
Compute ✓

Claude

Huge storage
Huge power

Outsourcing Computation

Alice

Limited storage
Limited power

Store ✓
Compute ✓

Privacy ?

Claude

Huge storage
Huge power

Outsourcing Computation

Alice

Limited storage
Limited power

Store ✓
Compute ✓

Privacy ✓

Fully
Homomorphic
Encryption

Claude

Huge storage
Huge power

Fully Homomorphic Encryption

$$f, \mathbf{C}(x_1), \cdots, \mathbf{C}(x_n) \quad \rightarrow \quad \mathbf{C}(f(x_1, \cdots, x_n))$$

Fully Homomorphic Encryption

$$f, \mathbf{C}(x_1), \cdots, \mathbf{C}(x_n) \quad \rightarrow \quad \mathbf{C}(f(x_1, \cdots, x_n))$$

$$\mathbf{C}(x_1) \quad = \quad \boxed{x_1}$$

$$\boxed{x_1} \quad + \quad \boxed{x_2} \quad = \quad \boxed{x_1 + x_2}$$

$$\boxed{x_1} \quad \cdot \quad \boxed{x_2} \quad = \quad \boxed{x_1 \cdot x_2}$$

Fully Homomorphic Encryption

$$f, \mathbf{C}(x_1), \cdots, \mathbf{C}(x_n) \quad \rightarrow \quad \mathbf{C}(f(x_1, \cdots, x_n))$$

$$\mathbf{C}(x_1) \quad = \quad \boxed{x_1}$$

$$\boxed{x_1} \quad + \quad \boxed{x_2} \quad = \quad \boxed{x_1 + x_2}$$

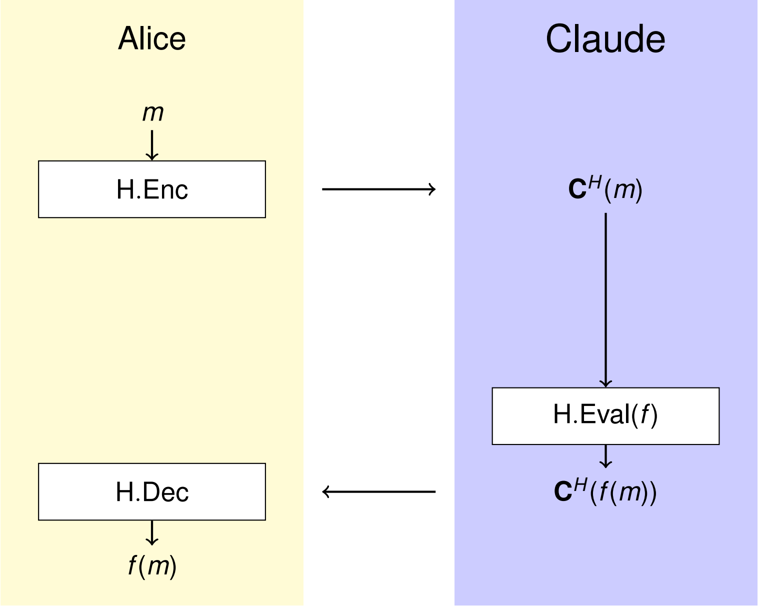
$$\boxed{x_1} \quad \cdot \quad \boxed{x_2} \quad = \quad \boxed{x_1 \cdot x_2}$$

Bottlenecks:

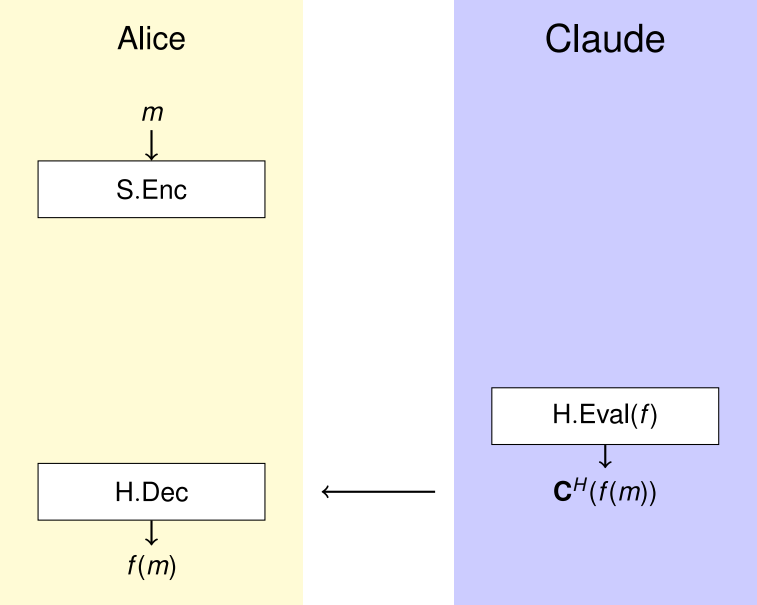
$\rightarrow$ high cost when high level of error

$\rightarrow$ high expansion factor

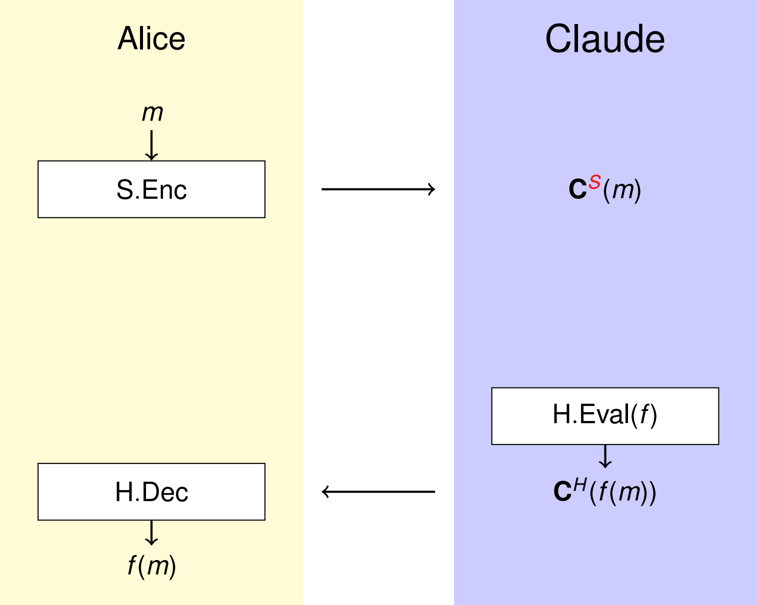
FHE Framework



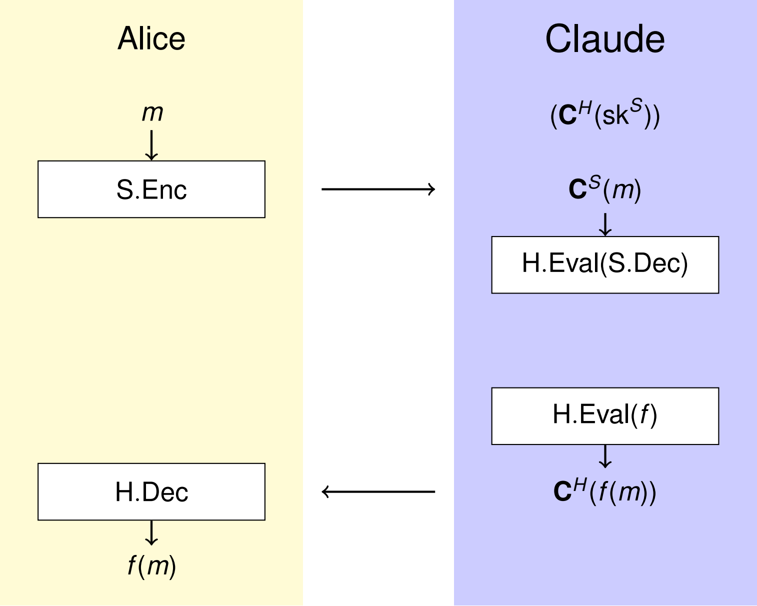
SE-HE Hybrid Framework



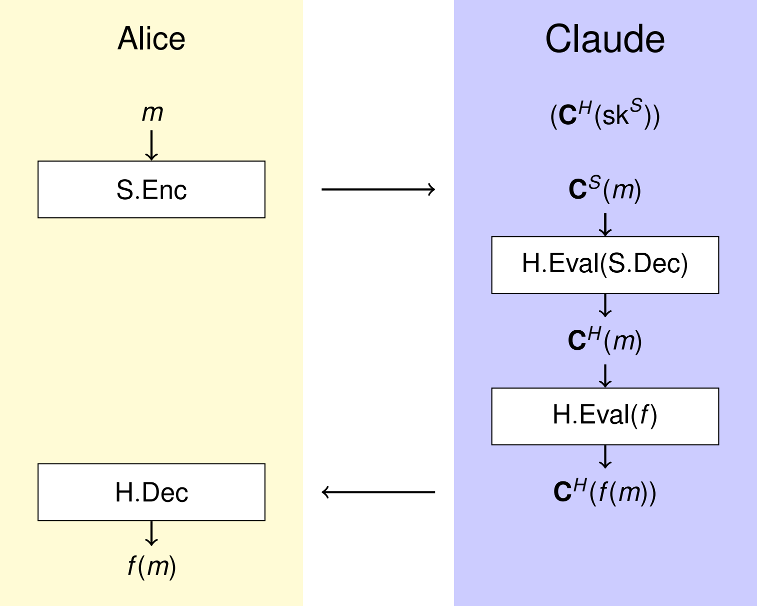
SE-HE Hybrid Framework



SE-HE Hybrid Framework



SE-HE Hybrid Framework



SE adapted to FHE

$\boxed{\text{H.Eval(S.Dec)}}$ as efficient as possible

SE adapted to FHE

$\boxed{\text{H.Eval(S.Dec)}}$ as efficient as possible

f in clear

$x_1 * x_2$

f in homomorphic

$\boxed{x_1} * \boxed{x_2}$

SE adapted to FHE

$\boxed{\text{H.Eval(S.Dec)}}$ as efficient as possible

f in clear

$x_1 * x_2$

Switch(x)

f in homomorphic

$\boxed{x_1} * \boxed{x_2}$

$\boxed{x} = ?$

SE adapted to FHE

$\boxed{\text{H.Eval(S.Dec)}}$ as efficient as possible

f in clear

$x_1 * x_2$

Switch(x)

$0 \wedge \cdots = 0$

$1 \vee \cdots = 1$

f in homomorphic

$\boxed{x_1} * \boxed{x_2}$

$\boxed{x}$ = ?

Evaluate
all the Circuit

SE adapted to FHE

$\boxed{\text{H.Eval(S.Dec)}}$ as efficient as possible

f in clear

$x_1 * x_2$

Switch(x)

$0 \wedge \cdots = 0$

$1 \vee \cdots = 1$

f in homomorphic

$\boxed{x_1} * \boxed{x_2}$

$\boxed{x} = ?$

Evaluate
all the Circuit

Optimize S.Dec circuit: Minimize homomorphic error growth

SE adapted to FHE

$\boxed{\text{H.Eval(S.Dec)}}$ as efficient as possible

f in clear

$x_1 * x_2$

$\text{Switch}(x)$

$0 \wedge \cdots = 0$

$1 \vee \cdots = 1$

f in homomorphic

$\boxed{x_1} * \boxed{x_2}$

$\boxed{x} = ?$

Evaluate all the Circuit

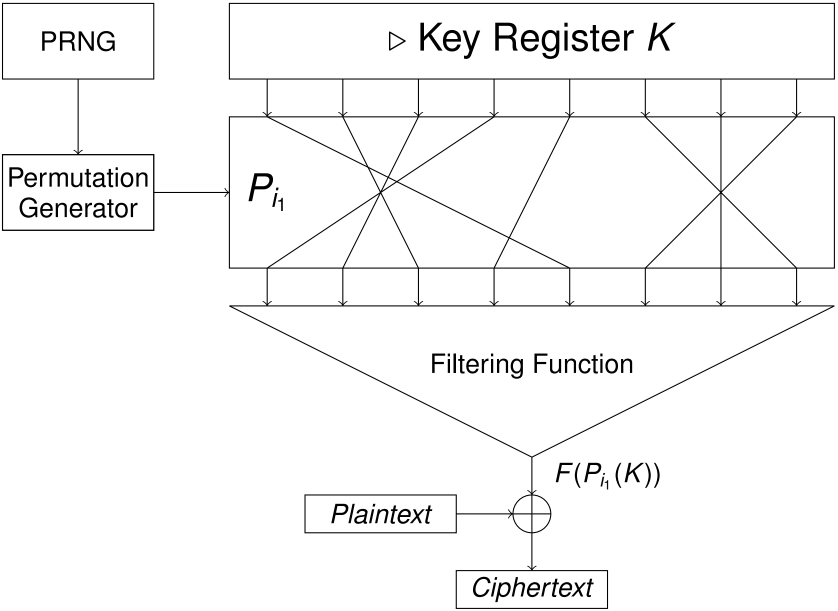
Optimize S.Dec circuit: Minimize homomorphic error growth

block cipher $\rightarrow$ too many rounds

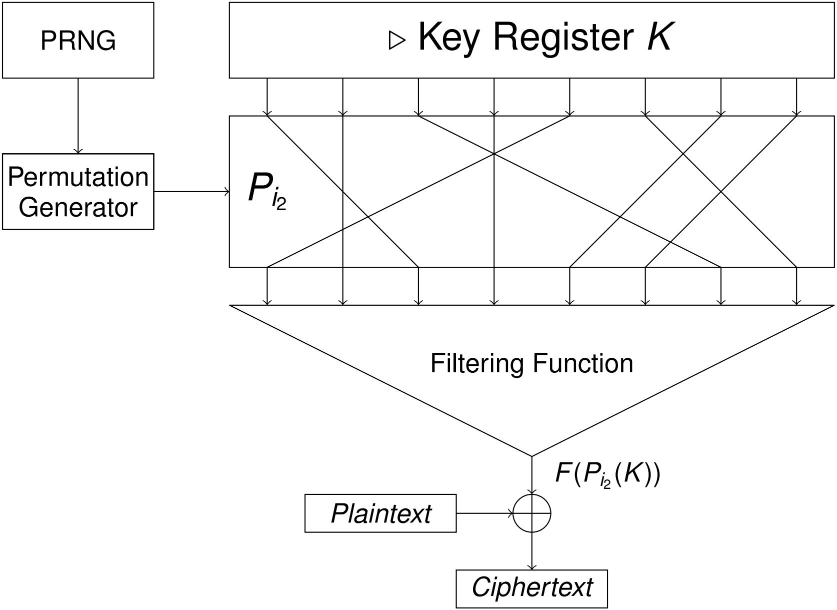
stream cipher $\rightarrow$ increasing complexity

Summary

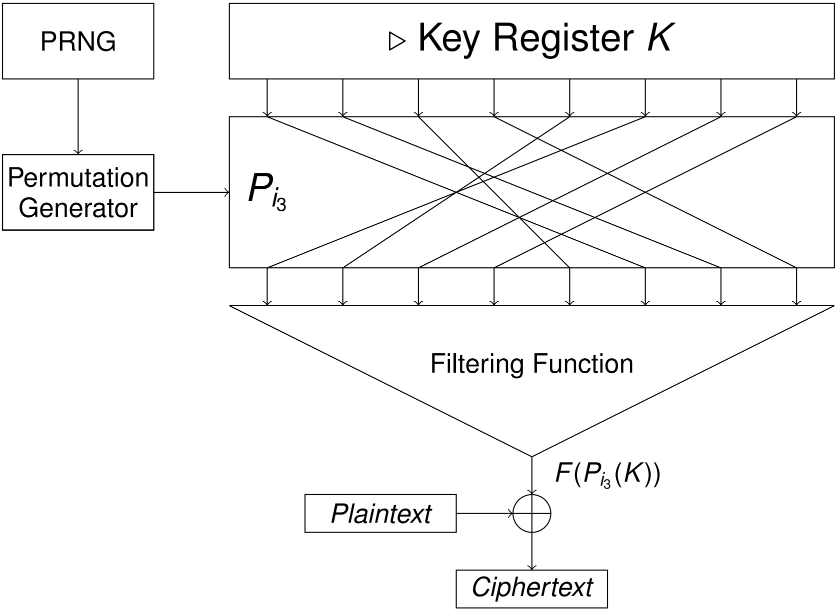
Filter Permutator: Construction



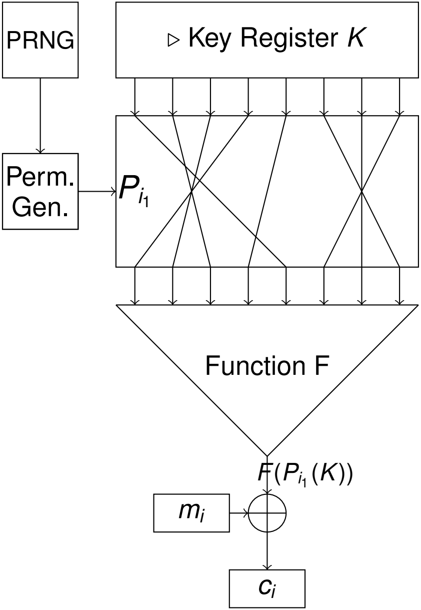
Filter Permutator: Construction



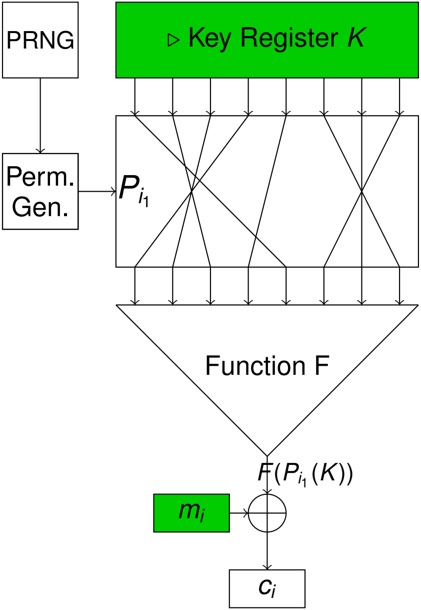
Filter Permutator: Construction



Filter Permutator: Homomorphic Evaluation

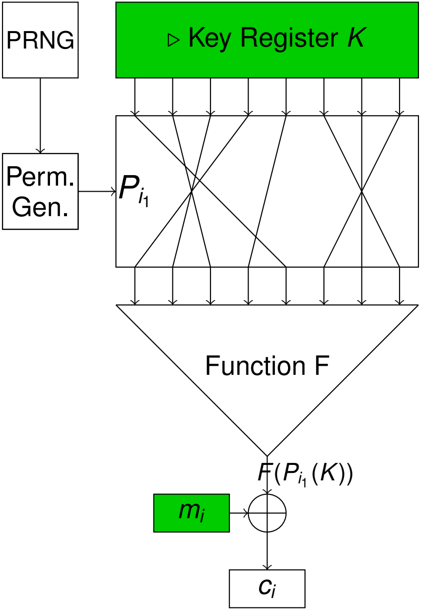


Filter Permutator: Homomorphic Evaluation



K_i, m_i: fresh

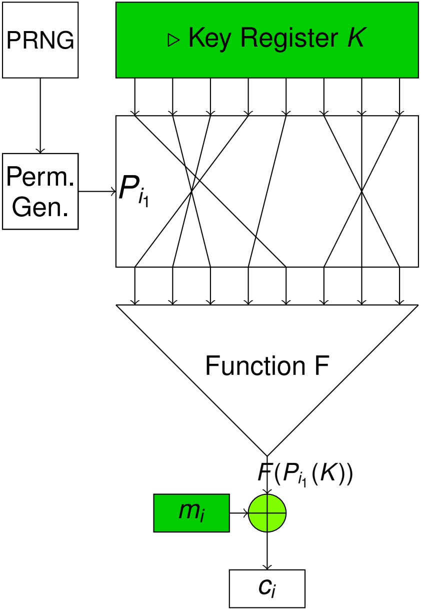
Filter Permutator: Homomorphic Evaluation



K_i, m_i: fresh

Permutation: no noise

Filter Permutator: Homomorphic Evaluation

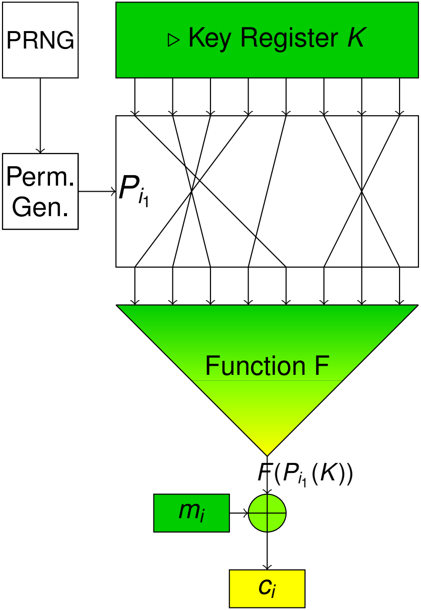


K_i, m_i: fresh

Permutation: no noise

XOR: small noise

Filter Permutator: Homomorphic Evaluation



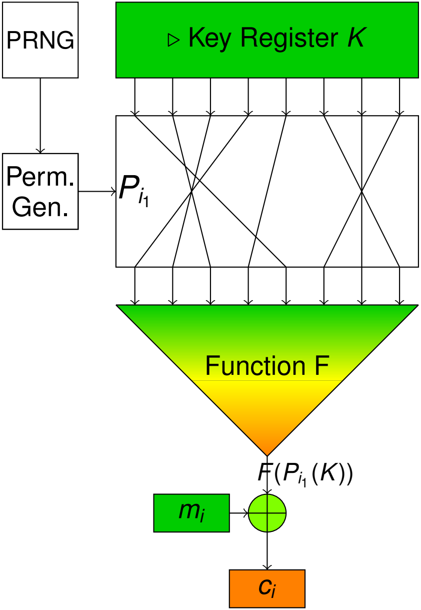
K_i, m_i: fresh

Permutation: no noise

XOR: small noise

F: determines ct noise

Filter Permutator: Homomorphic Evaluation



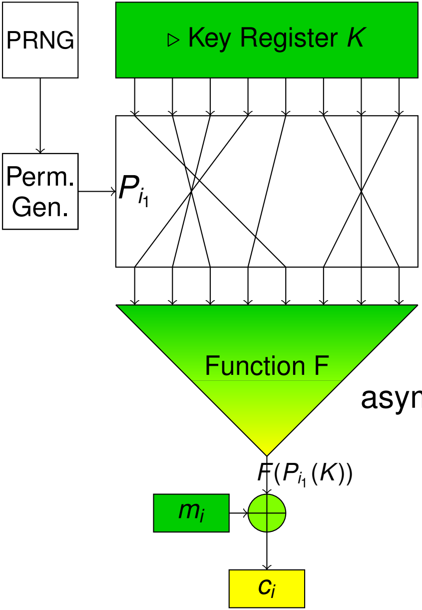
K_i, m_i: fresh

Permutation: no noise

XOR: small noise

F: determines ct noise

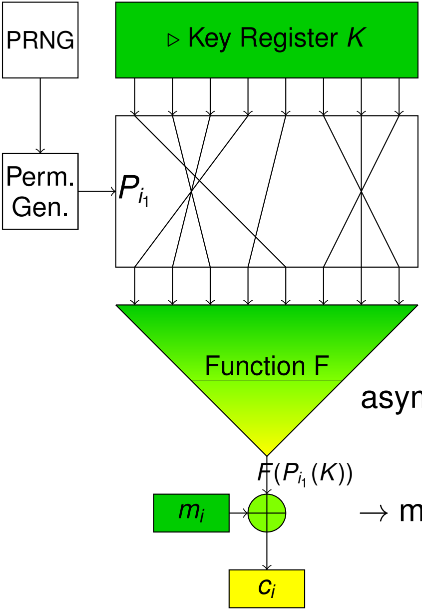
Filter Permutator: Homomorphic Evaluation



3*rd* generation FHE:

asymetric error growth for products

Filter Permutator: Homomorphic Evaluation



3*rd* generation FHE:

asymetric error growth for products

$\rightarrow$ additions

$\rightarrow$ multiplicative chains low noise ct

$\rightarrow$ few monomials

Summary

FP Symmetric Behavior

Cryptanalysis Angle

"good" PRNG + "good" Shuffle $\approx$ random Permutations; what about F?

FP Symmetric Behavior

Cryptanalysis Angle

"good" PRNG + "good" Shuffle $\approx$ random Permutations; what about F?

Attacks on Filtering Function

- Algebraic
- Fast Algebraic
- Correlation
- High Order Correlation
- etc

FP Symmetric Behavior

Cryptanalysis Angle

"good" PRNG + "good" Shuffle $\approx$ random Permutations; what about F?

Attacks on Filtering Function

- Algebraic
- Fast Algebraic
- Correlation
- High Order Correlation
- etc

Standard Criteria

- Algebraic Immunity
- Fast Algebraic Immunity
- Resiliency
- Non Linearity

FP Symmetric Behavior

Cryptanalysis Angle

"good" PRNG + "good" Shuffle $\approx$ random Permutations; what about F?

Attacks on Filtering Function

- Algebraic
- Fast Algebraic
- Correlation
- High Order Correlation
- etc

Standard Criteria

- Algebraic Immunity
- Fast Algebraic Immunity
- Resiliency
- Non Linearity

Low cost constraints

- additions
- long multiplicative chains of simple functions
- few monomials

(Fast) Algebraic Attack

Algebraic Attack [CM03]

Let F be the keystream function of a stream cipher

1. find g a low algebraic degree function s.t. gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^{\omega})$.

(Fast) Algebraic Attack

Algebraic Attack [CM03]

Let F be the keystream function of a stream cipher

1. find g a low algebraic degree function s.t. gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^{\omega})$.

Algebraic Immunity

Let $F : \mathbb{F}_2^N \to \mathbb{F}_2$
we define

$$\begin{aligned} \mathrm{AI}(F) &= \min\{\max(\deg(g), \deg(gF), g \neq 0)\} \\ &= \{deg(g), g \neq 0 \mid gF = 0 \text{ or } g(F \oplus 1) = 0\} \end{aligned}$$

Attack complexity depends on $deg(g) \geq \mathrm{AI}(F)$

(Fast) Algebraic Attack

Algebraic Attack [CM03]

Let F be the keystream function of a stream cipher

1. find g a low algebraic degree function s.t. gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^\omega)$.

Fast Algebraic Attack [C03]

Let F be the keystream function of a stream cipher

- find g and h low algebraic degree functions s.t. $gF = h$ with $\deg(g) < \mathrm{AI}(F)$ and possibly $deg(h) > deg(g)$,
- use codes methods to cancel monomials of degree higher than $deg(g)$,
- solve the system with better complexity than Algebraic Attack.

(Fast) Algebraic Attack

Algebraic Attack [CM03]

Let F be the keystream function of a stream cipher

1. find g a low algebraic degree function s.t. gF has low degree,
2. create T equations with monomials of degree $\leq deg(g)$,
3. linearize the system of T equations in $D = \sum_{i=0}^{deg(g)} \binom{N}{i}$ variables,
4. solve the system in $\mathcal{O}(D^{\omega})$.

Fast Algebraic Attack [C03]

Let F be the keystream function of a stream cipher

- find g and h low algebraic degree functions s.t. $gF = h$ with $\deg(g) < \mathrm{AI}(F)$ and possibly $deg(h) > deg(g)$,
- use codes methods to cancel monomials of degree higher than $deg(g)$,
- solve the system with better complexity than Algebraic Attack.

we define $\mathrm{FAI}(F) = \min\{2\mathrm{AI}(F), \min_{1 \leq deg(g) \leq \mathrm{AI}(F)}\{deg(g) + deg(Fg), 3deg(g)\}\}$

Good Algebraic Immunity

(F)AI properties

upper bound:

$$\mathrm{AI}(F) \leq \lceil N/2 \rceil$$

Good Algebraic Immunity

(F)AI properties

upper bound:

$$\mathrm{AI}(F) \leq \lceil N/2 \rceil$$

Majority function

$$x = (x_1, \cdots, x_N) \in \mathbb{F}_2^N, \quad Maj_N(x) = \begin{cases} 0 & \text{if } Hw(x) \leq \lfloor \frac{N}{2} \rfloor \\ 1 & \text{otherwise} \end{cases}$$

$N = 3$; $Maj_3(x) = x_1x_2 + x_1x_3 + x_2x_3$

Good Algebraic Immunity

(F)AI properties

upper bound:

$$\mathrm{AI}(F) \leq \lceil N/2 \rceil$$

Majority function

$$x = (x_1, \cdots, x_N) \in \mathbb{F}_2^N, \quad Maj_N(x) = \begin{cases} 0 & \text{if } Hw(x) \leq \lfloor \frac{N}{2} \rfloor \\ 1 & \text{otherwise} \end{cases}$$

$\mathrm{AI}(Maj_N) = \lceil N/2 \rceil$
ANF: $\geq \binom{N}{\lceil N/2 \rceil}$ monomials

Low Cost and Good Algebraic Immunity

(F)AI properties

upper bound:

$$\mathsf{AI}(F) \leq \lceil N/2 \rceil$$

Direct sum property, $F(x_1, \cdots, x_N) = f_1(x_1, \cdots, x_\ell) + f_2(x_{\ell+1}, \cdots, x_N)$

$$\max(\mathsf{AI}(f_1), \mathsf{AI}(f_2)) \leq \mathsf{AI}(F) \leq \mathsf{AI}(f_1) + \mathsf{AI}(f_2)$$

Low Cost and Good Algebraic Immunity

(F)AI properties

upper bound:

$$\mathrm{AI}(F) \leq \lceil N/2 \rceil$$

Direct sum property, $F(x_1, \cdots, x_N) = f_1(x_1, \cdots, x_\ell) + f_2(x_{\ell+1}, \cdots, x_N)$

$$\max(\mathrm{AI}(f_1), \mathrm{AI}(f_2)) \leq \mathrm{AI}(F) \leq \mathrm{AI}(f_1) + \mathrm{AI}(f_2)$$

Triangular function

Let T_k be a Boolean function of $N = \frac{k(k+1)}{2}$ variables, built as the direct sum of k monomials of degree from 1 to k.

$T_4 = x_0 + x_1x_2 + x_3x_4x_5 + x_6x_7x_8x_9$

Low Cost and Good Algebraic Immunity

(F)AI properties

upper bound:

$$\mathrm{AI}(F) \leq \lceil N/2 \rceil$$

Direct sum property, $F(x_1, \cdots, x_N) = f_1(x_1, \cdots, x_\ell) + f_2(x_{\ell+1}, \cdots, x_N)$

$$\max(\mathrm{AI}(f_1), \mathrm{AI}(f_2)) \leq \mathrm{AI}(F) \leq \mathrm{AI}(f_1) + \mathrm{AI}(f_2)$$

Triangular function

Let T_k be a Boolean function of $N = \frac{k(k+1)}{2}$ variables, built as the direct sum of k monomials of degree from 1 to k.

$\mathrm{AI}(T_k) = k$
ANF: k monomials

Correlation Attack

Correlation attack/ BKW-like attack

Let F be the keystream function of a stream cipher

1. find g the best linear approximation of F,
2. create the linear system replacing F by g,
3. solve the LPN instance with Bernoulli mean the error made by the approximation.

Correlation Attack

Correlation attack/ BKW-like attack

Let F be the keystream function of a stream cipher

1. find g the best linear approximation of F,
2. create the linear system replacing F by g,
3. solve the LPN instance with Bernoulli mean the error made by the approximation.

Possible improvements: use of codes techniques or higher order approximation.

Correlation Attack

Correlation attack/ BKW-like attack

Let F be the keystream function of a stream cipher

1. find g the best linear approximation of F,
2. create the linear system replacing F by g,
3. solve the LPN instance with Bernoulli mean the error made by the approximation.

Possible improvements: use of codes techniques or higher order approximation.

Nonlinearity

Let $F : \mathbb{F}_2^N \to \mathbb{F}_2$ and
we define $\mathrm{NL}(F) = \min_{g \text{ affine}} \{d_H(f, g)\}$,
where $d_H(f, g) = \#\{x \in \mathbb{F}_2^N \mid F(x) \neq g(x)\}$, the Hamming distance

The approximation error is $\frac{\mathrm{NL}(F)}{2^N}$.

Correlation Attack

Nonlinearity

Let $F : \mathbb{F}_2^N \to \mathbb{F}_2$ and
we define $\mathrm{NL}(F) = \min_{g \text{ affine}} \{d_H(f, g)\}$,
where $d_H(f, g) = \#\{x \in \mathbb{F}_2^N \mid F(x) \neq g(x)\}$, the Hamming distance

The approximation error is $\frac{\mathrm{NL}(F)}{2^N}$.

Balancedness

$F : \mathbb{F}_2^N \to \mathbb{F}_2$ is balanced if its output are uniformly distributed over $\{0, 1\}$

Resiliency

$F : \mathbb{F}_2^N \to \mathbb{F}_2$ is m resilient if any of its restrictions obtained by fixing at most m of its coordinates is balanced

Low Cost and good criteria

direct sum properties

Let F be the direct sum of f_1 in n_1 variables and f_2 in n_2 variables

- $\mathrm{res}(f) = \mathrm{res}(f_1) + \mathrm{res}(f_2) + 1$,
- $\mathrm{NL}(F) = 2^{n_2}\mathrm{NL}(f_1) + 2^{n_1}\mathrm{NL}(f_2) - 2\mathrm{NL}(f_1)\mathrm{NL}(f_2)$

Low Cost and good criteria

direct sum properties

Let F be the direct sum of f_1 in n_1 variables and f_2 in n_2 variables

- $\mathrm{res}(f) = \mathrm{res}(f_1) + \mathrm{res}(f_2) + 1$,
- $\mathrm{NL}(F) = 2^{n_2}\mathrm{NL}(f_1) + 2^{n_1}\mathrm{NL}(f_2) - 2\mathrm{NL}(f_1)\mathrm{NL}(f_2)$

Low cost functions

- Resiliency:
  $L_n = \sum_{i=1}^{n} x_i$; $n-1$ resilient
- Nonlinearity:
  $Q_{\frac{n}{2}} = \sum_{i=1}^{\frac{n}{2}} x_{2i-1}x_{2i}$
- Algebraic Immunity:
  $T_k = \sum_{i=1}^{k} \prod_{j=1}^{i} x_{\frac{i(i+1)}{2}+j}$

Low Cost and good criteria

direct sum properties

Let F be the direct sum of f_1 in n_1 variables and f_2 in n_2 variables

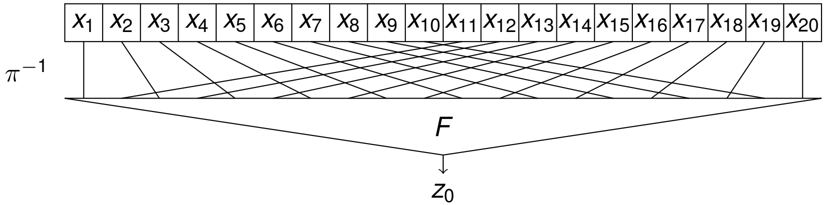
- $\mathrm{res}(f) = \mathrm{res}(f_1) + \mathrm{res}(f_2) + 1$,
- $\mathrm{NL}(F) = 2^{n_2}\mathrm{NL}(f_1) + 2^{n_1}\mathrm{NL}(f_2) - 2\mathrm{NL}(f_1)\mathrm{NL}(f_2)$

Low cost functions

- Resiliency:
  $L_n = \sum_{i=1}^{n} x_i$; $n-1$ resilient
- Nonlinearity:
  $Q_{\frac{n}{2}} = \sum_{i=1}^{\frac{n}{2}} x_{2i-1}x_{2i}$
- Algebraic Immunity:
  $T_k = \sum_{i=1}^{k} \prod_{j=1}^{i} x_{\frac{i(i+1)}{2}+j}$
- Low cost and optimized criteria:
  $F = L_{n_1} + Q_{\frac{n_2}{2}} + T_k$

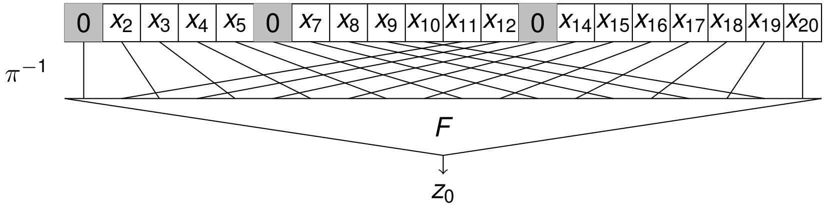
Summary

Guess and Determine Attacks



$$
\begin{aligned}
z_0 = {} & x_{\pi(1)} + x_{\pi(2)} + x_{\pi(3)} + x_{\pi(4)} \\
+ {} & x_{\pi(5)}x_{\pi(6)} + x_{\pi(7)}x_{\pi(8)} + x_{\pi(9)}x_{\pi(10)} \\
+ {} & x_{\pi(11)} + x_{\pi(12)}x_{\pi(13)} + x_{\pi(14)}x_{\pi(15)}x_{\pi(16)} + x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)}
\end{aligned}
$$

Guess and Determine Attacks

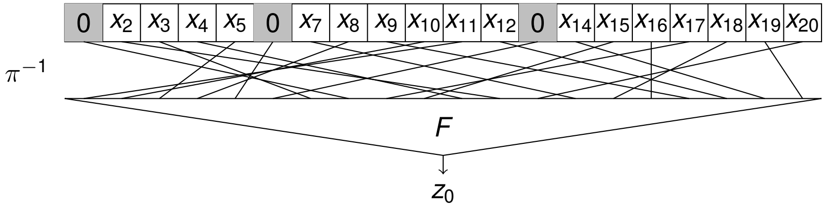


$$\begin{aligned} z_0 &= \cancel{x_{\pi(1)}} + x_{\pi(2)} + x_{\pi(3)} + x_{\pi(4)} \\ &+ \cancel{x_{\pi(5)}x_{\pi(6)}} + x_{\pi(7)}x_{\pi(8)} + x_{\pi(9)}x_{\pi(10)} \\ &+ \cancel{x_{\pi(11)}} + x_{\pi(12)}x_{\pi(13)} + x_{\pi(14)}x_{\pi(15)}x_{\pi(16)} + x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)} \end{aligned}$$

Guess & Determine attack [DLR16]

- Guess ℓ positions being 0,

Guess and Determine Attacks

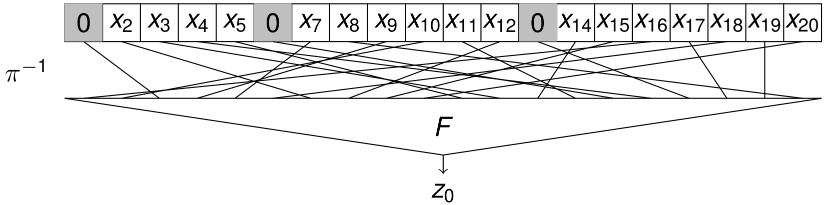


$$\begin{aligned} z_0 = \; & x_{\pi(1)} + x_{\pi(2)} + x_{\pi(3)} + x_{\pi(4)} \\ + \; & \cancel{x_{\pi(5)}x_{\pi(6)}} + \cancel{x_{\pi(7)}x_{\pi(8)}} + x_{\pi(9)}x_{\pi(10)} \\ + \; & x_{\pi(11)} + x_{\pi(12)}x_{\pi(13)} + x_{\pi(14)}x_{\pi(15)}x_{\pi(16)} + x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)} \end{aligned}$$

Guess & Determine attack [DLR16]

- Guess ℓ positions being 0,
- focus on permutations cancelling the monomials of degree > 2,

Guess and Determine Attacks

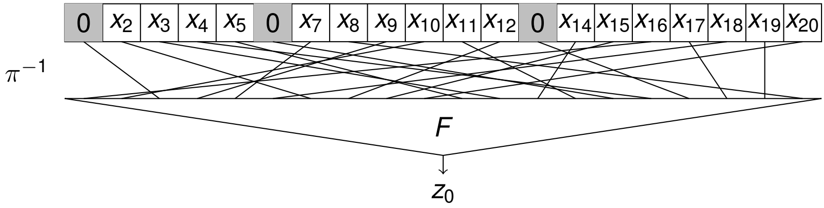


$$
\begin{aligned}
z_0 \quad = \quad & x_{\pi(1)} + x_{\pi(2)} + \cancel{x_{\pi(3)}} + x_{\pi(4)} \\
+ \quad & x_{\pi(5)}x_{\pi(6)} + x_{\pi(7)}x_{\pi(8)} + x_{\pi(9)}x_{\pi(10)} \\
+ \quad & x_{\pi(11)} + x_{\pi(12)}x_{\pi(13)} + \cancel{x_{\pi(14)}x_{\pi(15)}x_{\pi(16)}} + \cancel{x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)}}
\end{aligned}
$$

Guess & Determine attack [DLR16]

- Guess ℓ positions being 0,
- focus on permutations cancelling the monomials of degree > 2,
- collect all degree 2 equations,

Guess and Determine Attacks



$$
\begin{aligned}
z_0 \;=\;& x_{\pi(1)} + x_{\pi(2)} + \cancel{x_{\pi(3)}} + x_{\pi(4)} \\
+\;& x_{\pi(5)}x_{\pi(6)} + x_{\pi(7)}x_{\pi(8)} + x_{\pi(9)}x_{\pi(10)} \\
+\;& x_{\pi(11)} + x_{\pi(12)}x_{\pi(13)} + \cancel{x_{\pi(14)}x_{\pi(15)}x_{\pi(16)}} + \cancel{x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)}}
\end{aligned}
$$

Guess & Determine attack [DLR16]

- Guess ℓ positions being 0,
- focus on permutations cancelling the monomials of degree > 2,
- collect all degree 2 equations,
- linearise and try to solve the system,
- time complexity $2^{\ell}(1 + N + \binom{N}{2})^{\omega}$, data complexity $1/Pr(P)$.

G&D attacks and new Boolean criteria

Attack lessons

- zero cost homomorphic update $\rightarrow$ unchanged key bits,
- ℓ guesses $\rightarrow$ F restricted to F' on $N - \ell$ variables,
- attack on F' degree [DLR16],

G&D attacks and new Boolean criteria

Attack lessons

- zero cost homomorphic update $\rightarrow$ unchanged key bits,
- ℓ guesses $\rightarrow$ F restricted to F' on $N - \ell$ variables,
- attack on F' degree [DLR16],
- $\mathrm{AI}(F')$ $\rightarrow$ G&D + (fast) algebraic attacks ?
- $\mathrm{NL}(F'), \mathrm{res}(F')$ $\rightarrow$ G&D + correlation attacks ?

G&D attacks and new Boolean criteria

Attack lessons

- zero cost homomorphic update $\rightarrow$ unchanged key bits,
- ℓ guesses $\rightarrow$ F restricted to F' on $N - \ell$ variables,
- attack on F' degree [DLR16],
- $\mathrm{AI}(F')$ $\rightarrow$ G&D + (fast) algebraic attacks ?
- $\mathrm{NL}(F'), \mathrm{res}(F')$ $\rightarrow$ G&D + correlation attacks ?

Attack depends on: criteria of F' and probabilities of getting F'

G&D attacks and new Boolean criteria

Attack lessons

- zero cost homomorphic update $\rightarrow$ unchanged key bits,
- ℓ guesses $\rightarrow$ F restricted to F' on $N - \ell$ variables,
- attack on F' degree [DLR16],
- $\mathrm{AI}(F') \rightarrow$ G&D + (fast) algebraic attacks ?
- $\mathrm{NL}(F'), \mathrm{res}(F') \rightarrow$ G&D + correlation attacks ?

Attack depends on: criteria of F' and probabilities of getting F'

Recurrent criteria

Recurrent AI; $\mathrm{AI}[\ell](F)$:
$\mathrm{AI}[\ell](F)$ is the minimal algebraic immunity over all functions obtained by fixing ℓ variables of F.

Similarly,
$\mathrm{FAI}[\ell](F), \mathrm{NL}[\ell](F)$,and $\mathrm{res}[\ell](F)$

Recurrent Algebraic immunity

Recurrent AI; AI[ℓ](F)

AI[ℓ](F) is the minimal algebraic immunity over all functions obtained by fixing ℓ variables of F.
example:
$\mathrm{AI}[1](f(x_1, x_2)) = \min[\mathrm{AI}(f(0, x_2)), \mathrm{AI}(f(1, x_2)), \mathrm{AI}(f(x_1, 0)), \mathrm{AI}(f(x_1, 1))]$

Recurrent Algebraic immunity

Recurrent AI; AI[ℓ](F)

AI[ℓ](F) is the minimal algebraic immunity over all functions obtained by fixing ℓ variables of F.
example:
$\mathrm{AI}[1](f(x_1, x_2)) = \min[\mathrm{AI}(f(0, x_2)), \mathrm{AI}(f(1, x_2)), \mathrm{AI}(f(x_1, 0)), \mathrm{AI}(f(x_1, 1))]$

AI[ℓ](F) Property

For all Boolean function F:

$$\mathrm{AI}(F) - \ell \leq \mathrm{AI}[\ell](F) \leq \mathrm{AI}(F)$$

Recurrent Algebraic immunity

Recurrent AI; AI[ℓ](F)

AI[ℓ](F) is the minimal algebraic immunity over all functions obtained by fixing ℓ variables of F.
example:
$\mathrm{AI}[1](f(x_1, x_2)) = \min[\mathrm{AI}(f(0, x_2)), \mathrm{AI}(f(1, x_2)), \mathrm{AI}(f(x_1, 0)), \mathrm{AI}(f(x_1, 1))]$

AI[ℓ](F) Property

For all Boolean function F:

$$\mathrm{AI}(F) - \ell \leq \mathrm{AI}[\ell](F) \leq \mathrm{AI}(F)$$

upper bound: g defining AI(F); a guess where g is not null.
lower bound: hypothesis $\mathrm{AI}[1](F) < \mathrm{AI}(F) - 1$ leads to contradiction

Recurrent Algebraic immunity

AI[ℓ](F) Property

For all Boolean function F:

$$\mathrm{AI}(F) - \ell \leq \mathrm{AI}[\ell](F) \leq \mathrm{AI}(F)$$

Majority function, $\ell = 2$

$$x = (x_1, \cdots, x_N) \in \mathbb{F}_2^N, \quad Maj_N(x) = \begin{cases} 0 & \text{if } Hw(x) \leq \lfloor \frac{N}{2} \rfloor \\ 1 & \text{otherwise} \end{cases}$$

$F = Maj_N$;
$\mathrm{AI}(F) = \lceil N/2 \rceil$

$$\lceil N/2 \rceil - 2 \leq \mathrm{AI}[2](F) \leq \lceil N/2 \rceil$$

Recurrent Algebraic immunity

AI[ℓ](F) Property

For all Boolean function F:

$$\mathrm{AI}(F) - \ell \leq \mathrm{AI}[\ell](F) \leq \mathrm{AI}(F)$$

Majority function, $\ell = 2$, fixing $x_1 = 1$,and $x_2 = 0$

$$\bar{x} = (x_3, \cdots, x_N) \in \mathbb{F}_2^{N-2}, \quad F'(\bar{x}) = \begin{cases} 0 & \text{if } Hw(x) \leq \lfloor \frac{N}{2} \rfloor - 1 \\ 1 & \text{otherwise} \end{cases}$$

$F' = Maj_{N-2}$;
$\mathrm{AI}(F') = \lceil (N-2)/2 \rceil$

$$\lceil N/2 \rceil - 2 \leq \mathrm{AI}[2](F) \leq \lceil N/2 \rceil - 1$$

Recurrent Algebraic immunity

AI[ℓ](F) Property

For all Boolean function F:

$$\mathrm{AI}(F) - \ell \leq \mathrm{AI}[\ell](F) \leq \mathrm{AI}(F)$$

Majority function, $\ell = 2$, fixing $x_1 = x_2 = 1$

$$\bar{x} = (x_3, \cdots, x_N) \in \mathbb{F}_2^{N-2}, \quad F'(\bar{x}) = \begin{cases} 0 & \text{if } Hw(x) \leq \lfloor \frac{N}{2} \rfloor - 2 \\ 1 & \text{otherwise} \end{cases}$$

$(F' + 1) \cdot S_{\lceil (N-4)/2 \rceil} = 0;$
$\mathrm{AI}(F') = \lceil (N-4)/2 \rceil$

$$\lceil N/2 \rceil - 2 = \mathrm{AI}[2](F)$$

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

F direct sum of monomials $\leftrightarrow$ vector $\mathbf{m}_F = [m_1, m_2, \cdots, m_k]$
Example: T_4; $\mathbf{m}_{T_4} = [1, 1, 1, 1]$

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

F direct sum of monomials $\leftrightarrow$ vector $\mathbf{m}_F = [m_1, m_2, \cdots, m_k]$

Two recurrent criteria:

- $\mathbf{m}_F^*$ the number of nonzero values of $\mathbf{m}_F$,
- $\delta_{\mathbf{m}_F} = \frac{1}{2} - \frac{\mathrm{NL}(F)}{2^N}$; "bias".

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

F direct sum of monomials $\leftrightarrow$ vector $\mathbf{m}_F = [m_1, m_2, \cdots, m_k]$

Two recurrent criteria:

- $\mathbf{m}_F^*$ the number of nonzero values of $\mathbf{m}_F$,
- $\delta_{\mathbf{m}_F} = \frac{1}{2} - \frac{\mathrm{NL}(F)}{2^N}$; "bias".

Criteria bounds

For all choice of ℓ fixed variables, $F[\ell]$ follows these properties

- $\sum_{i=1}^{\deg(F[\ell])} m_i[\ell] \geq (\sum_{i=1}^{\deg(F)} m_i) - \ell$,
- $\mathbf{m}_{F[\ell]}^* \geq \mathbf{m}_F^* - \lfloor \frac{\ell}{\min_{1 \leq i \leq \deg(F)} m_i} \rfloor$,
- $\delta_{\mathbf{m}_{F[\ell]}} \leq \delta_{\mathbf{m}_F} 2^\ell$.

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

F direct sum of monomials $\leftrightarrow$ vector $\mathbf{m}_F = [m_1, m_2, \cdots, m_k]$

Two recurrent criteria:

- $\mathbf{m}_F^*$ the number of nonzero values of $\mathbf{m}_F$,
- $\delta_{\mathbf{m}_F} = \frac{1}{2} - \frac{\mathrm{NL}(F)}{2^N}$; "bias".

Criteria bounds

For all choice of ℓ fixed variables, $F[\ell]$ follows these properties

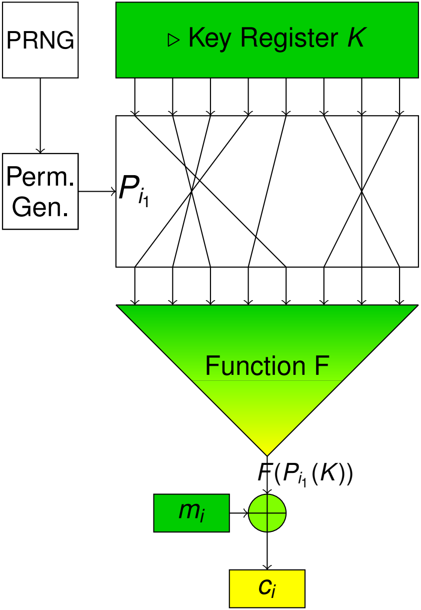
- $\sum_{i=1}^{\deg(F[\ell])} m_i[\ell] \geq (\sum_{i=1}^{\deg(F)} m_i) - \ell$,
- $\mathbf{m}_{F[\ell]}^* \geq \mathbf{m}_F^* - \lfloor \frac{\ell}{\min_{1 \leq i \leq \deg(F)} m_i} \rfloor$,
- $\delta_{\mathbf{m}_{F[\ell]}} \leq \delta_{\mathbf{m}_F} 2^\ell$.

Concrete bounds for (fast) algebraic attacks and correlation attacks for all ℓ:

$$\mathbf{m}_{F[\ell]}^* \leftrightarrow \text{upper bound on } \mathrm{AI}[\ell](F),$$
$$\delta_{\mathbf{m}_{F[\ell]}} \leftrightarrow \text{upper bound on } \mathrm{NL}[\ell](F).$$

Summary

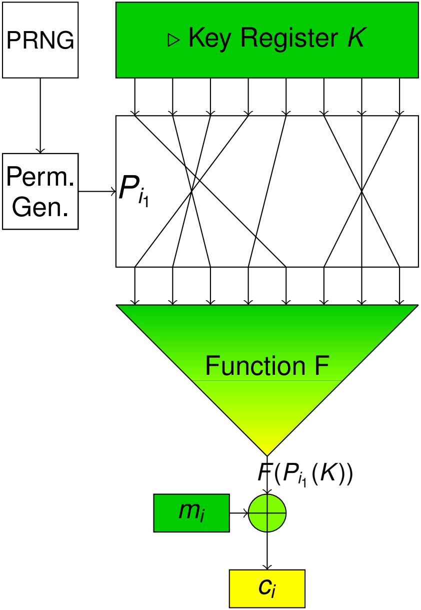
Filter Permutator: Hamming weight of F input



$$\psi_K : i \mapsto P_i(K)$$

$$Im(\psi) \subsetneq \mathbb{F}_2^N$$

Filter Permutator: Hamming weight of F input

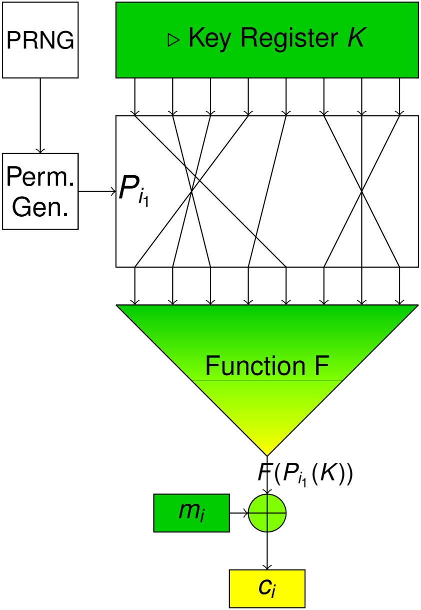


$$\psi_K : i \mapsto P_i(K)$$

$$Im(\psi) \subsetneq \mathbb{F}_2^N$$

$$\forall i,\ \mathrm{w_H}(P_i(K)) = \mathrm{w_H}(K)$$

Filter Permutator: Hamming weight of F input



$$\psi_K : i \mapsto P_i(K)$$

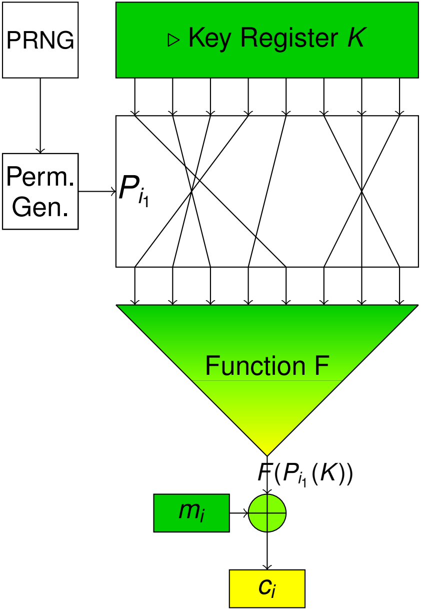
$$Im(\psi) \subsetneq \mathbb{F}_2^N$$

$$\forall i,\ \mathrm{w_H}(P_i(K)) = \mathrm{w_H}(K)$$

F should be studied on

$$E_{N,k} := \{x \mid \mathrm{w_H}(x) = k\}$$

Filter Permutator: Hamming weight of F input



$$\psi_K : i \mapsto P_i(K)$$

$$Im(\psi) \subsetneq \mathbb{F}_2^N$$

$$\forall i,\ \mathrm{w_H}(P_i(K)) = \mathrm{w_H}(K)$$

F should be studied on

$$E_{N,k} := \{x \mid \mathrm{w_H}(x) = k\}$$

$\rightarrow$ balancedness
$\rightarrow$ non-linearity
$\rightarrow$ algebraic immunity

Balancedness on constant Hamming weight input

$S_1 = x_1 + x_2 + \cdots + x_n \quad ; n-1$ resilient but constant for all k

Balancedness on constant Hamming weight input

$$S_1 = x_1 + x_2 + \cdots + x_n \quad ; n-1 \text{ resilient but constant for all } k$$

Weightwise Perfectly Balanced Function

Boolean function f defined over $\mathbb{F}_2^n$, is *weightwise perfectly balanced* (*WPB*):

$$\forall k \in [1, n-1], \mathrm{w_H}(f)_k = \frac{\binom{n}{k}}{2}, \text{ and, } f(0, \ldots, 0) = 0; \quad f(1, \ldots, 1) = 1.$$

Balancedness on constant Hamming weight input

$S_1 = x_1 + x_2 + \cdots + x_n$; $n - 1$ resilient but constant for all k

Weightwise Perfectly Balanced Function

Boolean function f defined over $\mathbb{F}_2^n$, is *weightwise perfectly balanced* (*WPB*):

$$\forall k \in [1, n-1], \mathrm{w_H}(f)_k = \frac{\binom{n}{k}}{2}, \text{ and, } f(0, \dots, 0) = 0; \quad f(1, \dots, 1) = 1.$$

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

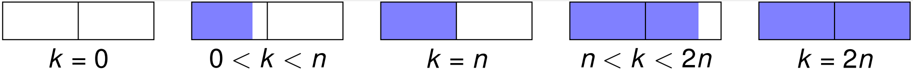
$$h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$



Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x,y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

$k = 0$ $\quad$ $0 < k < n$ $\quad$ $k = n$ $\quad$ $n < k < 2n$ $\quad$ $k = 2n$

case $k = 0$

$\mathrm{w_H}(x) = 0 \qquad \mathrm{w_H}(y) = 0$

$$f(0,\cdots,0) = g(0,\cdots,0) = f'(0,\cdots,0) = 0$$

h(0,0)=0

Balancedness on constant Hamming weight input

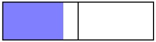
Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x,y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

$k = 0$ $\quad$ $0 < k < n$ $\quad$ $k = n$ $\quad$ $n < k < 2n$ $\quad$ $k = 2n$

case $0 < k < n$

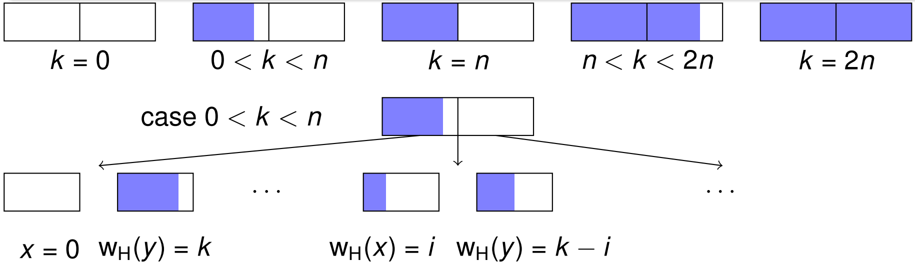


Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

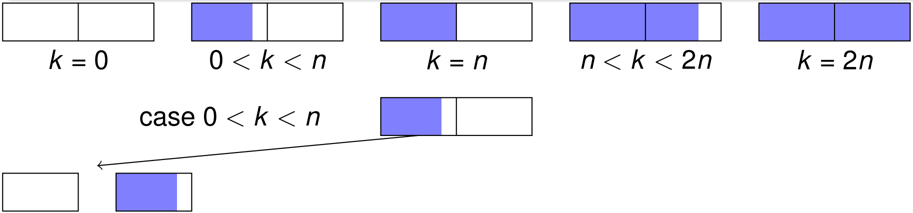


Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x,y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$



$x = 0$ $\mathrm{w_H}(y) = k$

case $x = 0$ $\qquad f(0, \cdots, 0) = f'(0, \cdots, 0) = 0$

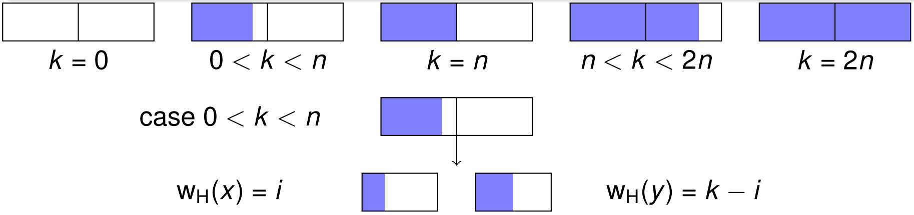
h(0,y)=g(y) $\qquad$ g balanced on $E_{n,k}$

Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x,y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

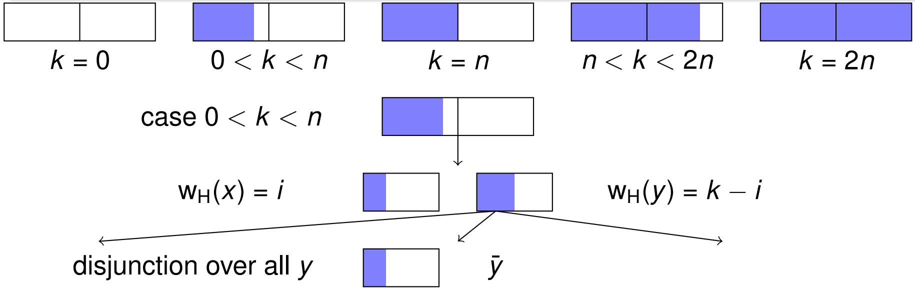


Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x,y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

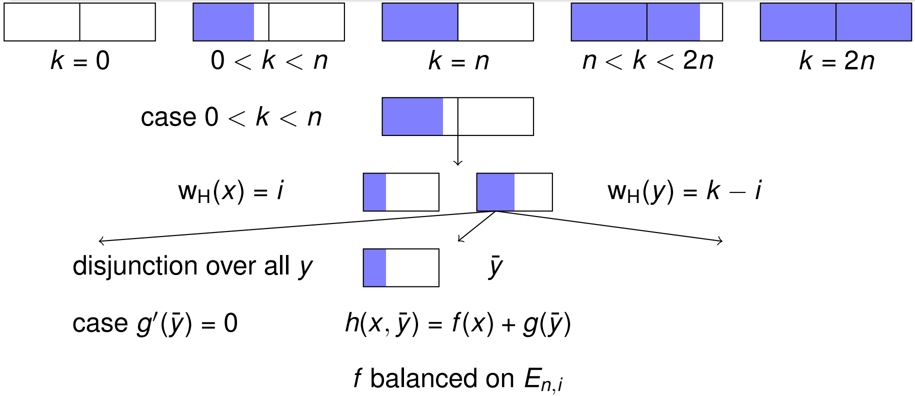


Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$

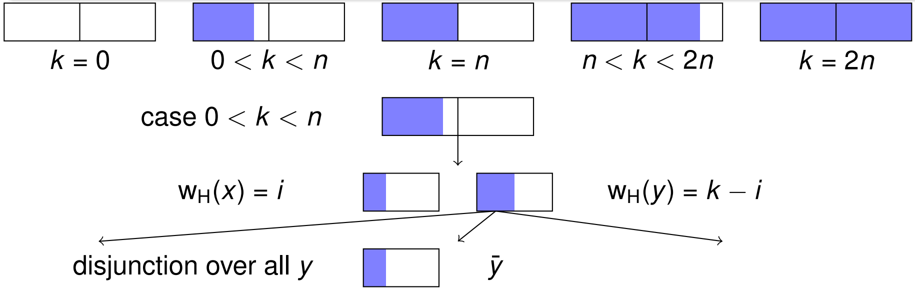


Balancedness on constant Hamming weight input

Secondary Construction of *WPB* Functions

From f, f', and g, 3 n-variable *WPB* functions and g' n-variable arbitrary function we build a $2n$-variable *WPB* function:

$$h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$$



case $g'(\bar{y}) = 1$ $\quad$ $h(x, \bar{y}) = f'(x) + g(\bar{y})$

f' balanced on $E_{n,i}$

Restricted non-linearity

Non-linearity over E

Let $E \subset \mathbb{F}_2^n$ and f any Boolean function defined over E.
$\mathrm{NL}_E(f) = \min_g\{d_H(f, g) \text{ over } E\}$, where g is an affine function over $\mathbb{F}_2^n$.

Upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E|}}{2}.$$

Restricted non-linearity

Upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in E} (-1)^{f(x)+a\cdot x} \Big|$$

$$\begin{aligned}
\sum_{a \in \mathbb{F}_2^n} \left(\sum_{x \in E} (-1)^{f(x)+a\cdot x} \right)^2 &= \sum_{x,y \in E} (-1)^{f(x)+f(y)} \sum_{a \in \mathbb{F}_2^n} (-1)^{a\cdot(x+y)} \\
&= ?
\end{aligned}$$

Restricted non-linearity

Upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a \in \mathbb{F}_2^n} \Big|\sum_{x \in E} (-1)^{f(x)+a \cdot x}\Big|$$

$$\begin{aligned}\sum_{a \in \mathbb{F}_2^n} \left(\sum_{x \in E} (-1)^{f(x)+a \cdot x}\right)^2 &= \sum_{x,y \in E} (-1)^{f(x)+f(y)} \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot (x+y)} \\ &= ?\end{aligned}$$

$$\text{if } x + y \neq 0, \quad \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot (x+y)} = 0$$

Restricted non-linearity

Upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \Big|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\Big|$$

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^n}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 &= \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(x+y)} \\ &= 2^n\,|E|.\end{aligned}$$

$$\text{else } x = y, \quad \sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(0)} = 2^n$$

Restricted non-linearity

Upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \Big|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\Big|$$

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^n}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 &= \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(x+y)} \\ &= 2^n\,|E|.\end{aligned}$$

$$\text{else } x = y,\quad \sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(0)} = 2^n$$

maximum always greater than mean; $\max \geq \sqrt{|E|}$.

Restricted non-linearity

Better upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E + \lambda|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \left|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right|$$

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^n}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 &= \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(x+y)} \\ &= 2^n\,|E|.\end{aligned}$$

$$\text{else } x = y, \quad \sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(0)} = 2^n$$

maximum always greater than mean; max $\geq \sqrt{|E|}$.

Restricted non-linearity

Better upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E+\lambda|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \Big|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\Big|$$

$$\begin{aligned}\sum_{a\in F}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 &= \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in F}(-1)^{a\cdot(x+y)} \\ &= \;?\end{aligned}$$

$$\text{else } x = y, \quad \sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(0)} = 2^n$$

maximum always greater than mean; $\max \geq \sqrt{|E|}$.

Restricted non-linearity

Better upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E+\lambda|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \left|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right|$$

$$\begin{aligned}\sum_{a\in F}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 &= \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in F}(-1)^{a\cdot(x+y)} \\ &= \ ?\end{aligned}$$

$$\text{if } x+y\in F^{\perp}, \quad \sum_{a\in F}(-1)^{a\cdot(0)} = |F|$$

maximum always greater than mean; $\max \geq \sqrt{|E|}$.

Restricted non-linearity

Better upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E+\lambda|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \left|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right|$$

$$\sum_{a\in F}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 = \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in F}(-1)^{a\cdot(x+y)}$$

$$= |F|\Big(\sum_{\substack{(x,y)\in E^2\\ x+y\in F^\perp}}(-1)^{f(x)+f(y)}\Big).$$

if $x+y\in F^\perp$, $\quad \sum_{a\in F}(-1)^{a\cdot(0)} = |F|$

maximum always greater than mean; $\max \geq \sqrt{|E|}$.

Restricted non-linearity

Better upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E+\lambda|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \Big|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\Big|$$

$$\sum_{a\in F}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 = \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in F}(-1)^{a\cdot(x+y)}$$

$$= |F|\Big(|E| + \sum_{\substack{(x,y)\in E^2\\ 0\neq x+y\in F^\perp}}(-1)^{f(x)+f(y)}\Big).$$

if $x+y\in F^\perp$, $\quad \sum_{a\in F}(-1)^{a\cdot(0)} = |F|$

maximum always greater than mean; $\max \geq \sqrt{|E|}$.

Restricted non-linearity

Better upper bound on NL_E

For every subset E of $\mathbb{F}_2^n$ and every Boolean function f defined over E, we have:

$$\mathrm{NL}_E(f) \leq \frac{|E|}{2} - \frac{\sqrt{|E + \lambda|}}{2}.$$

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} \Big|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\Big|$$

$$\begin{aligned}\sum_{a\in F}\left(\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right)^2 &= \sum_{x,y\in E}(-1)^{f(x)+f(y)}\sum_{a\in F}(-1)^{a\cdot(x+y)} \\ &= |F|(|E| + \sum_{\substack{(x,y)\in E^2 \\ 0\neq x+y\in F^\perp}} (-1)^{f(x)+f(y)}).\end{aligned}$$

$$\text{if } x + y \in F^\perp, \quad \sum_{a\in F}(-1)^{a\cdot(0)} = |F|$$

λ can be assumed > 0 for some cases, in particular $\mathrm{NL}_{E_{n,k}}(f) < \frac{\binom{n}{k}}{2} - \frac{\sqrt{\binom{n}{k}}}{2}$.

Non-linearity degradation

Bent functions with NL_k null

For all even $n \geq 4$ there exists quadratic bent functions such that $\forall k$, $\mathrm{NL}_k = 0$.

Non-linearity degradation

Bent functions with NL_k null

For all even $n \geq 4$ there exists quadratic bent functions such that $\forall k$, $\mathrm{NL}_k = 0$.

$$\begin{aligned}\forall k,\ \mathrm{NL}_k(f) = 0 \quad &\Leftrightarrow \quad f(x) = \varphi_0(x) + \sum_{i=1}^{n} \varphi_i(x)\, x_i \\ &\Leftrightarrow \quad f(x) = \ell'_0(x) + \sum_{i=1}^{n} S_i(x)\ell'_i(x)\end{aligned}$$

Non-linearity degradation

Bent functions with NL_k null

For all even $n \geq 4$ there exists quadratic bent functions such that $\forall k$, $\mathrm{NL}_k = 0$.

$$
\begin{aligned}
\forall k,\ \mathrm{NL}_k(f) = 0 \quad &\Leftrightarrow \quad f(x) = \varphi_0(x) + \sum_{i=1}^{n} \varphi_i(x)\, x_i \\
&\Leftrightarrow \quad f(x) = \ell'_0(x) + \sum_{i=1}^{n} S_i(x)\ell'_i(x) \\
f \text{ quadratic} \quad &\Leftrightarrow \quad f(x) = S_1\ell(x) + \epsilon S_2(x)
\end{aligned}
$$

Non-linearity degradation

Bent functions with NL_k null

For all even $n \geq 4$ there exists quadratic bent functions such that $\forall k$, $\mathrm{NL}_k = 0$.

$$\begin{aligned} \forall k,\ \mathrm{NL}_k(f) = 0 \quad &\Leftrightarrow \quad f(x) = \varphi_0(x) + \sum_{i=1}^{n} \varphi_i(x)\, x_i \\ &\Leftrightarrow \quad f(x) = \ell'_0(x) + \sum_{i=1}^{n} S_i(x)\ell'_i(x) \\ f \text{ quadratic} \quad &\Leftrightarrow \quad f(x) = S_1\ell(x) + \epsilon S_2(x) \end{aligned}$$

Bent functions and simplectic form [Car10]

f with associated simplectic form; $(x, y) \to f(x, y) + f(x) + f(y) + f(0)$ is bent iff the kernel $E = \{x \in F_2^n; \forall y \in F_2^n, f(x + y) + f(x) + f(y) + f(0) = 0\}$ is equal to $\{0\}$.

$$\text{simplectic form:} \qquad S_1(y)\ell(x) + S(x)\ell(y) + \epsilon \sum_{1 \leq j \neq i \leq n} x_j y_i,$$

Non-linearity degradation

Bent functions and simplectic form [Car10]

f with associated simplectic form; $(x, y) \rightarrow f(x, y) + f(x) + f(y) + f(0)$ is bent iff the kernel $E = \{x \in F_2^n; \forall y \in F_2^n, f(x + y) + f(x) + f(y) + f(0) = 0\}$ is equal to $\{0\}$.

$$\text{simplectic form:} \quad S_1(y)\ell(x) + S(x)\ell(y) + \epsilon \sum_{1 \leq j \neq i \leq n} x_j y_i,$$

we fix $\epsilon = 1$ and $\ell(1, \cdot, 1) = 0$, and study the equations defining E:

Non-linearity degradation

Bent functions and simplectic form [Car10]

f with associated simplectic form; $(x, y) \to f(x, y) + f(x) + f(y) + f(0)$ is bent iff the kernel $E = \{x \in F_2^n; \forall y \in F_2^n, f(x+y) + f(x) + f(y) + f(0) = 0\}$ is equal to $\{0\}$.

$$\text{simplectic form:} \quad S_1(y)\ell(x) + S(x)\ell(y) + \epsilon \sum_{1 \leq j \neq i \leq n} x_j y_i,$$

we fix $\epsilon = 1$ and $\ell(1, \cdot, 1) = 0$, and study the equations defining E:

$$(L_i) : \ell(x) + \ell_i \sum_{j=1}^{n} x_j + \sum_{j \neq i} x_j = 0,$$

Non-linearity degradation

Bent functions and simplectic form [Car10]

f with associated simplectic form; $(x,y) \to f(x,y)+f(x)+f(y)+f(0)$ is bent iff the kernel $E = \{x \in F_2^n; \forall y \in F_2^n, f(x+y)+f(x)+f(y)+f(0) = 0\}$ is equal to $\{0\}$.

$$\text{simplectic form:} \quad S_1(y)\ell(x) + S(x)\ell(y) + \epsilon \sum_{1 \le j \ne i \le n} x_j y_i,$$

we fix $\epsilon = 1$ and $\ell(1,\cdot,1) = 0$, and study the equations defining E:

$$(L_i) : \ell(x) + \ell_i \sum_{j=1}^{n} x_j + \sum_{j \ne i} x_j = 0,$$

$$(L_i + L_{i'}) : (\ell_i + \ell_{i'}) \sum_{j=1}^{n} x_j + x_i + x_{i'} = 0.$$

Non-linearity degradation

Bent functions and simplectic form [Car10]

f with associated simplectic form; $(x, y) \to f(x, y) + f(x) + f(y) + f(0)$ is bent iff the kernel $E = \{x \in F_2^n; \forall y \in F_2^n, f(x + y) + f(x) + f(y) + f(0) = 0\}$ is equal to $\{0\}$.

$$\text{simplectic form:} \quad S_1(y)\ell(x) + S(x)\ell(y) + \epsilon \sum_{1 \le j \ne i \le n} x_j y_i,$$

we fix $\epsilon = 1$ and $\ell(1, \cdot, 1) = 0$, and study the equations defining E:

$$(L_i) : \ell(x) + \ell_i \sum_{j=1}^{n} x_j + \sum_{j \ne i} x_j = 0,$$

$$(L_i + L_{i'}) : (\ell_i + \ell_{i'}) \sum_{j=1}^{n} x_j + x_i + x_{i'} = 0.$$

$$\text{if } x \mid \sum_{j=1}^{n} x_j = 0 \Rightarrow \text{ all bits are the same }; x = (1, \cdots, 1) \Rightarrow (L_i) = 1,$$

Non-linearity degradation

Bent functions and simplectic form [Car10]

f with associated simplectic form; $(x,y) \to f(x,y)+f(x)+f(y)+f(0)$ is bent iff the kernel $E = \{x \in F_2^n; \forall y \in F_2^n, f(x+y)+f(x)+f(y)+f(0)=0\}$ is equal to $\{0\}$.

$$\text{simplectic form:} \quad S_1(y)\ell(x) + S(x)\ell(y) + \epsilon \sum_{1\leq j\neq i\leq n} x_j y_i,$$

we fix $\epsilon = 1$ and $\ell(1,\cdot,1) = 0$, and study the equations defining E:

$$(L_i) : \ell(x) + \ell_i \sum_{j=1}^{n} x_j + \sum_{j\neq i} x_j = 0,$$

$$(L_i + L_{i'}) : (\ell_i + \ell_{i'}) \sum_{j=1}^{n} x_j + x_i + x_{i'} = 0.$$

$$\text{if } x \mid \sum_{j=1}^{n} x_j = 0 \Rightarrow \text{ all bits are the same }; x = (1,\cdots,1) \Rightarrow (L_i) = 1,$$

$$\text{if } x \mid \sum_{j=1}^{n} x_j = 1 \Rightarrow (\sum_{i=1}^{n} L_i) : \sum_{i=1}^{n} \ell_i + \sum_{j=1}^{n} x_j = 1.$$

Restricted algebraic immunity

Algebraic immunity over E

Let f defined over a set E:

$$\mathrm{AI}_E(f) = \min\{\deg(g); g \cdot f = 0 \text{ or } g \cdot (f+1) \text{ over } E \text{ and } g \neq 0 \text{ over } E\}.$$

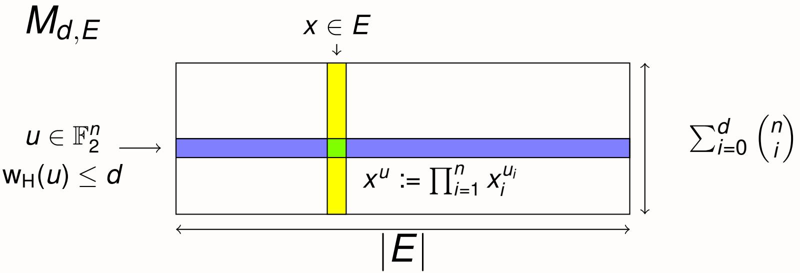
Restricted algebraic immunity

Algebraic immunity over E

Let f defined over a set E:

$$\mathrm{AI}_E(f) = \min\{\deg(g); g \cdot f = 0 \text{ or } g \cdot (f+1) \text{ over } E \text{ and } g \neq 0 \text{ over } E\}.$$

Upper bound on algebraic immunity



$$\mathrm{AI}_E(f) \leq \min_d\{\mathrm{rank}(M_{d,E}) > |E|/2\}$$

Restricted algebraic immunity

Upper bound on algebraic immunity

$$\mathrm{AI}_E(f) \leq \min_d \{\mathrm{rank}(M_{d,E}) > |E|/2\}$$

We first prove:

$$\mathrm{rank}(M_{d,E}) + \mathrm{rank}(M_{e,E}) > |E| \Rightarrow \exists g, h \mid g \cdot f = h \text{ over } E,$$

where $g \neq 0, \deg(g) \leq e$, and $\deg(h) \leq d$.

Restricted algebraic immunity

Upper bound on algebraic immunity

$$\mathrm{AI}_E(f) \leq \min_d \{\mathrm{rank}(M_{d,E}) > |E|/2\}$$

We first prove:

$$\mathrm{rank}(M_{d,E}) + \mathrm{rank}(M_{e,E}) > |E| \Rightarrow \exists g, h \mid g \cdot f = h \text{ over } E,$$

where $g \neq 0, \deg(g) \leq e$, and $\deg(h) \leq d$.

$\mathcal{F}_d$: max size free family of restrictions to E of degree $\leq d$,
$\mathcal{F}_e f$: products of elements of $\mathcal{F}_e$ with f.

Restricted algebraic immunity

Upper bound on algebraic immunity

$$\mathrm{AI}_E(f) \le \min_d\{\mathrm{rank}(M_{d,E}) > |E|/2\}$$

We first prove:

$$\mathrm{rank}(M_{d,E}) + \mathrm{rank}(M_{e,E}) > |E| \Rightarrow \exists g, h \mid g \cdot f = h \text{ over } E,$$

where $g \neq 0, \deg(g) \le e$, and $\deg(h) \le d$.

$\mathcal{F}_d$: max size free family of restrictions to E of degree $\le d$,
$\mathcal{F}_e f$: products of elements of $\mathcal{F}_e$ with f.

If $|\mathcal{F}_d| + |\mathcal{F}_e f| > |E|$ then $\exists$ lin. combinaison giving 0 with not all null coeff.
The part from $\mathcal{F}_e$; g is not null over E ($\mathcal{F}_d$ is free).

Restricted algebraic immunity

Upper bound on algebraic immunity

$$\mathrm{AI}_E(f) \leq \min_d \{\mathrm{rank}(M_{d,E}) > |E|/2\}$$

We first prove:

$$\mathrm{rank}(M_{d,E}) + \mathrm{rank}(M_{e,E}) > |E| \Rightarrow \exists g, h \mid g \cdot f = h \text{ over } E,$$

where $g \neq 0, \deg(g) \leq e$, and $\deg(h) \leq d$.

$\mathcal{F}_d$: max size free family of restrictions to E of degree $\leq d$,
$\mathcal{F}_e f$: products of elements of $\mathcal{F}_e$ with f.

If $|\mathcal{F}_d| + |\mathcal{F}_e f| > |E|$ then $\exists$ lin. combinaison giving 0 with not all null coeff.
The part from $\mathcal{F}_e$; g is not null over E ($\mathcal{F}_d$ is free).

Taking $d = e$,

$$\text{if } g = h; \quad f \cdot g + h = (f+1) \cdot g = 0$$

Restricted algebraic immunity

Upper bound on algebraic immunity

$$\mathrm{AI}_E(f) \leq \min_d \{\mathrm{rank}(M_{d,E}) > |E|/2\}$$

We first prove:

$$\mathrm{rank}(M_{d,E}) + \mathrm{rank}(M_{e,E}) > |E| \Rightarrow \exists g, h \mid g \cdot f = h \text{ over } E,$$

where $g \neq 0, \deg(g) \leq e$, and $\deg(h) \leq d$.

$\mathcal{F}_d$: max size free family of restrictions to E of degree $\leq d$,
$\mathcal{F}_e f$: products of elements of $\mathcal{F}_e$ with f.

If $|\mathcal{F}_d| + |\mathcal{F}_e f| > |E|$ then $\exists$ lin. combinaison giving 0 with not all null coeff.
The part from $\mathcal{F}_e$; g is not null over E ($\mathcal{F}_d$ is free).

Taking $d = e$,

$$\text{if } g = h; \quad f \cdot g + h = (f+1) \cdot g = 0$$

$$\text{else } g \cdot f = h; \quad (g + h) \cdot f = 0$$

Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d,k,n-k)}$$

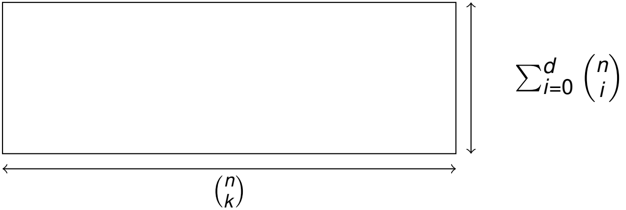
Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d,k,n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$
$\mathrm{w_H}(u) \leq d$



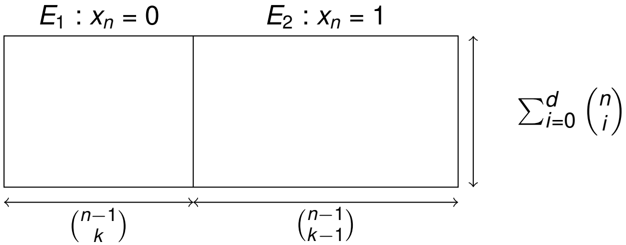
Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d, k, n-k)}$$

$$M_{n,d,k}$$

$$u \in \mathbb{F}_2^n$$
$$\mathrm{w_H}(u) \leq d$$



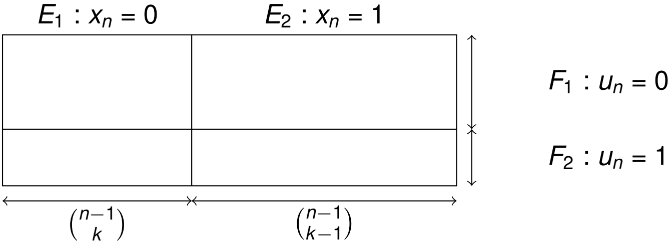
Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d, k, n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$
$\mathrm{w_H}(u) \leq d$



Restricted algebraic immunity

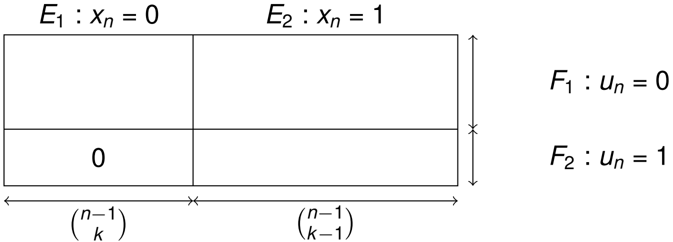
Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d, k, n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$

$\mathrm{w_H}(u) \leq d$



Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d,k,n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$

$\mathrm{w_H}(u) \leq d$

$$\begin{array}{c|c|c}
 & E_1 : x_n = 0 & E_2 : x_n = 1 \\
\hline
F_1 : u_n = 0 & M_{n-1,d,k} & \\
\hline
F_2 : u_n = 1 & 0 & \\
\hline
 & \binom{n-1}{k} & \binom{n-1}{k-1}
\end{array}$$

Restricted algebraic immunity

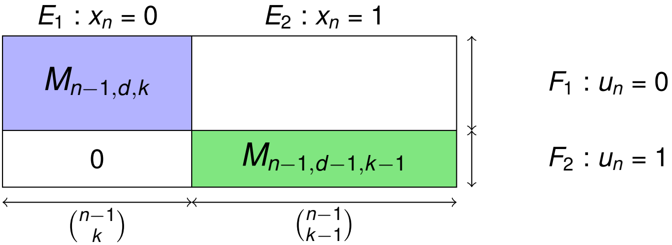
Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d, k, n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$

$\mathrm{w_H}(u) \leq d$



Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\operatorname{rank}(M_{n,d,k}) = \binom{n}{\min(d,k,n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$

$w_H(u) \le d$

$$\begin{array}{c|c|c|c}
 & E_1 : x_n = 0 & E_2 : x_n = 1 & \\
\hline
 & M_{n-1,d,k} & & F_1 : u_n = 0 \\
\hline
 & 0 & M_{n-1,d-1,k-1} & F_2 : u_n = 1 \\
\hline
 & \binom{n-1}{k} & \binom{n-1}{k-1} &
\end{array}$$

First we show: $\operatorname{rank}(M_{n,d,k}) = \operatorname{rank}(M) + \operatorname{rank}(M)$

$\Leftrightarrow$ if f null over E_1 (in M's kernel) then all monomials of f contain u_n.

Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d, k, n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$

$\mathrm{w_H}(u) \leq d$

$$\begin{array}{c|c|c} & E_1 : x_n = 0 & E_2 : x_n = 1 \\ \hline F_1 : u_n = 0 & M_{n-1,d,k} & \\ \hline F_2 : u_n = 1 & 0 & M_{n-1,d-1,k-1} \\ \hline & \binom{n-1}{k} & \binom{n-1}{k-1} \end{array}$$

First we show: $\mathrm{rank}(M_{n,d,k}) = \mathrm{rank}(M) + \mathrm{rank}(M)$

$\Leftrightarrow$ if f null over E_1 (in M's kernel) then all monomials of f contain u_n.

$$f(x_1, \cdots, x_n) = x_n \cdot g(x_1, \cdots, x_{n-1}) + h(x_1, \cdots, x_{n-1})$$

Restricted algebraic immunity

Algebraic immunity on constant Hamming weight input

$$\mathrm{rank}(M_{n,d,k}) = \binom{n}{\min(d,k,n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$
$\mathrm{w_H}(u) \leq d$

$$\begin{array}{c|c|c|c}
 & E_1 : x_n = 0 & E_2 : x_n = 1 & \\
\hline
F_1 : u_n = 0 & M_{n-1,d,k} & & \\
\hline
F_2 : u_n = 1 & 0 & M_{n-1,d-1,k-1} & \\
\hline
 & \binom{n-1}{k} & \binom{n-1}{k-1} &
\end{array}$$

First we show: $\mathrm{rank}(M_{n,d,k}) = \mathrm{rank}(M) + \mathrm{rank}(M)$

$\Leftrightarrow$ if f null over E_1 (in M's kernel) then all monomials of f contain u_n.

$$f(x_1, \cdots, x_n) = x_n \cdot g(x_1, \cdots, x_{n-1}) + h(x_1, \cdots, x_{n-1})$$

f null over all entries s.t. $x_n = 0 \Rightarrow h(x) = 0 \Rightarrow f = x_n \cdot g(x_1, \cdots, x_{n-1})$

$$\mathrm{rank}(M_{n,d,k}) = \mathrm{rank}(M_{n-1,d,k}) + \mathrm{rank}(M_{n-1,d-1,k-1})$$

Restricted algebraic immunity

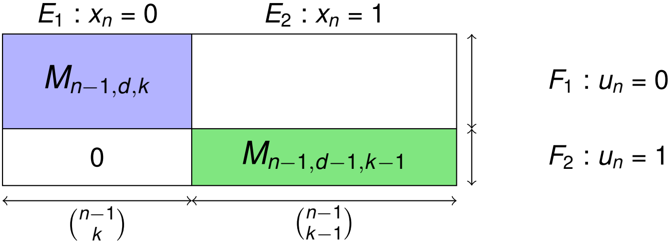
Algebraic immunity on constant Hamming weight input

$$\operatorname{rank}(M_{n,d,k}) = \binom{n}{\min(d, k, n-k)}$$

$M_{n,d,k}$

$u \in \mathbb{F}_2^n$

$w_H(u) \leq d$



First we show: $\operatorname{rank}(M_{n,d,k}) = \operatorname{rank}(M) + \operatorname{rank}(M)$

$\Leftrightarrow$ if f null over E_1 (in M's kernel) then all monomials of f contain u_n.

$$f(x_1, \cdots, x_n) = x_n \cdot g(x_1, \cdots, x_{n-1}) + h(x_1, \cdots, x_{n-1})$$

f null over all entries s.t. $x_n = 0 \Rightarrow h(x) = 0 \Rightarrow f = x_n \cdot g(x_1, \cdots, x_{n-1})$

$$\operatorname{rank}(M_{n,d,k}) = \operatorname{rank}(M_{n-1,d,k}) + \operatorname{rank}(M_{n-1,d-1,k-1})$$

initialisation: $d \geq k$ or $d \geq n-k$ gives canonical base; $\operatorname{rank}(M) = \binom{n}{k}$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

$$h(x, y) \text{ annihilator of } F \text{ over } E_{n+m,k}$$

$$\exists (a, b), \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, \quad h(a, b) = 1$$

Algebraic immunity degradation

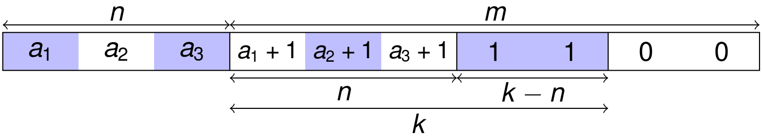
Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

$$h(x, y) \text{ annihilator of } F \text{ over } E_{n+m,k}$$

$$\exists (a, b), \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, \quad h(a, b) = 1$$



Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

$$h(x, y) \text{ annihilator of } F \text{ over } E_{n+m,k}$$

$$\exists (a, b), \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, \quad h(a, b) = 1$$

$$\overbrace{a_1 \quad a_2 \quad a_3}^{n} \quad \overbrace{\underbrace{\underbrace{a_1+1 \quad a_2+1 \quad a_3+1}_{n} \quad \underbrace{1 \quad 1}_{k-n}}_{k} \quad 0 \quad 0}^{m}$$

$$L(x) = (x_1 + 1, x_2 + 1, \ldots, x_n + 1, 1, \ldots, 1, 0, \ldots, 0),$$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

$$h(x, y) \text{ annihilator of } F \text{ over } E_{n+m,k}$$

$$\exists (a, b), \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, \quad h(a, b) = 1$$

n			m						
a_1	a_2	a_3	$a_1 + 1$	$a_2 + 1$	$a_3 + 1$	1	1	0	0
			n			$k - n$			
			k						

$$L(x) = (x_1 + 1, x_2 + 1, \ldots, x_n + 1, 1, \ldots, 1, 0, \ldots, 0),$$

$$L(a) = b \text{ then } h(x, L(x)) \neq 0, \text{ and } \forall x : \ h(x, L(x))[f(x) + g(L(x))] = 0.$$

Algebraic immunity degradation

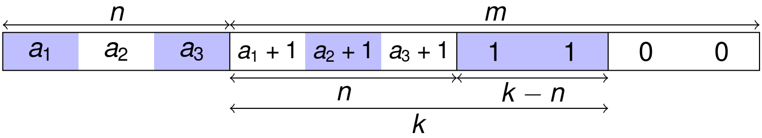
Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

$$h(x, y) \text{ annihilator of } F \text{ over } E_{n+m,k}$$

$$\exists (a, b), \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, \quad h(a, b) = 1$$



$$L(x) = (x_1 + 1, x_2 + 1, \ldots, x_n + 1, 1, \ldots, 1, 0, \ldots, 0),$$

$$L(a) = b \text{ then } h(x, L(x)) \neq 0, \text{ and } \forall x : h(x, L(x))[f(x) + g(L(x))] = 0.$$

$$\text{If } g(b) = 0, \quad [h(x, L(x))(g(L(x)) + 1)]f = 0; \quad \Rightarrow \mathrm{AI}(f) \leq \deg(g) + \deg(h),$$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

$$h(x, y) \text{ annihilator of } F \text{ over } E_{n+m,k}$$

$$\exists (a, b), \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, \quad h(a, b) = 1$$

$$\overbrace{a_1 \quad a_2 \quad a_3}^{n} \quad \overbrace{\underbrace{\underbrace{a_1+1 \quad a_2+1 \quad a_3+1}_{n} \quad \underbrace{1 \quad 1}_{k-n}}_{k} \quad 0 \quad 0}^{m}$$

$$L(x) = (x_1 + 1, x_2 + 1, \dots, x_n + 1, 1, \dots, 1, 0, \dots, 0),$$

$$L(a) = b \text{ then } h(x, L(x)) \neq 0, \text{ and } \forall x: \; h(x, L(x))[f(x) + g(L(x))] = 0.$$

$$\text{If } g(b) = 0, \quad [h(x, L(x))(g(L(x)) + 1)]f = 0; \quad \Rightarrow \mathrm{AI}(f) \leq \deg(g) + \deg(h),$$

$$\text{else } g(b) = 1, \quad [h(x, L(x))g(L(x))](f + 1) = 0; \quad \Rightarrow \mathrm{AI}(f) \leq \deg(g) + \deg(h).$$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

Example of direct sum reaching the bound

$$f(x_1, x_2, x_3) = x_1 + x_2 x_3, \quad \mathrm{AI}(f) = 2$$

$$g(x_4, x_5, x_6) = x_4 + x_5 + x_6, \quad \deg(g) = 1$$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

Example of direct sum reaching the bound

$$f(x_1, x_2, x_3) = x_1 + x_2 x_3, \quad \mathrm{AI}(f) = 2$$

$$g(x_4, x_5, x_6) = x_4 + x_5 + x_6, \quad \deg(g) = 1$$

$$F = f + g \quad \mathrm{AI}_3(F) \geq \mathrm{AI}(f) - \deg(g) \Rightarrow \mathrm{AI}_3(F) \geq 1$$

Algebraic immunity degradation

Direct sum and AI_k degradation

Let F be the direct sum of f and g of n and m variables; if $n \leq k \leq m$ then:

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

Example of direct sum reaching the bound

$$f(x_1, x_2, x_3) = x_1 + x_2 x_3, \quad \mathrm{AI}(f) = 2$$

$$g(x_4, x_5, x_6) = x_4 + x_5 + x_6, \quad \deg(g) = 1$$

$$F = f + g \quad \mathrm{AI}_3(F) \geq \mathrm{AI}(f) - \deg(g) \Rightarrow \mathrm{AI}_3(F) \geq 1$$

$$x_2(f + g) = x_2(1 + \sum_{i=1}^{6} x_i) = x_2(1 + S_1)$$

$$S_1(x) = 1 \text{ for odd k } \Rightarrow \mathrm{AI}_3(F) = 1$$

Summary

Conclusion and Open Problems

Filter Permutator optimal for FHE,
bringing new constraints on filtering function:

- higher number of variables with simpler circuit,
- resistant even when some inputs are known,
- robust on particular sets of inputs.

Conclusion and Open Problems

Filter Permutator optimal for FHE,
bringing new constraints on filtering function:

- ◇ higher number of variables with simpler circuit,
- ◇ resistant even when some inputs are known,
- ◇ robust on particular sets of inputs.

Still open questions ?

- ◇ Low cost functions without direct sums ?
- ◇ Simplest function providing security ?
- ◇ Concrete values of recurrent criteria for all functions ?
- ◇ Functions maximizing NL_k; AI_k ?
- ◇ Fixed Hamming weight input and cryptanalysis ?
- ◇ $\cdots$?

Conclusion and Open Problems

Filter Permutator optimal for FHE,
bringing new constraints on filtering function:

- ◇ higher number of variables with simpler circuit,
- ◇ resistant even when some inputs are known,
- ◇ robust on particular sets of inputs.

Still open questions ?

- ◇ Low cost functions without direct sums ?
- ◇ Simplest function providing security ?
- ◇ Concrete values of recurrent criteria for all functions ?
- ◇ Functions maximizing NL_k; AI_k ?
- ◇ Fixed Hamming weight input and cryptanalysis ?
- ◇ $\cdots$?

Thanks for your attention!