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

Pierrick MÉAUX

École normale supérieure, INRIA, CNRS, PSL

Boolean Functions and their Applications (BFA) — Os, Norway
Tuesday July 4

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

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

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

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

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

Fully Homomorphic Encryption

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

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

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

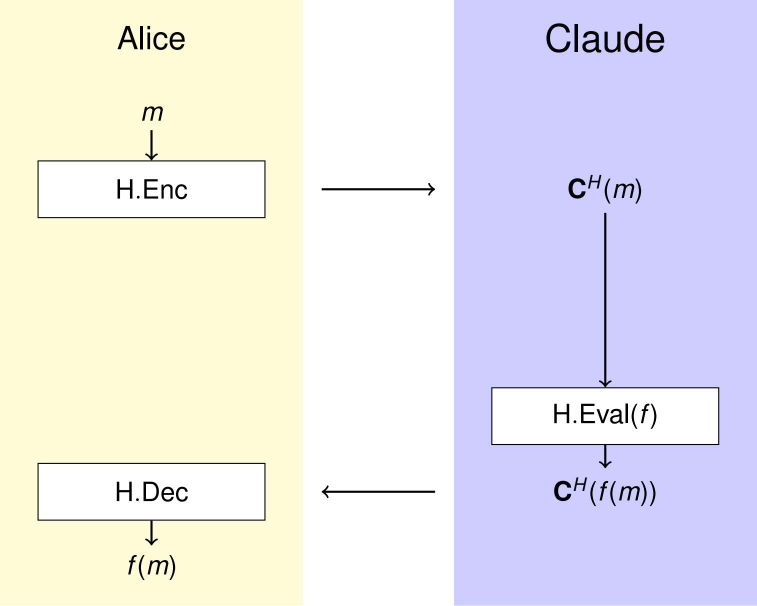
$$\boxed{x_1} \quad \cdot \quad \boxed{x_2} \quad = \quad \boxed{x_1 \cdot x_2}$$

Bottlenecks:

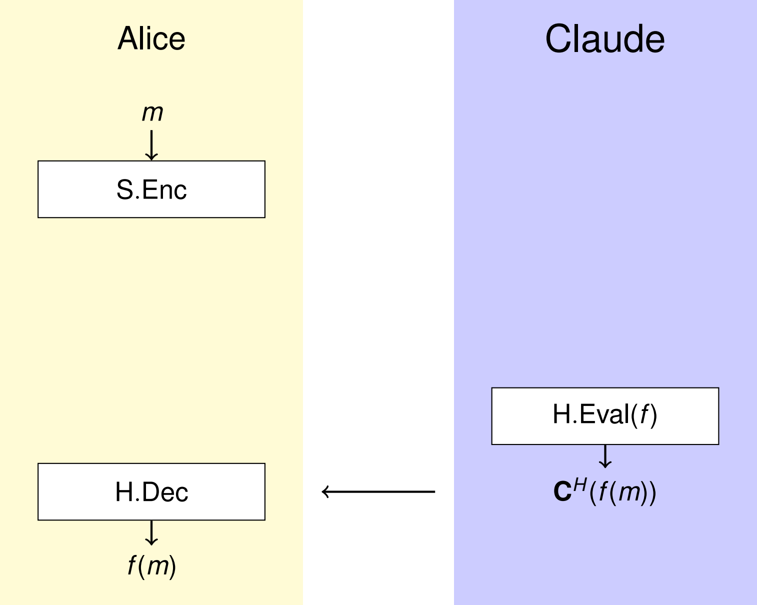
$\rightarrow$ high cost when high level of error

$\rightarrow$ high expansion factor

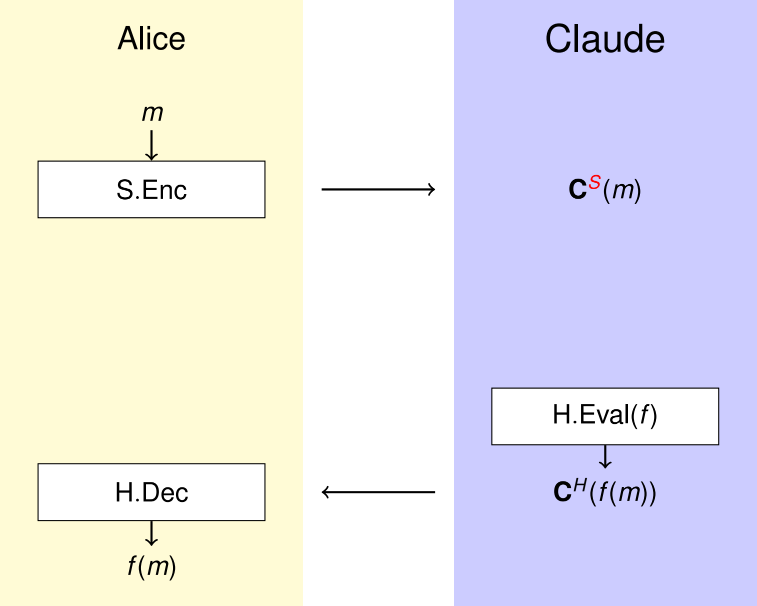
FHE Framework



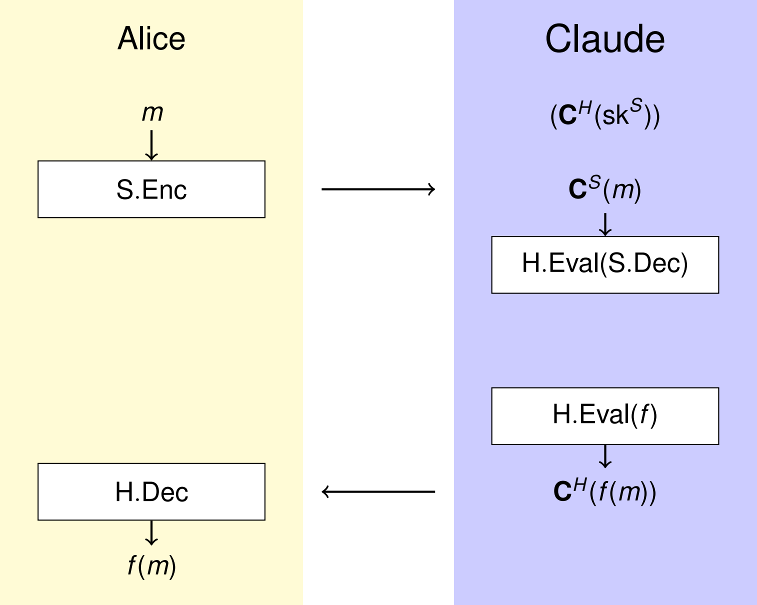
SE-HE Hybrid Framework



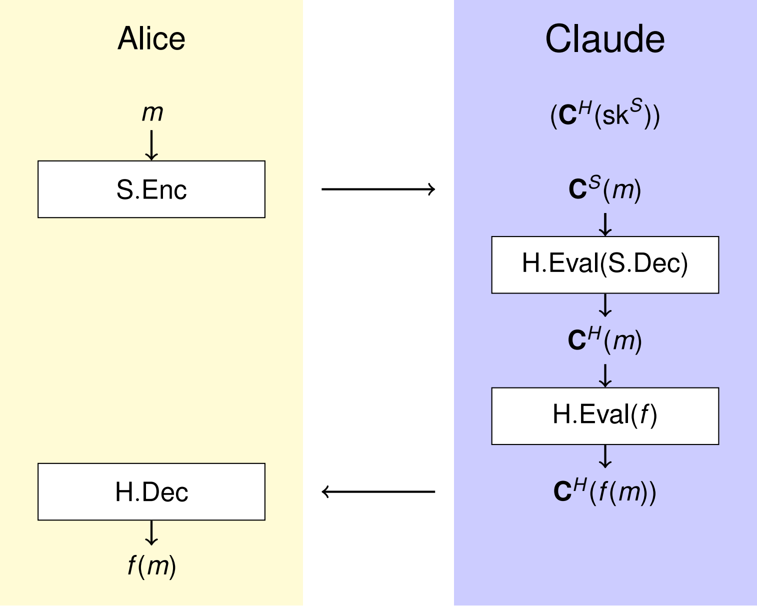
SE-HE Hybrid Framework



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

Optimize S.Dec circuit: Minimize homomorphic error growth

In practice for time and space constraints:

- $\approx$ 1000 homomorphic additions/multiplications
- total multiplicative depth < 10

SE adapted to FHE

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

Optimize S.Dec circuit: Minimize homomorphic error growth

In practice for time and space constraints:

- $\approx$ 1000 homomorphic additions/multiplications
- total multiplicative depth < 10

Block ciphers:

AES[GHS12,CLT14], SIMON[LN14], PRINCE[DSES14], LowMC[ARS+15]

$\rightarrow$ too many rounds

Stream ciphers:

Trivium, Kreyvium[CCF+15]

$\rightarrow$ increasing complexity

Summary

Filter Permutator

Joint work with:

Anthony Journault, François-Xavier Standaert and Claude Carlet,

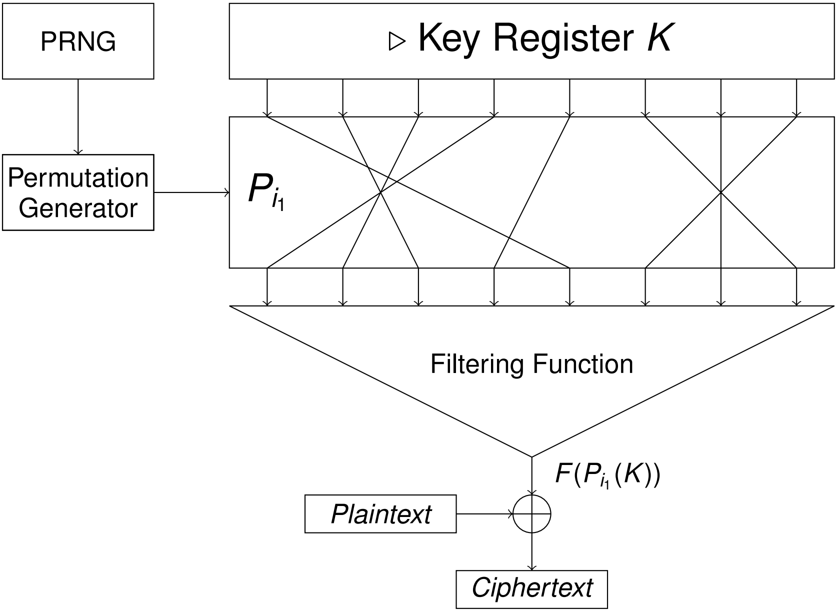
presented at Eurocrypt 2016,

title:

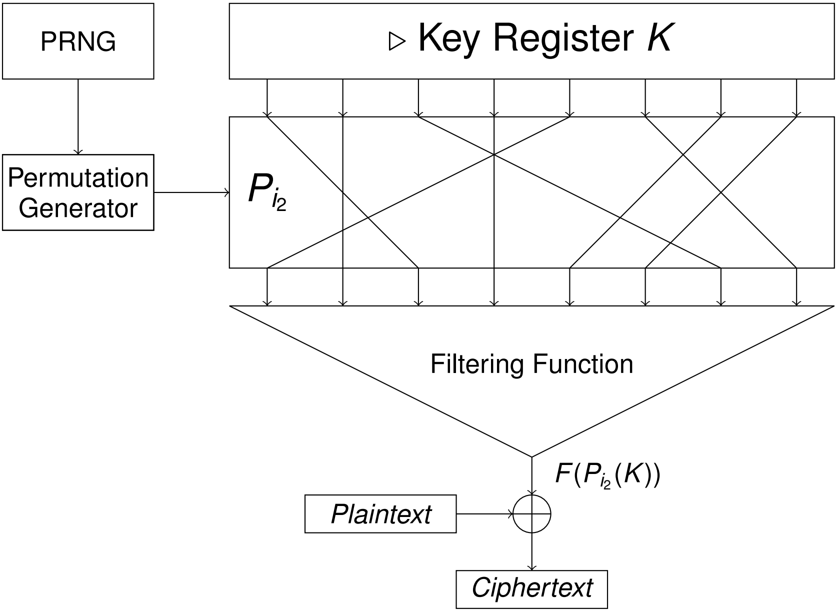
Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts.

ePrint: 254 (2016).

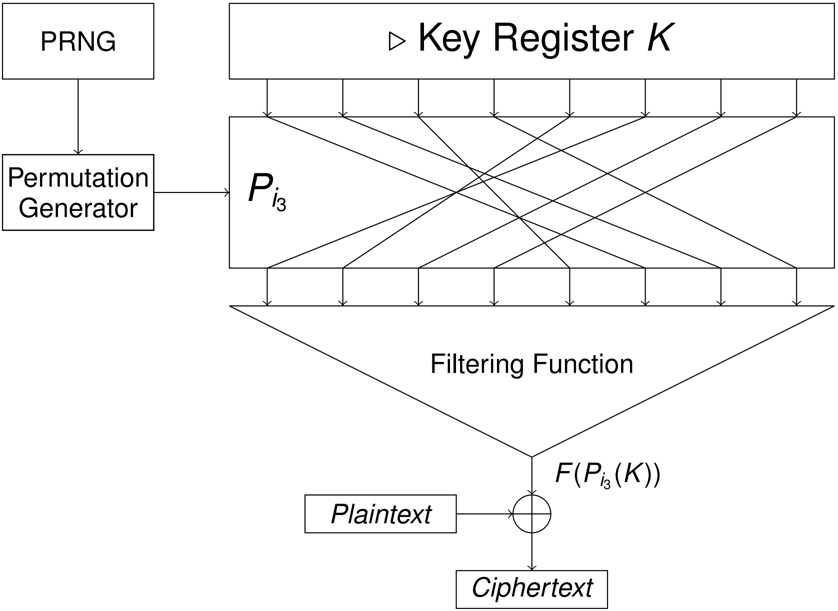
Filter Permutator: Construction



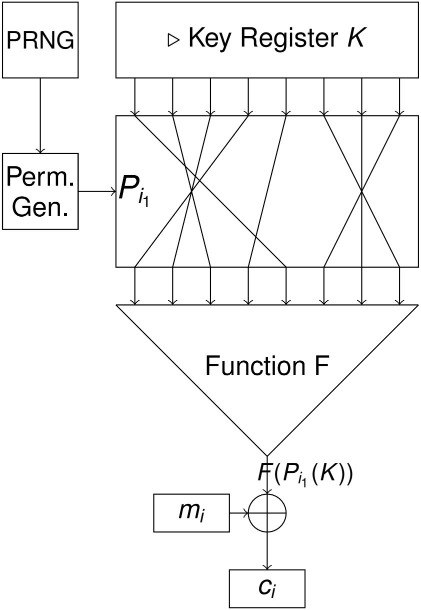
Filter Permutator: Construction



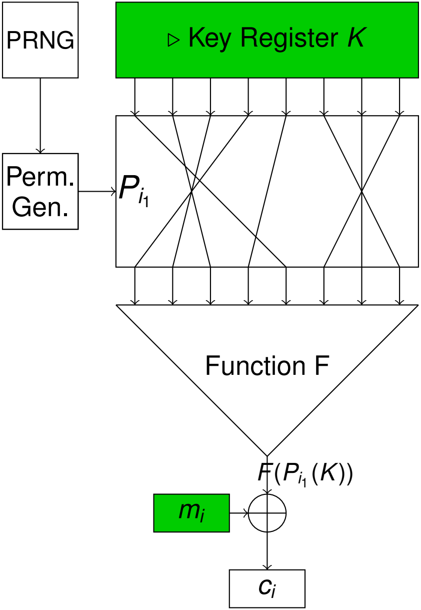
Filter Permutator: Construction



Filter Permutator: Homomorphic Evaluation

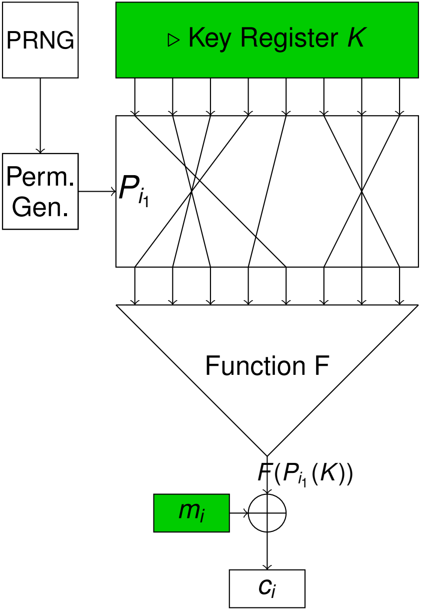


Filter Permutator: Homomorphic Evaluation



K_i, m_i: fresh

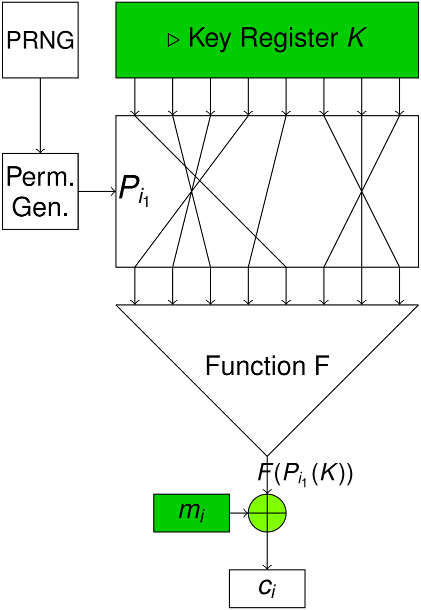
Filter Permutator: Homomorphic Evaluation



K_i, m_i: fresh

Permutation: no noise

Filter Permutator: Homomorphic Evaluation

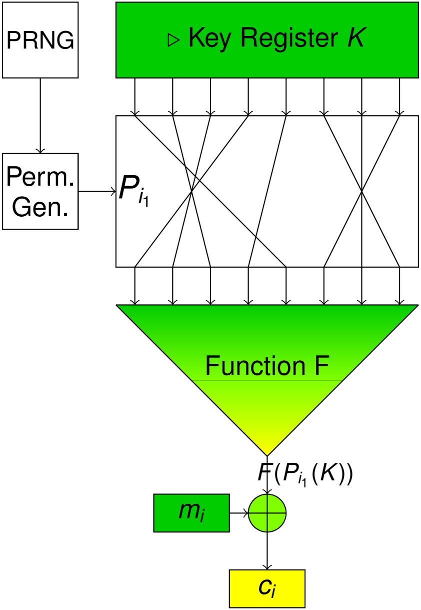


K_i, m_i: fresh

Permutation: no noise

XOR: small noise

Filter Permutator: Homomorphic Evaluation



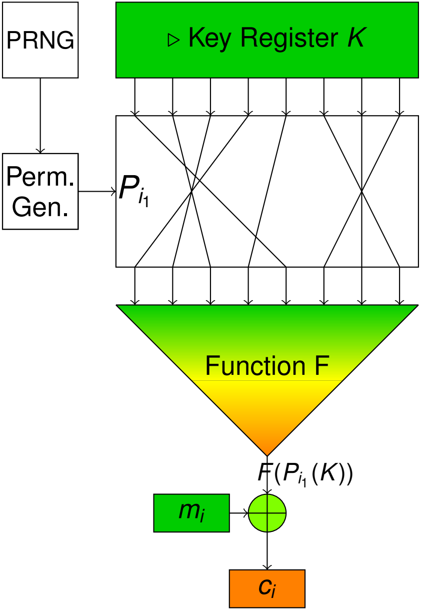
K_i, m_i: fresh

Permutation: no noise

XOR: small noise

F: determines ct noise

Filter Permutator: Homomorphic Evaluation



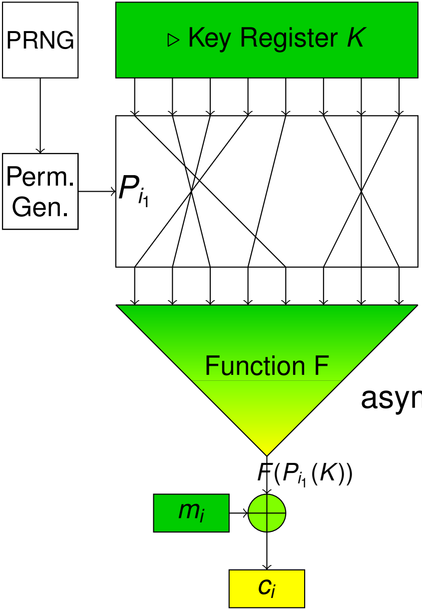
K_i, m_i: fresh

Permutation: no noise

XOR: small noise

F: determines ct noise

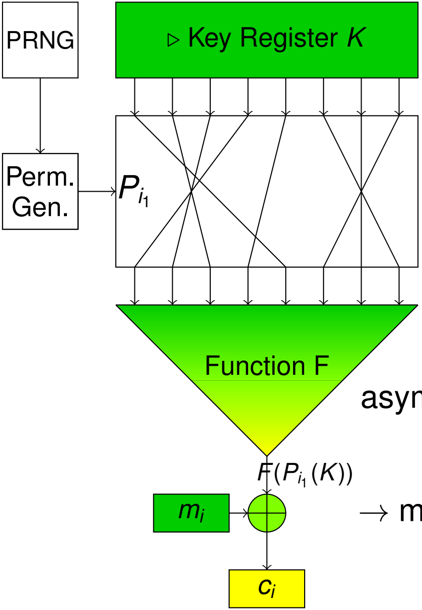
Filter Permutator: Homomorphic Evaluation



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

Filter Permutator: Security

Cryptanalysis Angle:

"good" PRNG + "good" Shuffle $\approx$ random Permutations,
$\rightarrow$ all security rely on F:

Filter Permutator: Security

Cryptanalysis Angle:

"good" PRNG + "good" Shuffle $\approx$ random Permutations,
$\rightarrow$ all security rely on F:

Attacks on Filtering Function

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

Filter Permutator: Security

Cryptanalysis Angle:

"good" PRNG + "good" Shuffle $\approx$ random Permutations,
$\rightarrow$ all security rely on F:

Attacks on Filtering Function

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

Standard Criteria

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

Filter Permutator: Security

Cryptanalysis Angle:

"good" PRNG + "good" Shuffle $\approx$ random Permutations,
$\rightarrow$ all security rely on 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 on F:

- controled number of additions
- multiplicative chains of simple functions
- few monomials
- small degree

Summary

(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:

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

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

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

Majority function

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

Remark:

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

Good Algebraic Immunity

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

Majority function

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

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

Direct Sum

f_1 in ℓ variables $x_1, \cdots, x_\ell$ and f_2, $N - \ell$ variables $x_{\ell+1}, \cdots, x_N$; direct sum F:

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

Proposition:

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

Low Cost and Good Algebraic Immunity

Direct Sum

f_1 in ℓ variables $x_1, \cdots, x_\ell$ and f_2, $N - \ell$ variables $x_{\ell+1}, \cdots, x_N$; direct sum F:

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

Proposition:

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

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.
Example: $T_4 = x_1 + x_2x_3 + x_4x_5x_6 + x_7x_8x_9x_{10}$.

Proposition: $\mathrm{AI}(T_k) = k$
Remark: Minimal number of monomials reachable.

Low Cost and Good Algebraic Immunity

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.

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

Direct sum vector

Let F be a Boolean function obtained by direct sum of monomials (*i.e.* each variable appears once and only once in the ANF), we define the direct sum vector of F as:

$$\mathbf{m}_F = [m_1, m_2, \cdots, m_k],$$

where m_i is the number of monomials of degree i.

Low Cost and Good Algebraic Immunity

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.

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

Direct sum vector

Let F be a Boolean function obtained by direct sum of monomials (*i.e.* each variable appears once and only once in the ANF), we define the direct sum vector of F as:

$$\mathbf{m}_F = [m_1, m_2, \cdots, m_k],$$

where m_i is the number of monomials of degree i.

Theorem:

$$\mathrm{AI}(F) = \min_{1 \leq d \leq k} \left(d + \sum_{i > d} m_i \right).$$

Correlation-like Attacks

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-like Attacks

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-like Attacks

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

$$\mathrm{NL}(F) = \min_{g \text{ affine}} \{d_H(f, g)\},$$

where $d_H(f, g) = \#\{x \in \mathbb{F}_2^N \mid F(x) \neq g(x)\}$ is the Hamming distance.

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

Correlation-like Attacks

Nonlinearity

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

$$\mathrm{NL}(F) = \min_{g \text{ affine}} \{d_H(f, g)\},$$

where $d_H(f, g) = \#\{x \in \mathbb{F}_2^N \mid F(x) \neq g(x)\}$ is 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

Property:
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

Property:
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

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

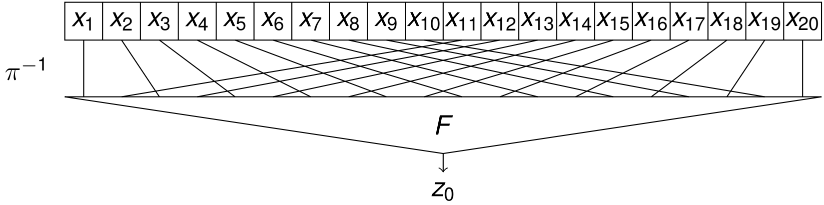
- $\mathrm{res}(f) = \mathrm{res}(f_1) + \mathrm{res}(f_2) + 1$,
- $\mathrm{NL}(F) = 2^{n_2}\mathrm{NL}(f_1) + 2^{n_1}\mathrm{NL}(f_2) - 2\mathrm{NL}(f_1)\mathrm{NL}(f_2)$.

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:
  $F = L_{n_1} + Q_{\frac{n_2}{2}} + \sum T_k$

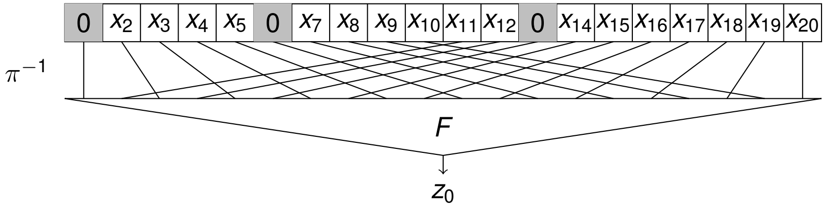
Summary

Guess and Determine Attacks



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

Guess and Determine Attacks

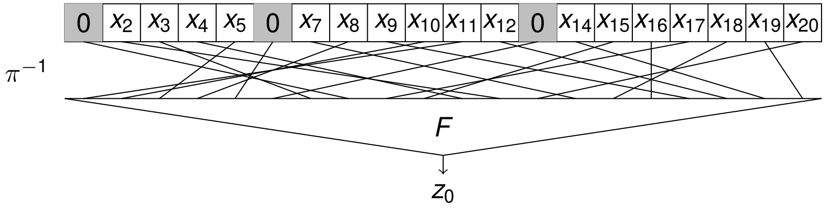


$$\begin{aligned} z_0 \quad = \quad & \cancel{x_{\pi(1)}} + x_{\pi(2)} + x_{\pi(3)} + x_{\pi(4)} \\ + \quad & \cancel{x_{\pi(5)}x_{\pi(6)}} + x_{\pi(7)}x_{\pi(8)} + x_{\pi(9)}x_{\pi(10)} \\ + \quad & \cancel{x_{\pi(11)}} + x_{\pi(12)}x_{\pi(13)} + x_{\pi(14)}x_{\pi(15)}x_{\pi(16)} + x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)}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

Guess & Determine attack [Duval,Lallemand,Rotella16]

- Guess ℓ positions being 0,

Guess and Determine Attacks

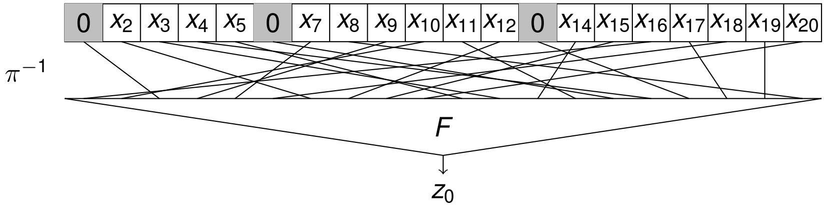


$$
\begin{aligned}
z_0 \;=\; & x_{\pi(1)} + x_{\pi(2)} + x_{\pi(3)} + x_{\pi(4)} \\
+\; & \cancel{x_{\pi(5)}x_{\pi(6)}} + \cancel{x_{\pi(7)}x_{\pi(8)}} + x_{\pi(9)}x_{\pi(10)} \\
+\; & x_{\pi(11)} + x_{\pi(12)}x_{\pi(13)} + x_{\pi(14)}x_{\pi(15)}x_{\pi(16)} + x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)}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

Guess & Determine attack [Duval,Lallemand,Rotella16]

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

Guess and Determine Attacks

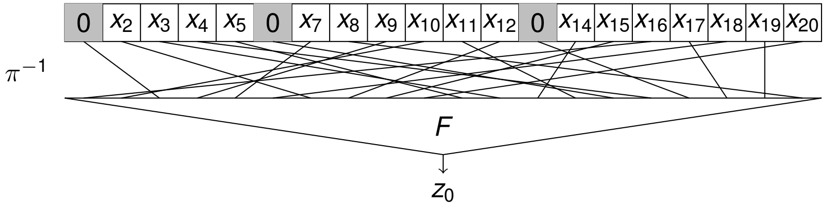


$$
\begin{aligned}
z_0 \quad = \quad & x_{\pi(1)} + x_{\pi(2)} + \cancel{x_{\pi(3)}} + x_{\pi(4)} \\
+ \quad & x_{\pi(5)}x_{\pi(6)} + x_{\pi(7)}x_{\pi(8)} + x_{\pi(9)}x_{\pi(10)} \\
+ \quad & x_{\pi(11)} + x_{\pi(12)}x_{\pi(13)} + \cancel{x_{\pi(14)}x_{\pi(15)}x_{\pi(16)}} + \cancel{x_{\pi(17)}x_{\pi(18)}x_{\pi(19)}x_{\pi(20)}}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

Guess & Determine attack [Duval,Lallemand,Rotella16]

- 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 [Duval,Lallemand,Rotella16]

- 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

For each Boolean criterion, we define its recurrent criterion denoted by $[\ell]$ as the minimal value of this criterion taken over all functions obtained by fixing ℓ of the N variables of F.

- Recurrent AI: $\mathrm{AI}[\ell](F)$,
- $\mathrm{FAI}[\ell](F)$,
- $\mathrm{res}[\ell](F)$,
- $\mathrm{NL}[\ell](F)$.

Recurrent Algebraic immunity

Recurrent AI; AI[ℓ](F)

We define AI[ℓ](F) as the minimal algebraic immunity over all functions obtained by fixing ℓ of the N 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)

We define AI[ℓ](F) as the minimal algebraic immunity over all functions obtained by fixing ℓ of the N variables of F.

Proposition: For all Boolean function F and ℓ such that $0 \leq \ell < N$:

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

Remark: Both bounds are tight.

Recurrent Algebraic immunity

Recurrent AI; AI[ℓ](F)

We define AI[ℓ](F) as the minimal algebraic immunity over all functions obtained by fixing ℓ of the N variables of F.

Proposition: For all Boolean function F and ℓ such that $0 \leq \ell < N$:

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

Remark: Both bounds are tight.

Proposition:
For all strictly positive N and ℓ such that $0 \leq \ell < N$:

$$\mathrm{AI}[\ell](Maj_N) = \max\left(0, \left\lceil \frac{N}{2} \right\rceil - \ell\right).$$

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

Let F be a direct sum of monomials with associated vector $[m_1, \cdots, m_k]$, we define two recurent criteria:

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

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

Let F be a direct sum of monomials with associated vector $[m_1, \cdots, m_k]$, we define two recurent criteria:

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

Remark: If F is a direct sum of monomials, so is $F[\ell]$.

Proposition: For all direct sum of monomials F:

- $\mathbf{m}_{F[\ell]}^* \geq \mathbf{m}_F^* - \left\lfloor \frac{\ell}{\min_{1 \leq i \leq k} m_i} \right\rfloor$,
- $\delta_{\mathbf{m}_{F[\ell]}} \leq \delta_{\mathbf{m}_F} 2^{\ell}$.

Recurrent Criteria and Direct Sums of Monomials

Criteria for Direct Sums of Monomials

Let F be a direct sum of monomials with associated vector $[m_1, \cdots, m_k]$, we define two recurent criteria:

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

Remark: If F is a direct sum of monomials, so is $F[\ell]$.

Proposition: For all direct sum of monomials F:

- $\mathbf{m}_{F[\ell]}^* \geq \mathbf{m}_F^* - \left\lfloor \frac{\ell}{\min_{1 \leq i \leq k} m_i} \right\rfloor$,
- $\delta_{\mathbf{m}_{F[\ell]}} \leq \delta_{\mathbf{m}_F} 2^\ell$.

Exact expression of $\mathbf{m}_{F[\ell]}^*$ and $\delta_{\mathbf{m}_{F[\ell]}}$ using $\mathbf{m}_F$ (see [MJSC16]):

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

Summary

Joint work with:

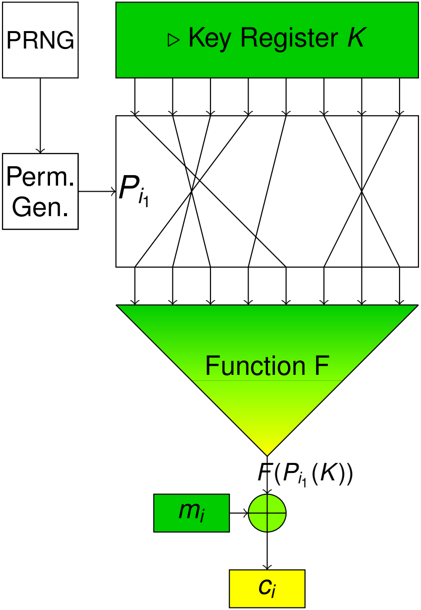
Claude Carlet and Yann Rotella,

title:

Boolean functions with restricted input and their robustness; application to the FLIP cipher.

ePrint: 97 (2017).

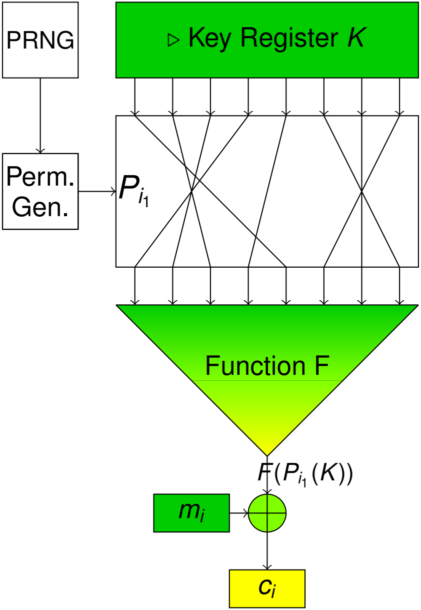
Filter Permutator: Hamming weight of F input



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

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

Filter Permutator: Hamming weight of F input

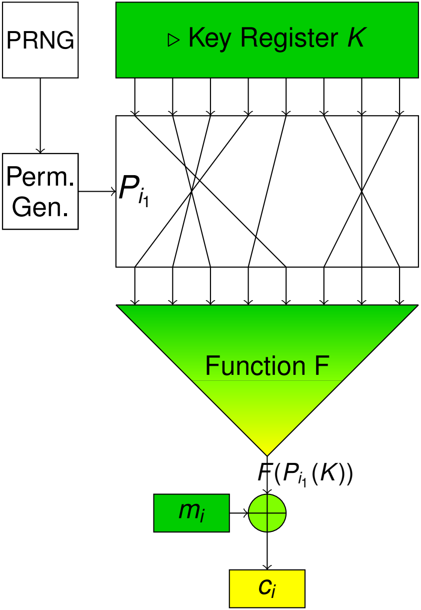


$$\psi_K : i \mapsto P_i(K)$$

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

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

Filter Permutator: Hamming weight of F input



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

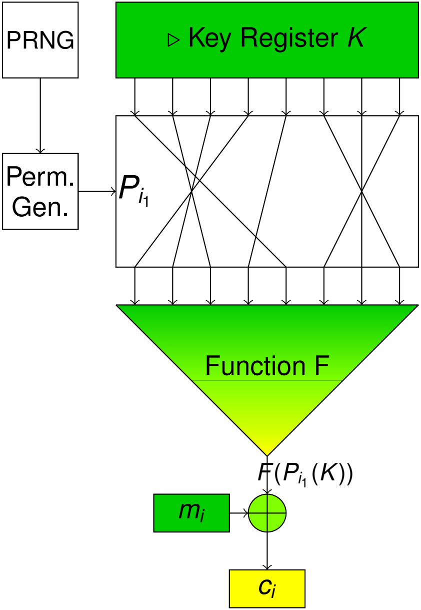
$$Im(\psi) \subsetneq \mathbb{F}_2^N$$

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

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

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

$\rightarrow$ algebraic immunity

$\rightarrow$ non-linearity

$\rightarrow$ balancedness

Restricted algebraic immunity

Algebraic immunity over E

Let f be defined over a set E:

$$\begin{aligned}\mathrm{AI}_E(f) &= \min\{\,\max(\deg(g), \deg(gf), g \neq 0 \text{ over } E)\,\} \\ &= \min\{deg(g), g \neq 0 \text{ over } E \mid gf = 0 \text{ or } g(f+1) = 0\}\end{aligned}$$

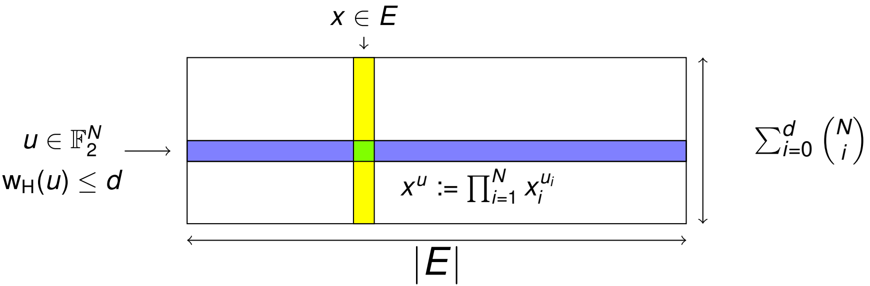
Restricted algebraic immunity

Algebraic immunity over E

Let f be defined over a set E:

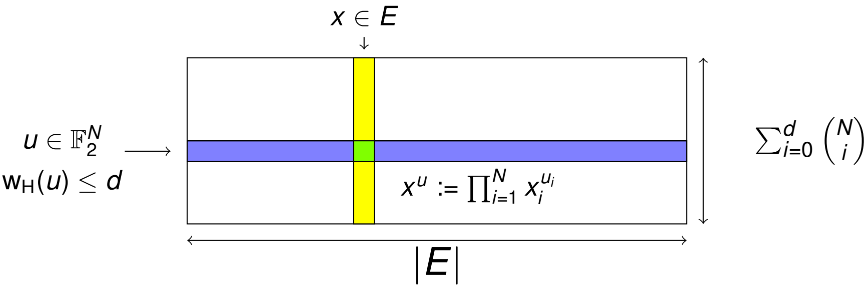
$$\begin{aligned} \mathrm{AI}_E(f) &= \min\{\max(\deg(g), \deg(gf), g \neq 0 \text{ over } E)\} \\ &= \min\{deg(g), g \neq 0 \text{ over } E \mid gf = 0 \text{ or } g(f+1) = 0\} \end{aligned}$$

Let $E \subseteq \mathbb{F}_2^N$, $d \in \mathbb{N}$, we define the matrix $\mathbf{M}_{d,E}$:



Restricted algebraic immunity

Let $E \subseteq \mathbb{F}_2^N$, $d \in \mathbb{N}$, we define the matrix $\mathbf{M}_{d,E}$:



Proposition: Let f be defined over E, $e \in \mathbb{N}$:
If $\mathrm{rank}(M_{d,E}) + \mathrm{rank}(M_{e,E}) > |E|$, then there exists $g \neq 0$ on E, and h such that:

$$\deg(g) \leq e, \deg(h) \leq d, \text{ and, } gf = h \text{ on } E.$$

Corollary:

$$\mathrm{AI}_E(f) \leq \min \left\{ d; \mathrm{rank}(M_{d,E}) > \frac{|E|}{2} \right\}.$$

Algebraic immunity over $E_{N,k}$

In particular, consider the set $E_{N,k} := \{x \mid \mathrm{w_H}(x) = k\}$,

Theorem:

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

Algebraic immunity over $E_{N,k}$

In particular, consider the set $E_{N,k} := \{x \mid \mathrm{w_H}(x) = k\}$,

Theorem:

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

Corollary: For all $0 \leq k \leq N/2$:

$$\mathrm{AI}_{E_{N,k}}(f) \leq \min\left\{d;\ 2\binom{N}{d} > \binom{N}{k}\right\}.$$

Remark: It proves that best $\mathrm{AI}_{E_{N,k}}$ is lower than in the general case.

Algebraic immunity over $E_{N,k}$

In particular, consider the set $E_{N,k} := \{x \mid \mathrm{w_H}(x) = k\}$,

Theorem:

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

Corollary: For all $0 \leq k \leq N/2$:

$$\mathrm{AI}_{E_{N,k}}(f) \leq \min\left\{d;\ 2\binom{N}{d} > \binom{N}{k}\right\}.$$

Remark: It proves that best $\mathrm{AI}_{E_{N,k}}$ is lower than in the general case.

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

$$\mathrm{AI}_{E_{N,k}}(F) \geq \mathrm{AI}(f) - \deg(g).$$

Restricted non-linearity

Non-linearity over E

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

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

Restricted non-linearity

Non-linearity over E

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

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

Looking for an upper bound, using the covering radius bound:

Proposition:

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

Looking for an upper bound, using the covering radius bound:

Proposition:

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

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

Proposition: Let $\mathcal{F}$ be a vector space, assuming that:

$$\exists v \in \mathbb{F}_2^N \text{ such that } v \cdot (x+y) = 1 \text{ for all } (x,y) \in E^2 \text{ such that } 0 \neq x+y \in \mathcal{F}^\perp,$$

we have:

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

where

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

Restricted non-linearity

Proposition: Let $\mathcal{F}$ be a vector space, assuming that:

$\exists v \in \mathbb{F}_2^N$ such that $v \cdot (x+y) = 1$ for all $(x,y) \in E^2$ such that $0 \neq x+y \in \mathcal{F}^\perp$,

we have:

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

where

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

Focusing on $N-1$ dimentional vector spaces,
Corollary:

$$\lambda = \max_{a\in\mathbb{F}_2^N; a\neq 0} \Big|\sum_{\substack{(x,y)\in E^2\\ x+y=a}} (-1)^{f(x)+f(y)}\Big| = \max_{a\in\mathbb{F}_2^N; a\neq 0} \Big|\sum_{x\in E\cap(a+E)} (-1)^{D_a f(x)}\Big|.$$

Non-linearity over $E_{N,k}$

In particular, considering the set $E_{N,k}$,

Proposition: For $(N, k) \neq (50, 3)$ nor $(50, 47)$ the bound:

$$\mathrm{NL}_{E_{N,k}}(f) \leq \frac{\binom{n}{k}}{2} - \frac{1}{2}\sqrt{\binom{n}{k}},$$

cannot be tight.

Non-linearity over $E_{N,k}$

In particular, considering the set $E_{N,k}$,

Proposition: For $(N, k) \neq (50, 3)$ nor $(50, 47)$ the bound:

$$\mathrm{NL}_{E_{N,k}}(f) \leq \frac{\binom{n}{k}}{2} - \frac{1}{2}\sqrt{\binom{n}{k}},$$

cannot be tight.

This bound has been improved in [Mesnager17] using power sum of Walsh transform.

Non-linearity over $E_{N,k}$

In particular, considering the set $E_{N,k}$,

Proposition: For $(N, k) \neq (50, 3)$ nor $(50, 47)$ the bound:

$$\mathrm{NL}_{E_{N,k}}(f) \leq \frac{\binom{n}{k}}{2} - \frac{1}{2}\sqrt{\binom{n}{k}},$$

cannot be tight.
This bound has been improved in [Mesnager17] using power sum of Walsh transform.

Remark: $\max(\mathrm{NL}_{E_{N,k}}) \geq d/2$,
where d is the minimal distance of a punctured 1st order Reed Müller code, which value has been proved in [Dumer,Kapralova13].

Non-linearity over $E_{N,k}$

In particular, considering the set $E_{N,k}$,

Proposition: For $(N,k) \neq (50,3)$ nor $(50,47)$ the bound:

$$\mathrm{NL}_{E_{N,k}}(f) \leq \frac{\binom{n}{k}}{2} - \frac{1}{2}\sqrt{\binom{n}{k}},$$

cannot be tight.
This bound has been improved in [Mesnager17] using power sum of Walsh transform.

Remark: $\max(\mathrm{NL}_{E_{N,k}}) \geq d/2$,
where d is the minimal distance of a punctured 1st order Reed Müller code, which value has been proved in [Dumer,Kapralova13].

Standard non-linearity can collapse:
Proposition:
For every even $N \geq 4$, the quadratic bent functions satisfying $\mathrm{NL}_{E_{N,k}}(f) = 0$ for every k are those functions of the form $f(x) = \sigma_1(x)\ell(x) + \sigma_2(x)$ where $\ell(1,\ldots,1) = 0$.

Balancedness on constant Hamming weight input

Balancedness over E

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

Balancedness on constant Hamming weight input

Balancedness over E

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

We could be interested by the behaviour on a family of sets:

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

Balancedness over E

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

We could be interested by the behaviour on a family of sets:

Weightwise Perfectly Balanced Function

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

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

Theorem:
Let g' be an arbitrary N-variable function, if f, f', and g, are 3 N-variable *WPB* functions then,

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

is a $2N$-variable *WPB* function.

Balancedness on constant Hamming weight input

Weightwise Almost Perfectly Balanced Function

f defined over $\mathbb{F}_2^N$, is *weightwise almost perfectly balanced* (*WAPB*):

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

Balancedness on constant Hamming weight input

Weightwise Almost Perfectly Balanced Function

f defined over $\mathbb{F}_2^N$, is *weightwise almost perfectly balanced* (*WAPB*):

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

Proposition: The function f_N in $N \geq 2$ variables defined as:

$$f_N = \begin{cases} x_1 & \text{if } N = 2, \\ f_{N-1} & \text{if } N \text{ odd}, \\ f_{N-1} + x_{N-2} + \prod_{i=1}^{2^{d-1}} x_{N-i} & \text{if } N = 2^d; d > 1, \\ f_{N-1} + x_{N-2} + \prod_{i=1}^{2^d} x_{n-i} & \text{if } N = p \cdot 2^d, p > 1 \text{ odd}, d \geq 1. \end{cases}$$

has the following properties for all $N \geq 2$:

- f_N is *WAPB*,
- $\deg(f_N) = 2^{d-1}$; where $2^d \leq N < 2^{d+1}$,
- f_N's ANF contains $N - 1 - (N \mod 2)$ monomials.

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 $\mathrm{NL}_{E_{N,k}}$; $\mathrm{AI}_{E_{N,k}}$?
- ◇ 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 $\mathrm{NL}_{E_{N,k}}$; $\mathrm{AI}_{E_{N,k}}$?
- ◇ Fixed Hamming weight input and cryptanalysis?
- ◇ $\cdots$?

Thanks for your attention!