Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts

Pierrick MÉAUX

École normale supérieure, CNRS, INRIA, PSL

Joint work with:
Anthony JOURNAULT, François-Xavier STANDAERT,
and Claude CARLET
Eurocrypt 2016 — Vienna, Austria
Monday May 9

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 ✓

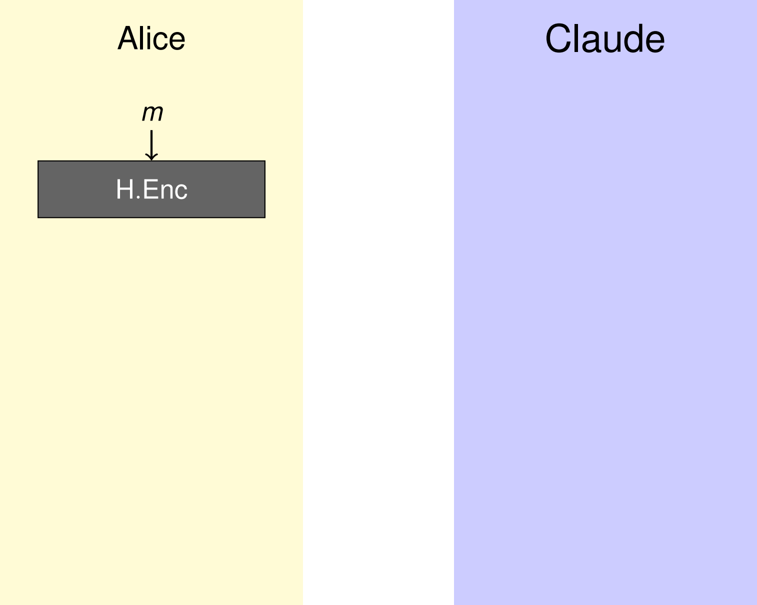
Fully Homomorphic Encryption

Claude

Huge storage

Huge power

FHE Framework



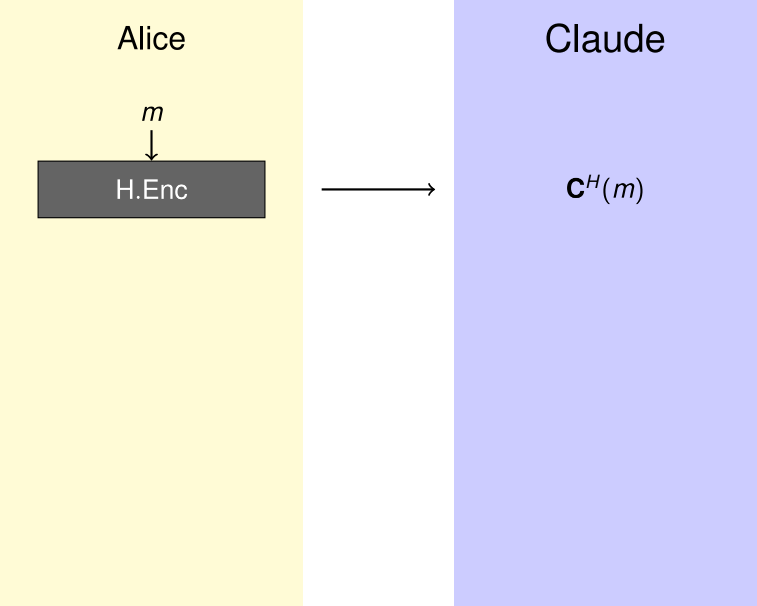
Alice

m

H.Enc

Claude

FHE Framework



Alice

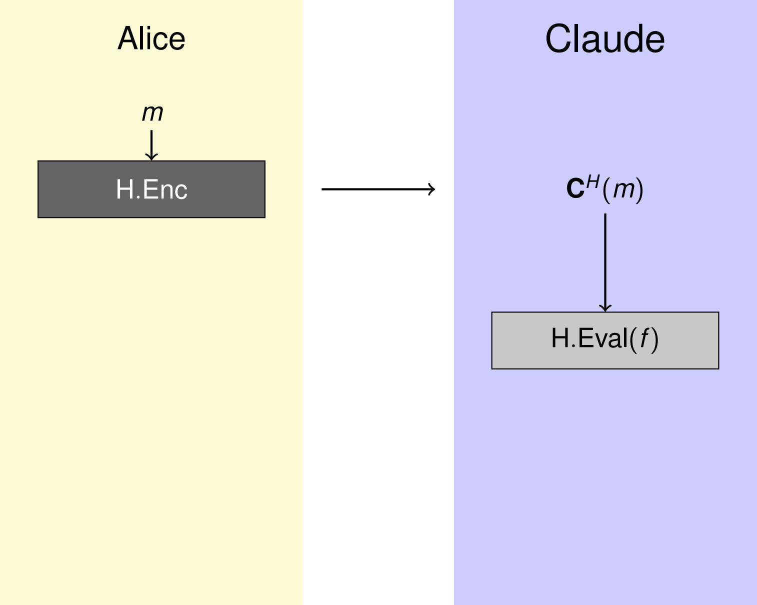
m

H.Enc

Claude

$\mathbf{c}^{H}(m)$

FHE Framework



Alice

m

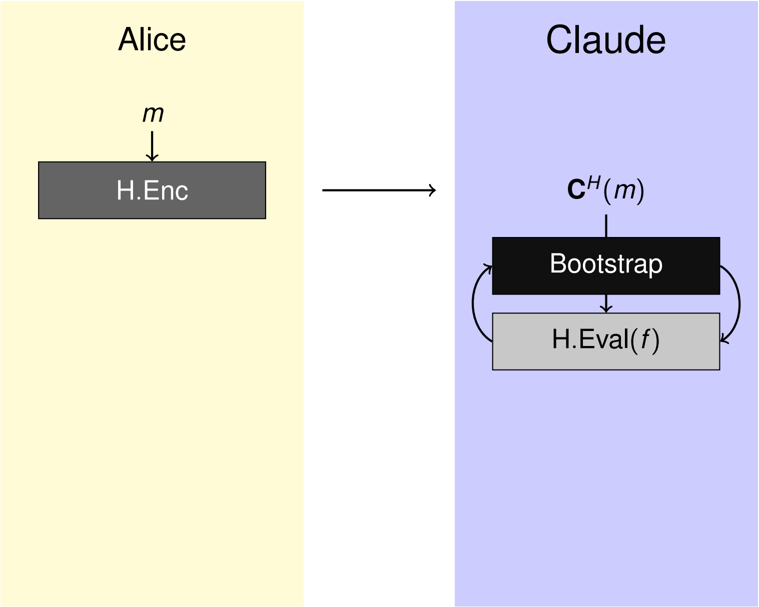
H.Enc

Claude

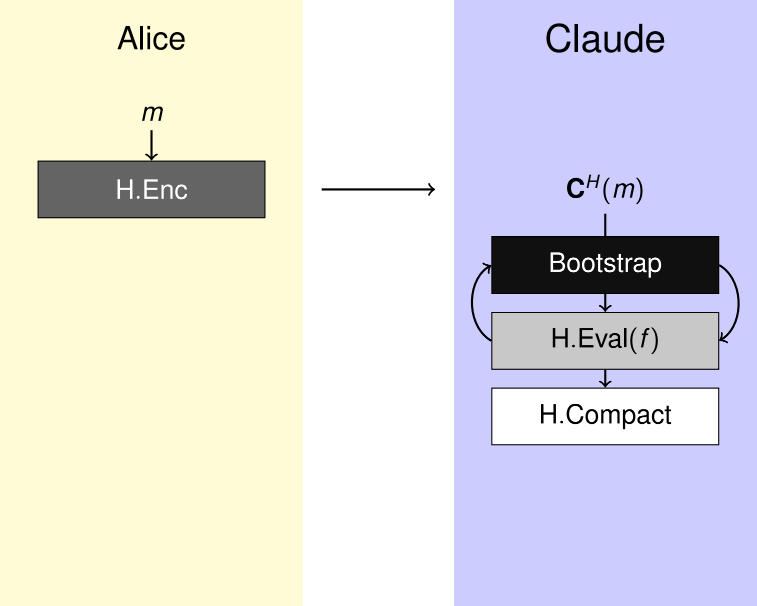
$\mathbf{C}^H(m)$

H.Eval(f)

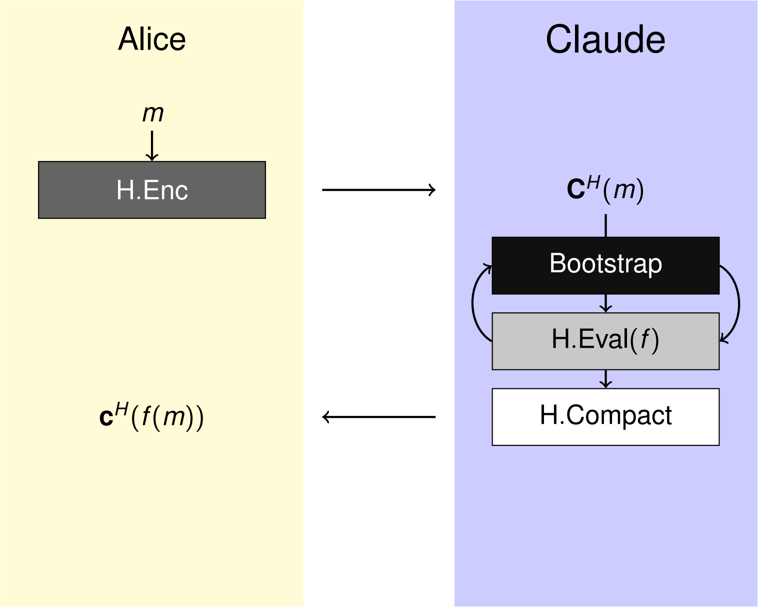
FHE Framework



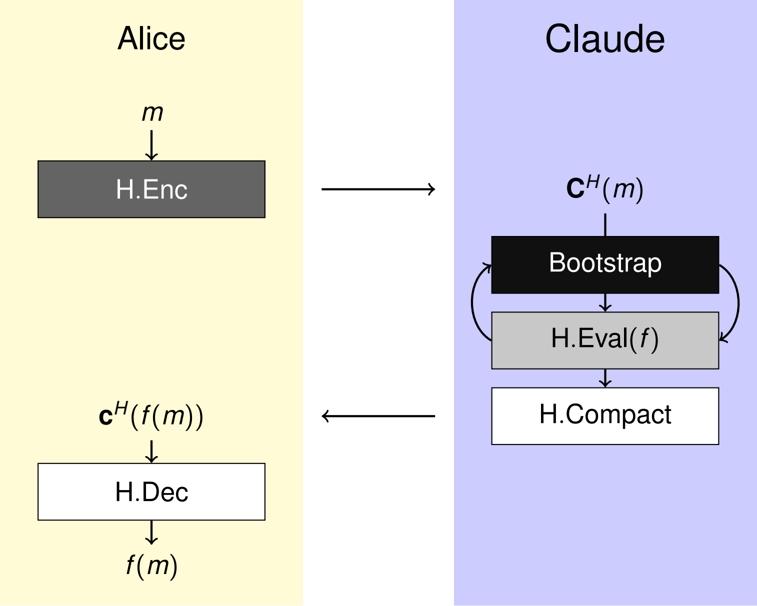
FHE Framework



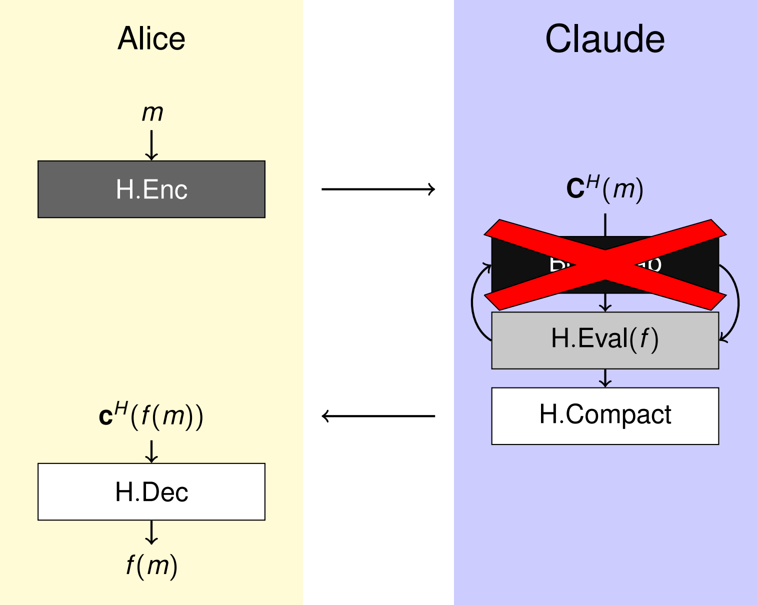
FHE Framework



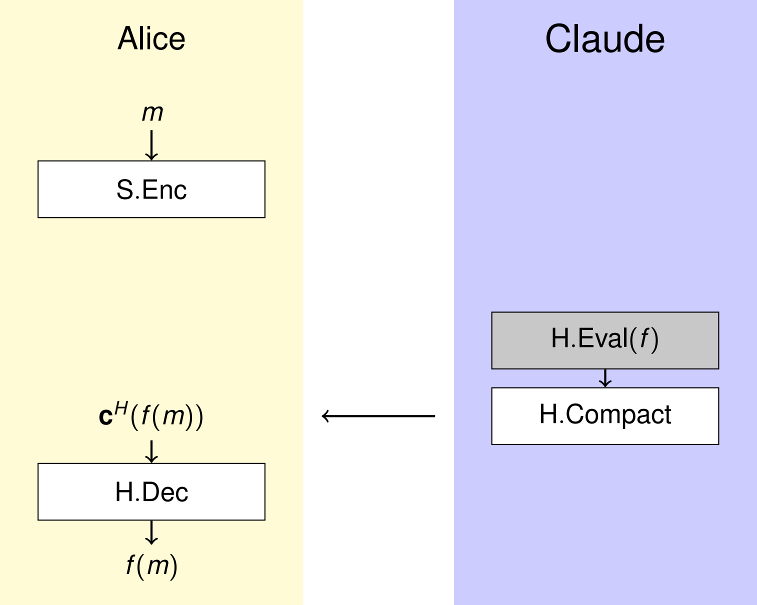
FHE Framework



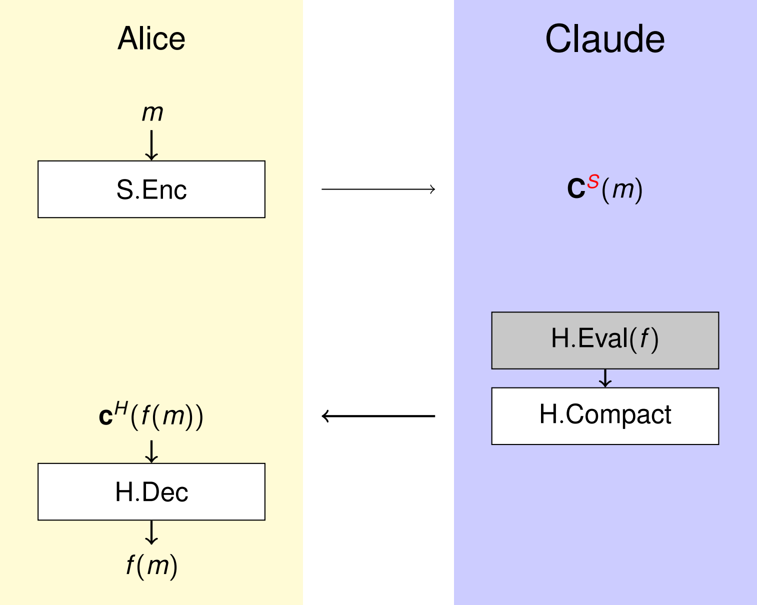
HE Framework



SE-HE Hybrid Framework



SE-HE Hybrid Framework



Alice

m

S.Enc

Claude

$\mathbf{c}^{S}(m)$

H.Eval(f)

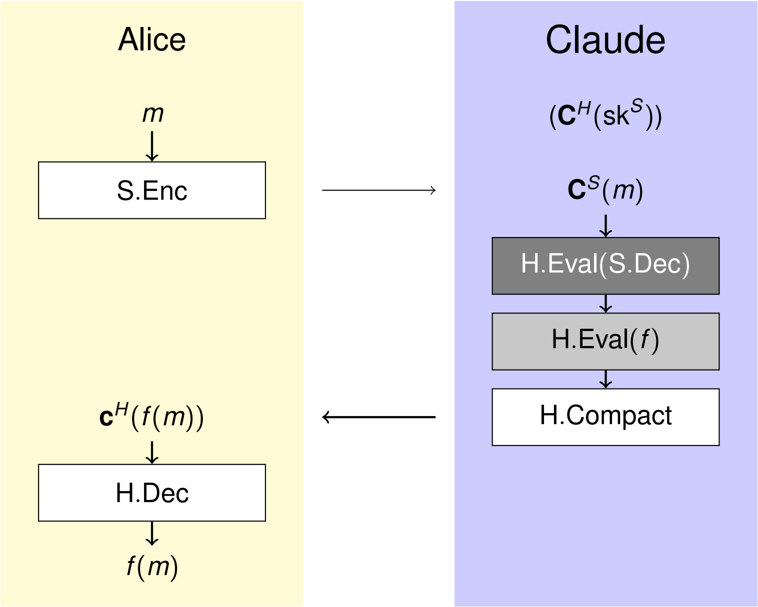
H.Compact

$\mathbf{c}^{H}(f(m))$

H.Dec

$f(m)$

SE-HE Hybrid Framework



Performance Metric (Intuition)

- ◇ Computational Cost

- ◇ Noise Increase

Performance Metric (Intuition)

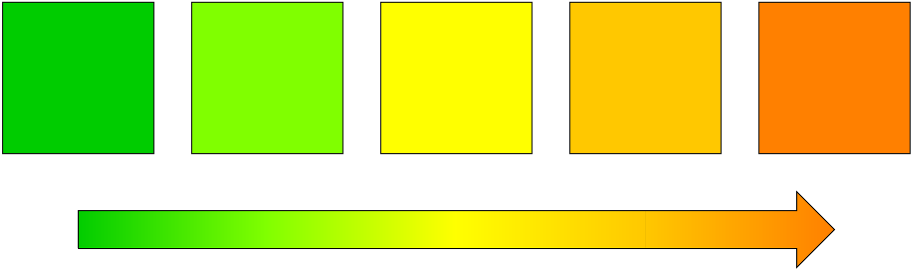
- Computational Cost $\approx$ number of multiplications

- Noise Increase

Performance Metric (Intuition)

- Computational Cost $\approx$ number of multiplications

- Noise Increase

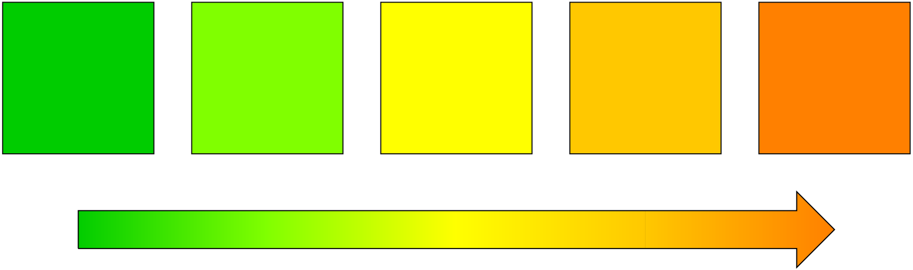


ciphertext noise

Performance Metric (Intuition)

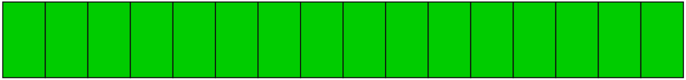
- Computational Cost $\approx$ number of multiplications

- Noise Increase $\approx$ multiplicative depth



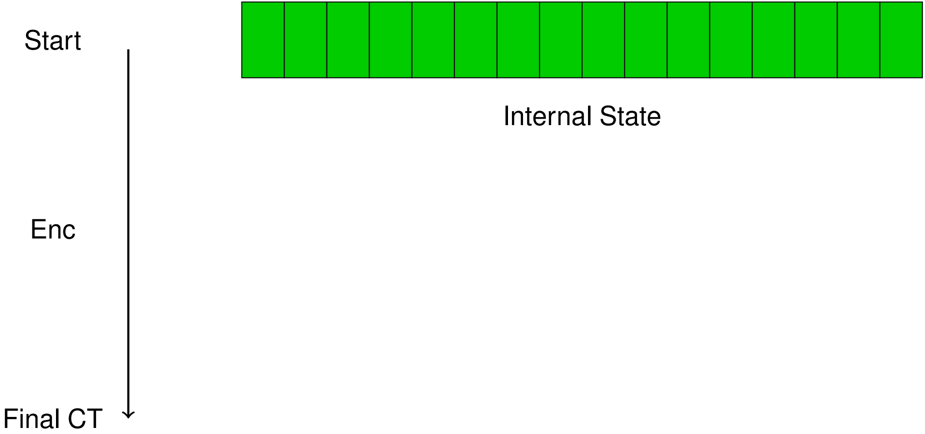
ciphertext noise

State of the Art

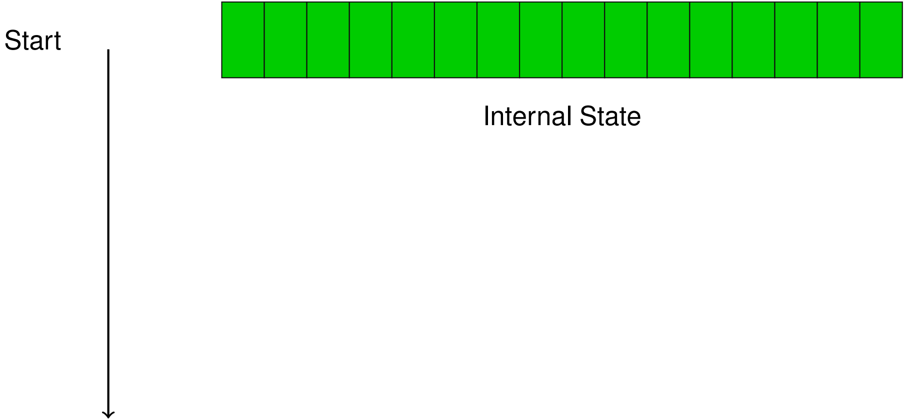


Internal State

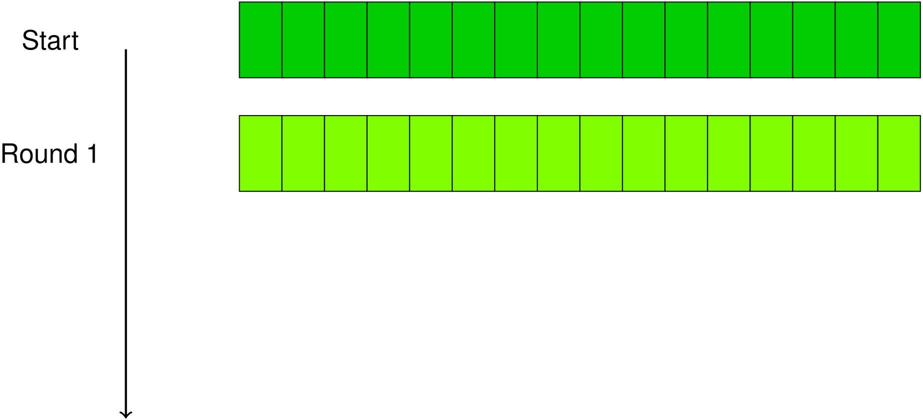
State of the Art



State of the Art: Block Ciphers



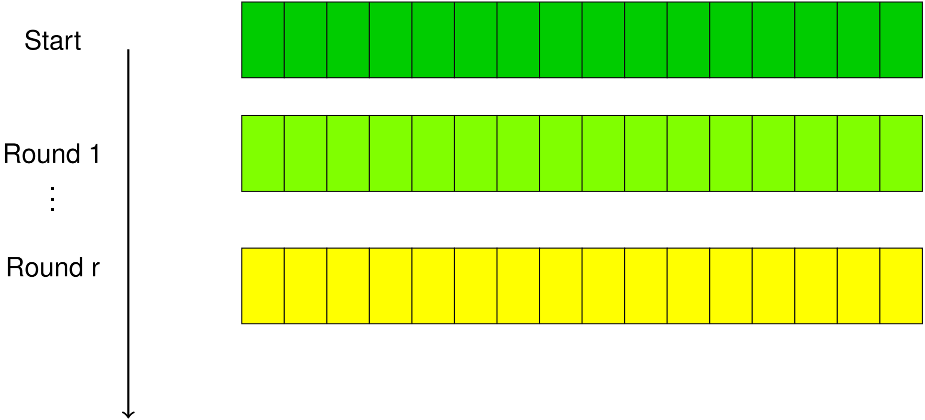
State of the Art: Block Ciphers



Start

Round 1

State of the Art: Block Ciphers



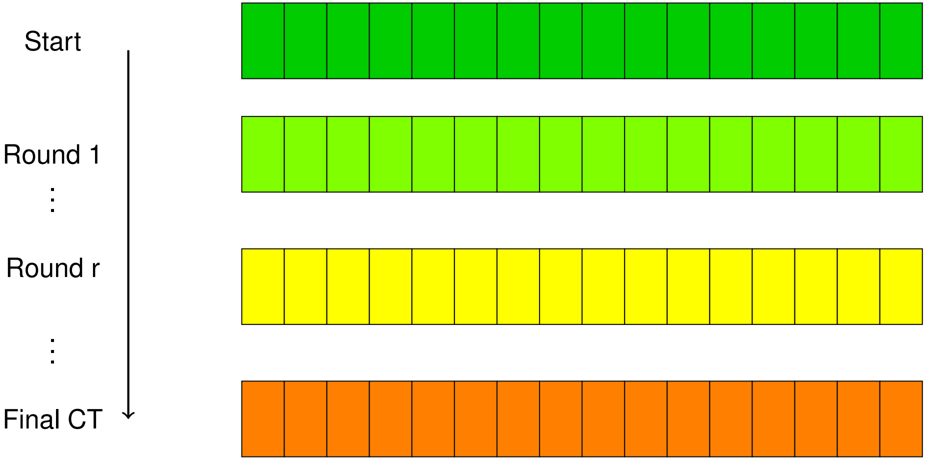
Start

Round 1

⋮

Round r

State of the Art: Block Ciphers



Start

Round 1

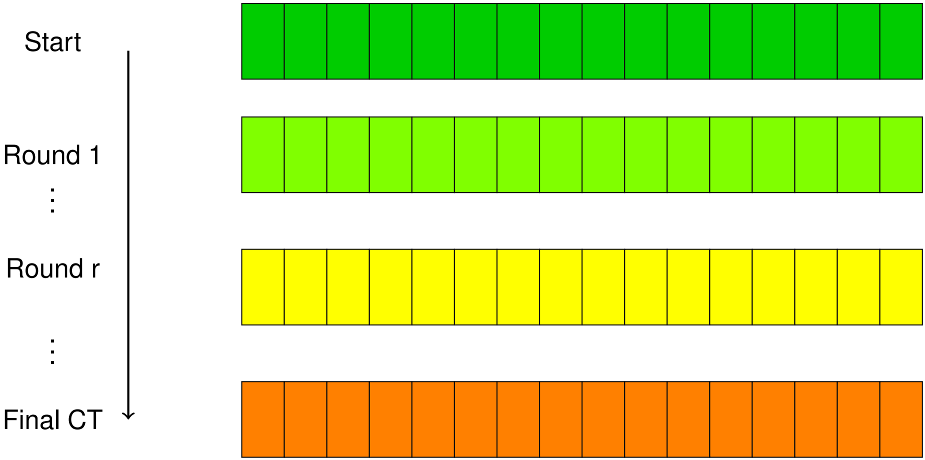
⋮

Round r

⋮

Final CT

State of the Art: Block Ciphers



Start

Round 1

⋮

Round r

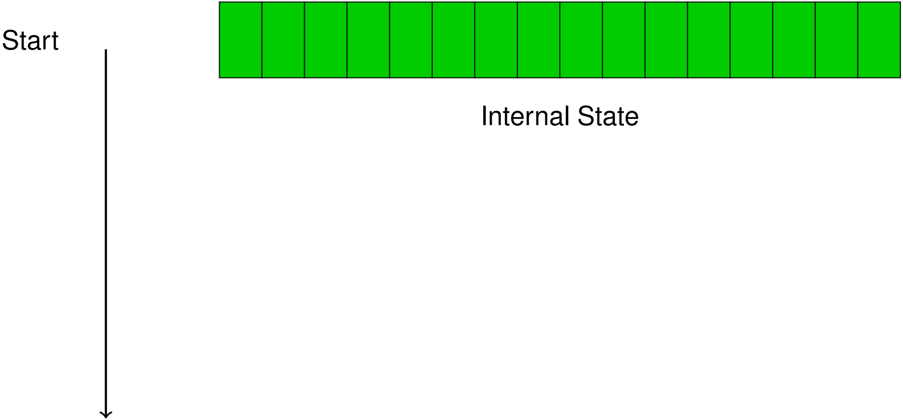
⋮

Final CT

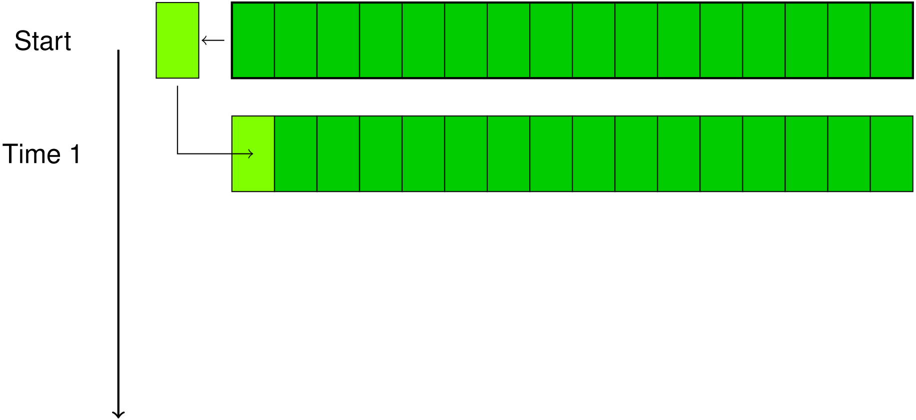
→ Constant but High Noise

AES[GHS12,CLT14], $\cdots$, LowMC[ARS+15]

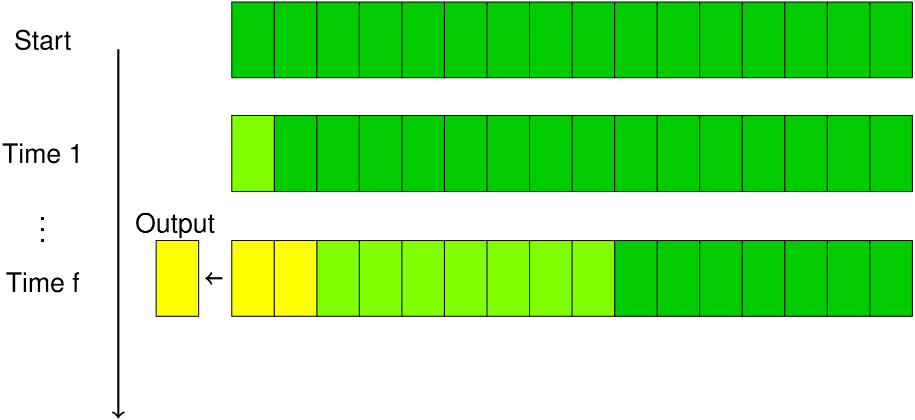
State of the Art: Stream Ciphers



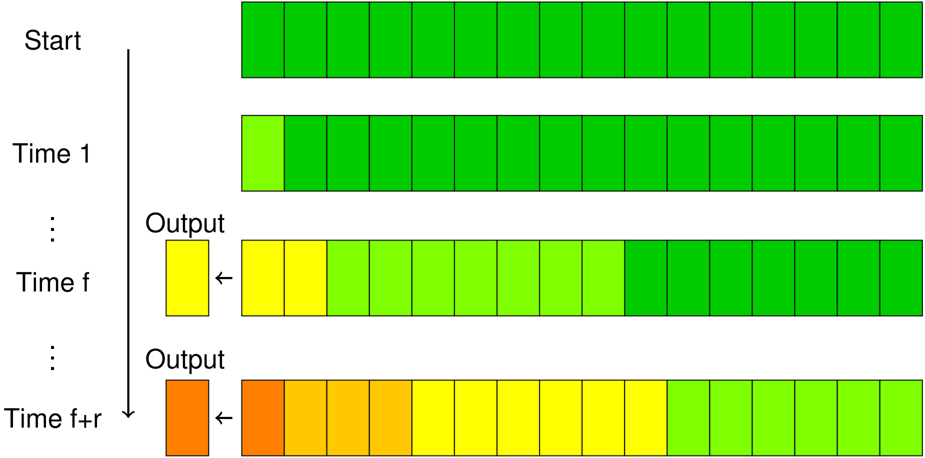
State of the Art: Stream Ciphers



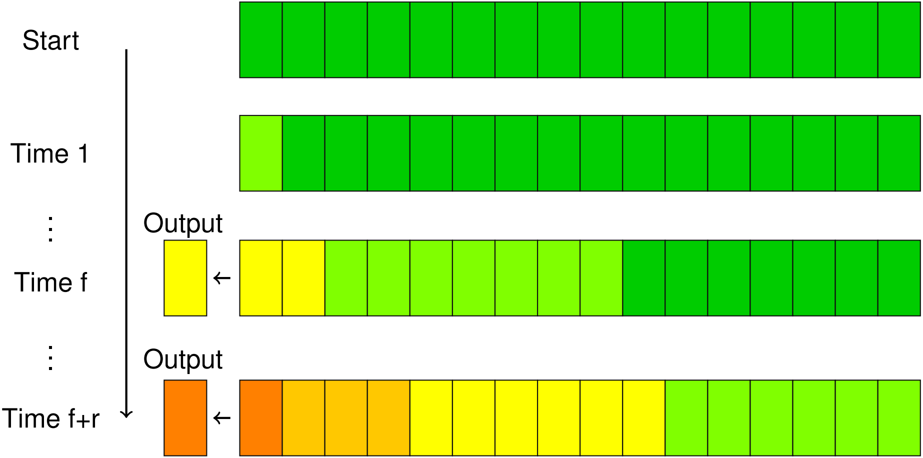
State of the Art: Stream Ciphers



State of the Art: Stream Ciphers



State of the Art: Stream Ciphers



Start

Time 1

⋮

Output

Time f

⋮

Output

Time f+r

→ Slowly Increasing Noise, Limited Output

Trivium, Kreyvium[CCF+15]

Our contributions

◇ Best of both worlds: Constant and Low noise increase

◇ Take advantage of 3^{rd} generation FHE

Our contributions

◇ Best of both worlds: Constant and Low noise increase

→ Filter Permutator

◇ Take advantage of 3^{rd} generation FHE

Our contributions

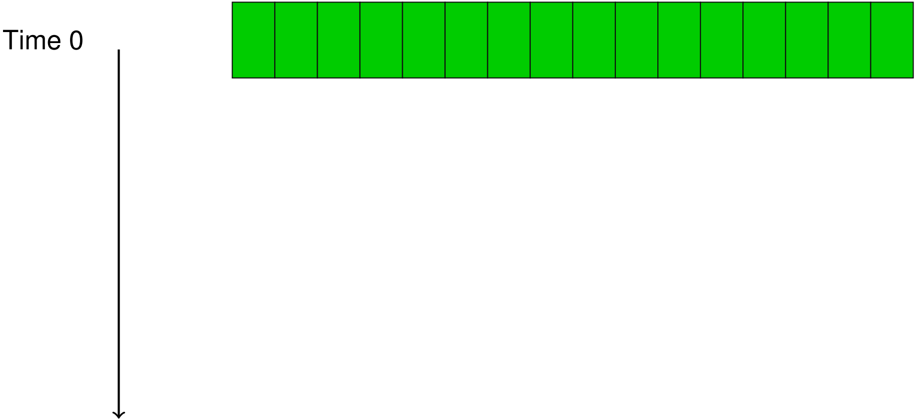
◇ Best of both worlds: Constant and Low noise increase

→ Filter Permutator

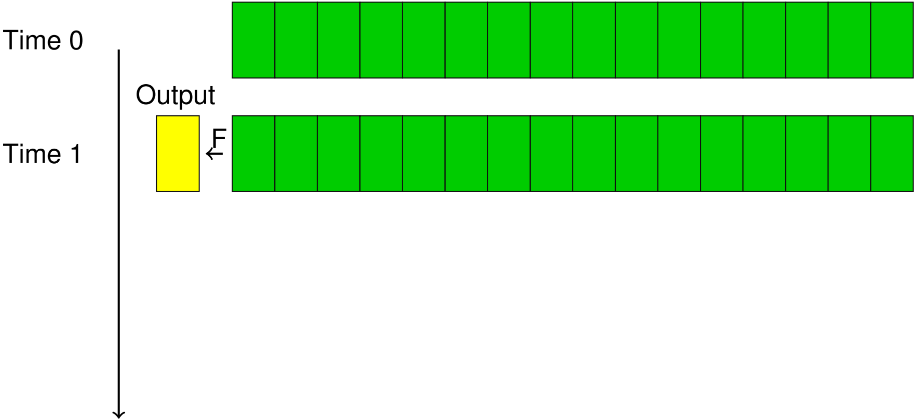
◇ Take advantage of 3rd generation FHE

→ FLIP$_F$

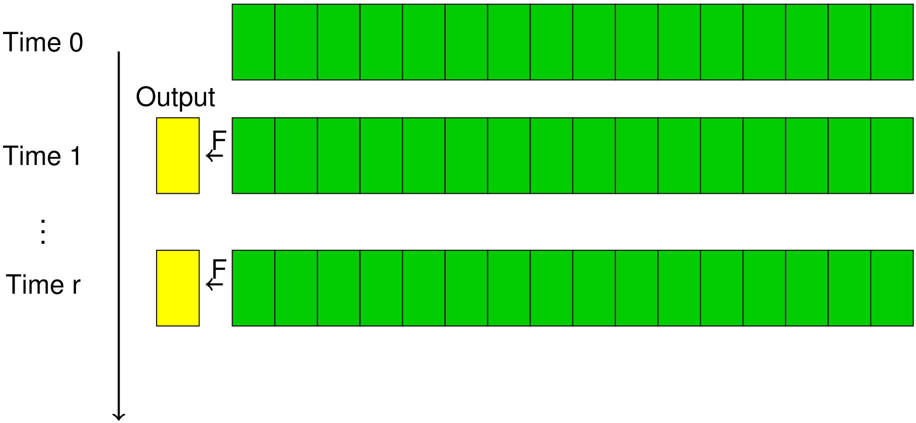
Filter Permutator Error Increase



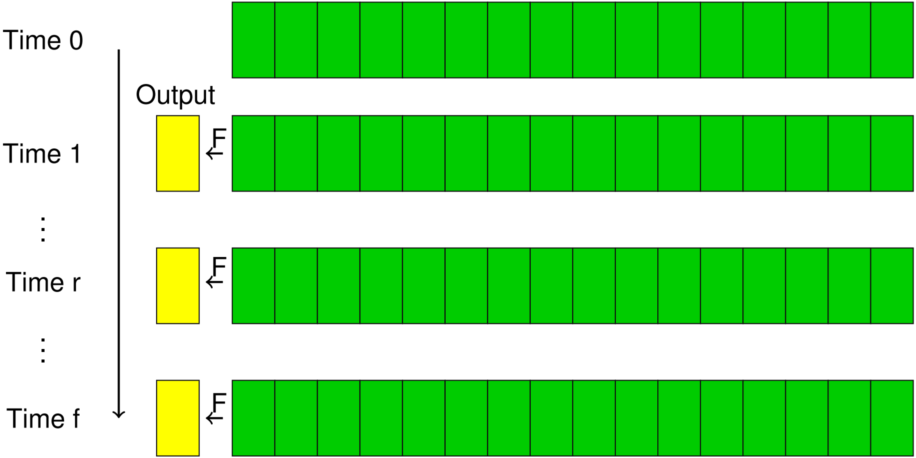
Filter Permutator Error Increase



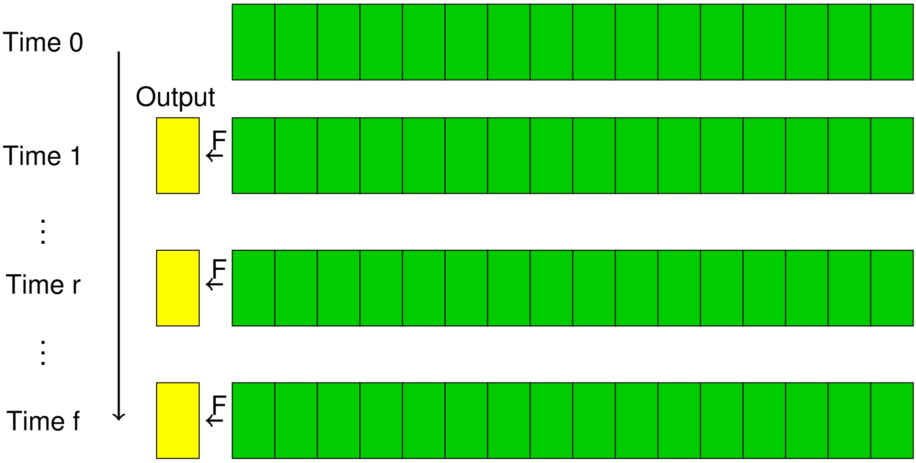
Filter Permutator Error Increase



Filter Permutator Error Increase

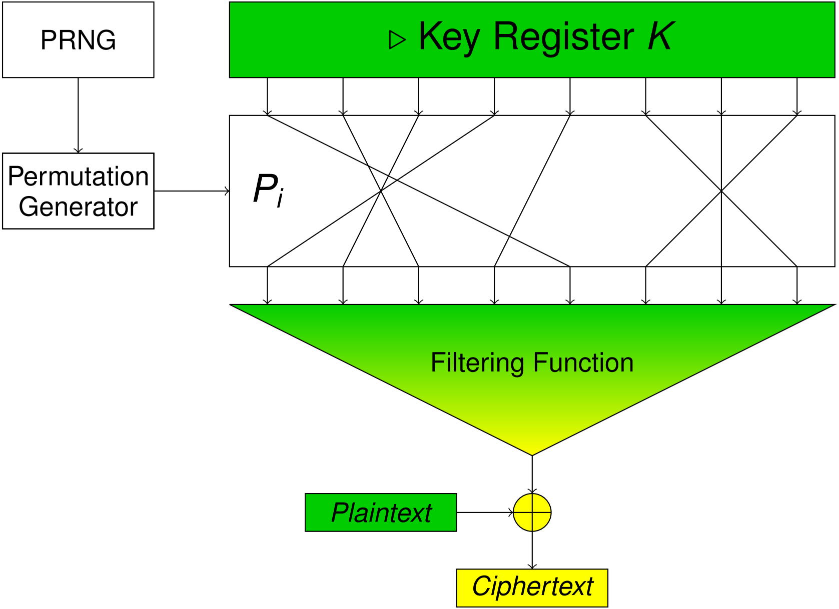


Filter Permutator Error Increase



→ Constant and Low Noise

Filter Permutator Construction



FLIP$_F$ Construction

Components

- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$

FLIP$_F$ Construction

Components

- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$

n_1 variables

$$\begin{array}{c} x_1 \\ \oplus \\ \vdots \\ \oplus \\ x_{n_1} \end{array}$$

FLIP$_F$ Construction

Components

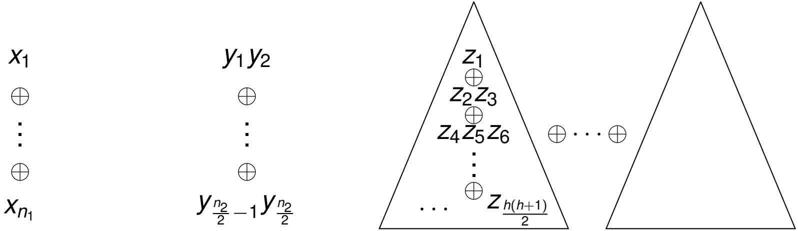
- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$

$$\begin{array}{cc}
 & n_2 \text{ variables} \\
x_1 & y_1 y_2 \\
\oplus & \oplus \\
\vdots & \vdots \\
\oplus & \oplus \\
x_{n_1} & y_{\frac{n_2}{2}-1} y_{\frac{n_2}{2}}
\end{array}$$

FLIP$_F$ Construction

Components

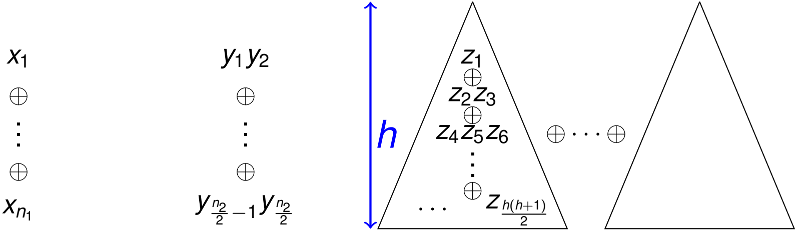
- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$



FLIP$_F$ Construction

Components

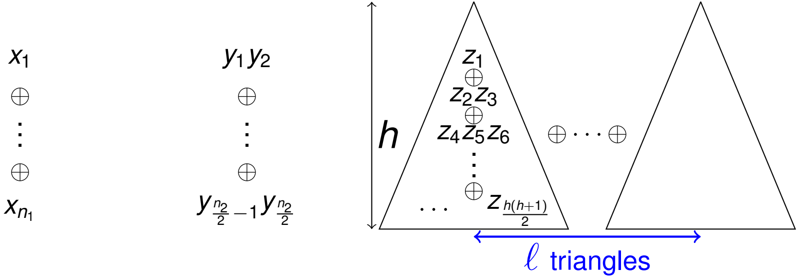
- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$



FLIP$_F$ Construction

Components

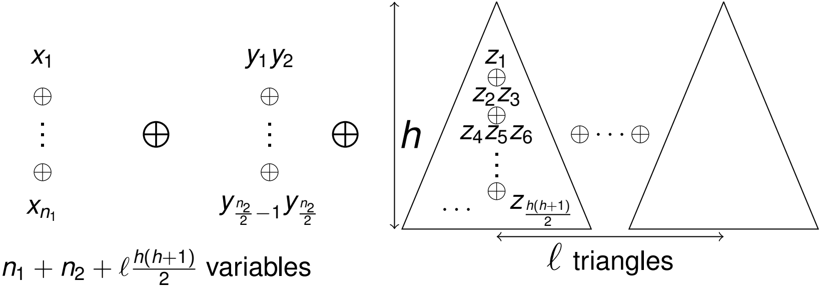
- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$



FLIP$_F$ Construction

Components

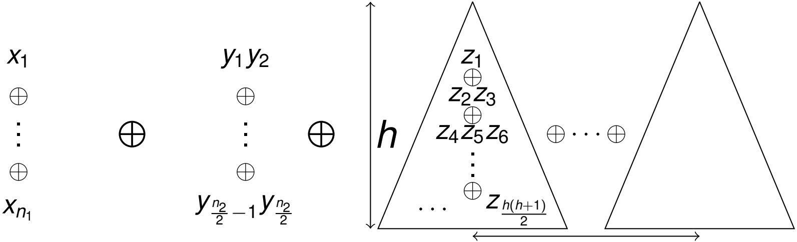
- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^h)$



FLIP$_F$ Construction

Components

- PRNG: forward secure PRNG based on AES-128
- Permutation Generator: Knuth Shuffle
- Filtering function $F = (n_1, n_2, {}^{\ell}\Delta^{h})$



$x_1 \oplus \vdots \oplus x_{n_1}$ $\oplus$ $y_1 y_2 \oplus \vdots \oplus y_{\frac{n_2}{2}-1} y_{\frac{n_2}{2}}$ $\oplus$ h $z_1 \oplus z_2 z_3 \oplus z_4 z_5 z_6 \vdots \oplus \ldots z_{\frac{h(h+1)}{2}}$ $\oplus \cdots \oplus$

$n_1 + n_2 + \ell\frac{h(h+1)}{2}$ variables

ℓ triangles

FLIP$(42, 64, {}^{8}\Delta^{9})$ FLIP$(82, 112, {}^{8}\Delta^{16})$

FLIP$_F$ Homomorphic Behavior

3^{rd} generation FHE Ciphertexts (GSW)

$$\mathbf{s}\mathbf{C} = \mu\mathbf{s} + \mathbf{e}$$

FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth

$$\underset{\substack{\text{secret key}\\ \approx\ \text{eigenvector}}}{\mathbf{s}}\overset{\text{ciphertext (small)}}{\mathbf{C}} = \underset{\substack{\text{plaintext}\\ \approx\ \text{eigenvalue}}}{\mu}\mathbf{s} + \overset{\text{error (small)}}{\mathbf{e}}$$

FLIP_F Homomorphic Behavior

3^{rd} generation FHE Noise Growth

$$\mathbf{s}\mathbf{C} = \mu\mathbf{s} + \mathbf{e}$$

H.Add : $\sum_{i=1}^{k} \mathbf{C}_i$

H.Mul : $\prod_{i=1}^{k} \mathbf{C}_i$

FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth

$$\mathbf{sC} = \mu\mathbf{s} + \mathbf{e}$$

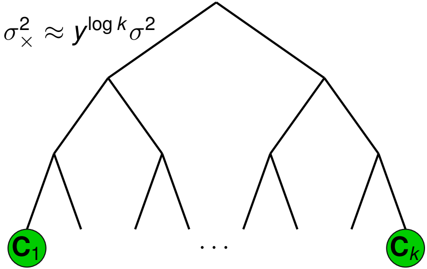
$$\text{H.Add} : \sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2 \qquad \text{H.Mul} : \prod_{i=1}^{k} \mathbf{C}_i$$

FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth

$$\mathbf{sC} = \mu\mathbf{s} + \mathbf{e}$$

H.Add : $\sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2$ H.Mul : $\prod_{i=1}^{k} \mathbf{C}_i$

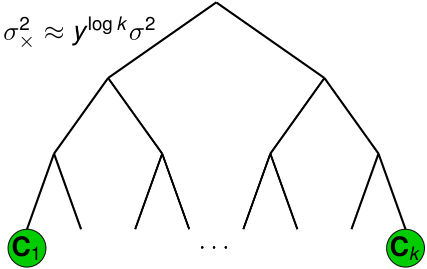


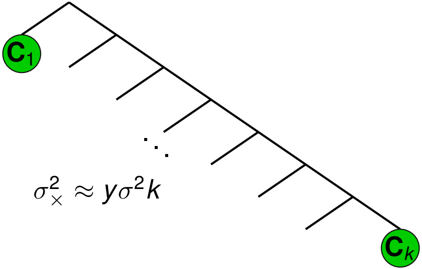
FLIP$_F$ Homomorphic Behavior

3^{rd} generation FHE Noise Growth

$$\mathbf{sC} = \mu\mathbf{s} + \mathbf{e}$$

H.Add : $\sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2$ H.Mul : $\prod_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_\times^2 \approx y\sigma^2 k$





FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth: H.Eval(F)

$$\text{H.Eval}(F) \approx \text{H.Mul}$$

$$\text{H.Add} : \sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2 \qquad \text{H.Mul} : \prod_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_\times^2 \approx y\sigma^2 k$$

FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth: H.Eval(F)

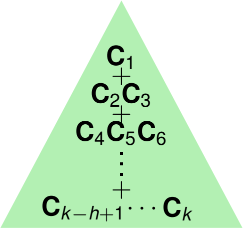
$$\text{H.Eval}(F) \approx \text{H.Mul}$$

$$\text{H.Add} : \sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2 \qquad \text{H.Mul} : \prod_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_\times^2 \approx y\sigma^2 k$$

${}^1\Delta^h$

k variables

$k = \frac{h(h+1)}{2}$



$$\mathbf{C}_1$$
$$+$$
$$\mathbf{C}_2\mathbf{C}_3$$
$$+$$
$$\mathbf{C}_4\mathbf{C}_5\mathbf{C}_6$$
$$\vdots$$
$$+$$
$$\mathbf{C}_{k-h+1}\cdots\mathbf{C}_k$$

FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth: H.Eval(F)

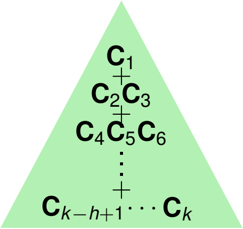
$$\text{H.Eval}(F) \approx \text{H.Mul}$$

$$\text{H.Add} : \sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2 \qquad \text{H.Mul} : \prod_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_\times^2 \approx y\sigma^2 k$$

${}^1\Delta^h$

k variables

$k = \frac{h(h+1)}{2}$



$\mathbf{C}_1$
$+$
$\mathbf{C}_2\mathbf{C}_3$
$+$
$\mathbf{C}_4\mathbf{C}_5\mathbf{C}_6$
$\vdots$
$+$
$\mathbf{C}_{k-h+1} \cdots \mathbf{C}_k$

$y\sigma^2 \times 1$

$y\sigma^2 \times 2$

$y\sigma^2 \times \vdots$

$y\sigma^2 \times h$

FLIP$_F$ Homomorphic Behavior

3rd generation FHE Noise Growth: H.Eval(F)

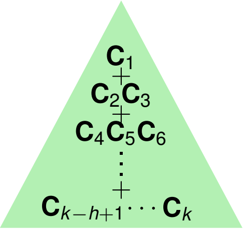
$$\text{H.Eval}(F) \approx \text{H.Mul}$$

$$\text{H.Add} : \sum_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_+^2 = \sum_{i=1}^{k} \sigma_i^2 \qquad \text{H.Mul} : \prod_{i=1}^{k} \mathbf{C}_i \rightarrow \sigma_\times^2 \approx y\sigma^2 k$$

${}^1\Delta^h$

k variables

$k = \frac{h(h+1)}{2}$



$\mathbf{C}_1$
$+$
$\mathbf{C}_2\mathbf{C}_3$
$+$
$\mathbf{C}_4\mathbf{C}_5\mathbf{C}_6$
$\vdots$
$+$
$\mathbf{C}_{k-h+1}\cdots\mathbf{C}_k$

$$\begin{array}{r|c|}
\cline{2-2}
y\sigma^2 \times & 1 \\
y\sigma^2 \times & 2 \\
y\sigma^2 \times & \vdots \\
y\sigma^2 \times & h \\
\cline{2-2}
\end{array}$$

$$y\sigma^2 \times \frac{h(h+1)}{2} = y\sigma^2 k$$

$$\text{H.Eval}({}^1\Delta^h)$$
$$\approx$$
$$\text{H.Mul}$$

FLIP$_F$ Symmetric Behavior

Cryptanalysis Angle

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

FLIP$_F$ 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
- G & D Attack [DLR16]
- etc

FLIP$_F$ 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
- G & D Attack [DLR16]
- etc

Standard Criteria

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

FLIP$_F$ 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
- G & D Attack [DLR16]
- etc

Standard Criteria

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

Theorem (Triangular function and Algebraic Immunity)

$$\forall \ell \in \mathbb{N}^*, \forall k \in \mathbb{N}^* \qquad \mathrm{AI}({}^{\ell}\Delta^{k}) = k$$

Noise Increase Performances

◇ Tests on Ring-GSW (efficiency)

◇ Measure noise increase from fresh ciphertext to FLIP ciphertext:
  - ◇ Log of ciphertext error ($\log \sigma$)
  - ◇ Homomorphic capacity already used (%).

Noise Increase Performances

- Tests on Ring-GSW (efficiency)

- Measure noise increase from fresh ciphertext to FLIP ciphertext:
  - Log of ciphertext error ($\log \sigma$)
  - Homomorphic capacity already used (%).

Experimental error growth

Ring (n, ℓ)		FLIP	Fresh		H.Mul		H.Eval(FLIP)	
			$\log \sigma$	%	$\log \sigma$	%	$\log \sigma$	%
256	80	$42, 128, {}^{8}\Delta^{9}$	$13, 07$	17 %	$19, 82$	25%	$24, 71$	31%
512	120	$82, 224, {}^{8}\Delta^{16}$	$14, 68$	12 %	$23, 27$	20%	$28, 77$	24%

Noise Increase Performances

- Tests on Ring-GSW (efficiency)

- Measure noise increase from fresh ciphertext to FLIP ciphertext:
    - Log of ciphertext error ($\log \sigma$)
    - Homomorphic capacity already used (%).

Experimental error growth

Ring (n, ℓ)		FLIP	Fresh		H.Mul		H.Eval(FLIP)	
			$\log \sigma$	%	$\log \sigma$	%	$\log \sigma$	%
256	80	$42, 128, {}^{8}\Delta^{9}$	$13, 07$	17 %	$19, 82$	25%	$24, 71$	31%
512	120	$82, 224, {}^{8}\Delta^{16}$	$14, 68$	12 %	$23, 27$	20%	$28, 77$	24%

$\rightarrow$ FLIP evaluation $\approx$ multiplication

$\rightarrow$ Practical SE-HE framework.

Performances Comparisons

Error Increase Comparisons

Algorithm	Reference	Multiplicative Depth
AES-128	[GHS12]	40
SIMON-64/128	[LN14]	44
Prince	[DSE+14]	24
Kreyvium-12	[CCF+15]	12
LowMc-128	[ARS+15]	12
FLIP$(82, 112, {}^{8}\Delta^{16})$	This work	$\lceil \log 16 \rceil = 4$

Performances Comparisons

Error Increase Comparisons

Algorithm	Reference	Multiplicative Depth
AES-128	[GHS12]	40
SIMON-64/128	[LN14]	44
Prince	[DSE+14]	24
Kreyvium-12	[CCF+15]	12
LowMc-128	[ARS+15]	12
FLIP$(82, 112, {}^{8}\Delta^{16})$	This work	$\lceil \log 16 \rceil = 4$

Timing Comparisons

λ	Algorithm	L+7	Latency (sec)	Throughput (bits/min)
80	Trivium-13	20	11379.7	516.3
	FLIP$(42, 128, {}^{8}\Delta^{9})$	12	17.39	2070.16
128	Kreyvium-12	19	4956.0	384.4
	LowMC-128	20	9977.1	739.0
	FLIP$(82, 224, {}^{8}\Delta^{16})$	13	124.97	345.68

Conclusion and Open Problems

Filter Permutator

- New stream cipher family adapted to FHE
- Security of reduced degree and increased key size construction?
- Impact of design tweaks:
    - Whitening?
    - XOR of parallel Filter Permutator?

Conclusion and Open Problems

Filter Permutator

- ◇ New stream cipher family adapted to FHE
- ◇ Security of reduced degree and increased key size construction?
- ◇ Impact of design tweaks:
  - ◇ Whitening?
  - ◇ XOR of parallel Filter Permutator?

FLIP_F

- ◇ Optimal noise increase for 3rd generation FHE
- ◇ Efficient FHE framework
- ◇ Optimization for 2nd generation FHE?
- ◇ Refining security analysis:
  - ◇ Increasing/decreasing parameter sizes?
  - ◇ Boolean functions with fixed weight entries?

Conclusion and Open Problems

Filter Permutator

- ◇ New stream cipher family adapted to FHE
- ◇ Security of reduced degree and increased key size construction?
- ◇ Impact of design tweaks:
    - ◇ Whitening?
    - ◇ XOR of parallel Filter Permutator?

FLIP_F

- ◇ Optimal noise increase for 3rd generation FHE
- ◇ Efficient FHE framework
- ◇ Optimization for 2nd generation FHE?
- ◇ Refining security analysis:
    - ◇ Increasing/decreasing parameter sizes?
    - ◇ Boolean functions with fixed weight entries?

Thanks for your attention!