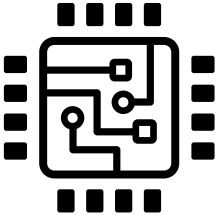
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

ChiLow and ChiChi: New Constructions for Code Encryption

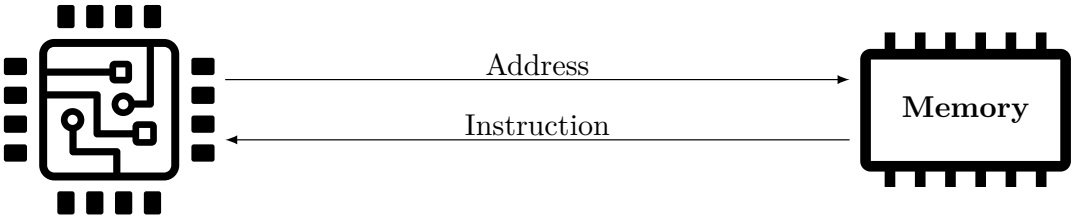
Eurocrypt 2025, Madrid, May 5

Yanis Belkheyar, Patrick Derbez, Shibam Ghosh, Gregor Leander, Silvia Mella, Léo Perrin, Shahram Rasoolzadeh, Lukas Stennes, Siwei Sun, Gilles Van Assche, and Damian Vizár

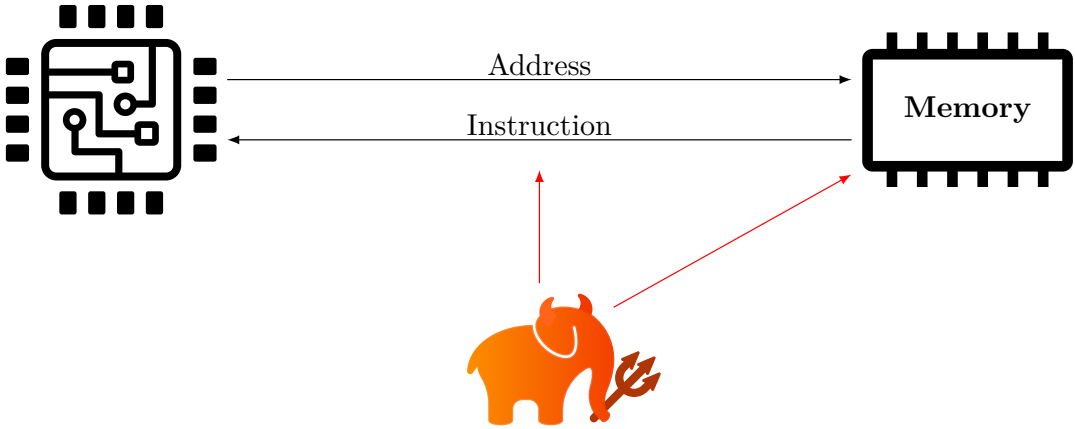
The Setting – Embedded Code Encryption



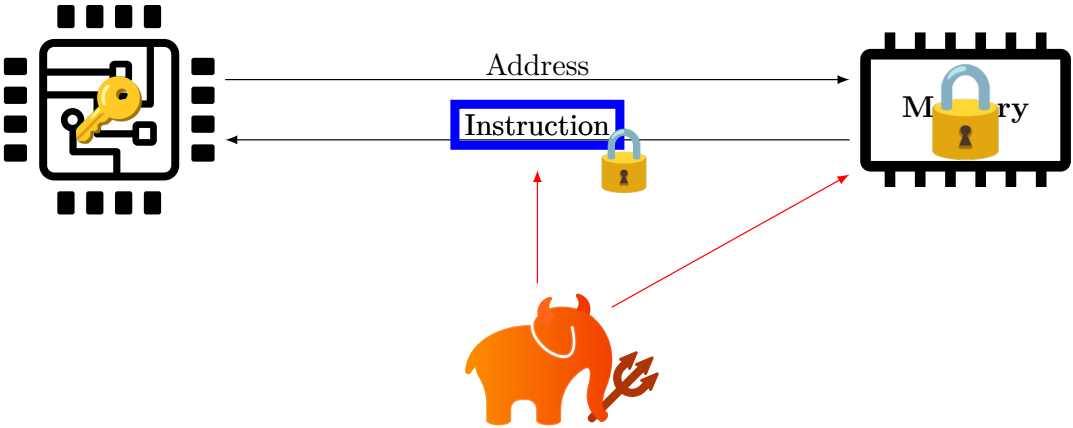
The Setting – Embedded Code Encryption



The Setting – Embedded Code Encryption



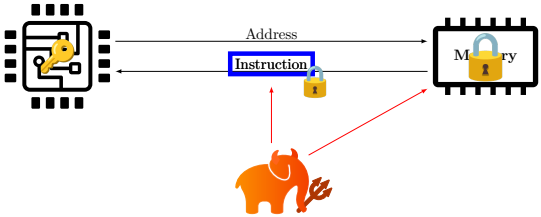
The Setting – Embedded Code Encryption



Requirements for Our New Design

CASA
Cyber Security in the Age of Large-Scale Adversaries

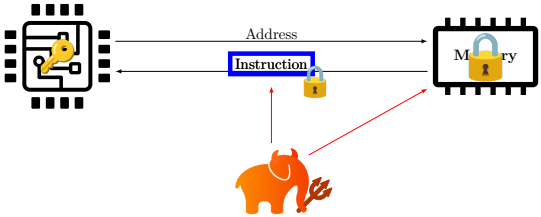
- Authenticated encryption
- Ultra low latency for decryption (1 clock cycle)
- Small block size
- Small authentication tags



Requirements for Our New Design

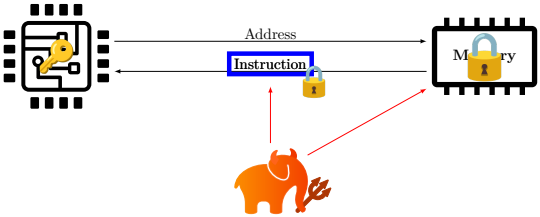
CASA
Cyber Security in the Age of Large-Scale Adversaries

- Authenticated encryption
- Ultra low latency for decryption (1 clock cycle)
- Small block size
- Small authentication tags



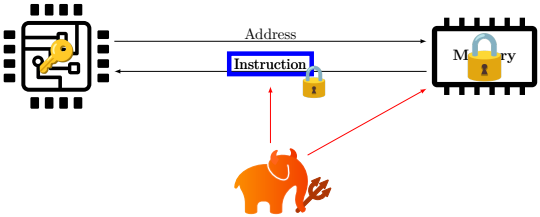
Requirements for Our New Design

- Authenticated encryption
- Ultra low latency for decryption (1 clock cycle)
- Small block size
- Small authentication tags



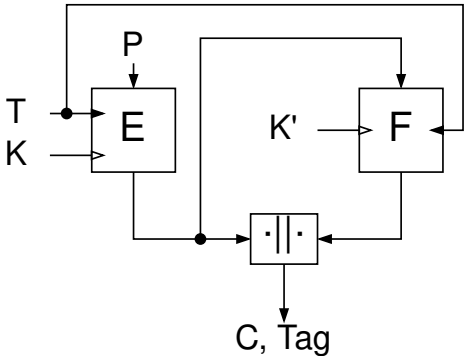
Requirements for Our New Design

- Authenticated encryption
- Ultra low latency for decryption (1 clock cycle)
- Small block size
- Small authentication tags

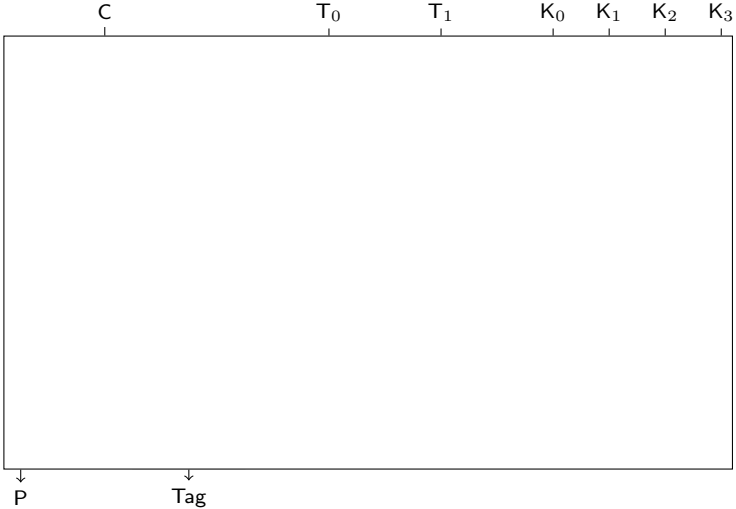


Requirements for Our New Design

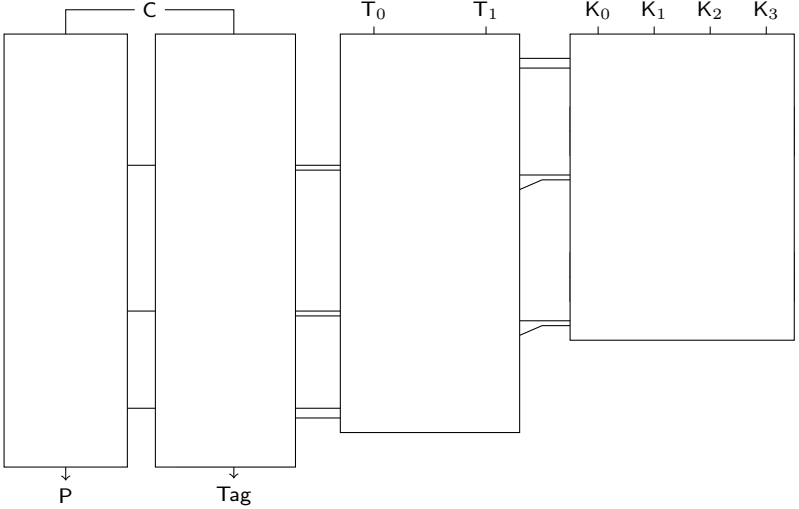
- Authenticated encryption
- Ultra low latency for decryption (1 clock cycle)
- Small block size
- Small authentication tags



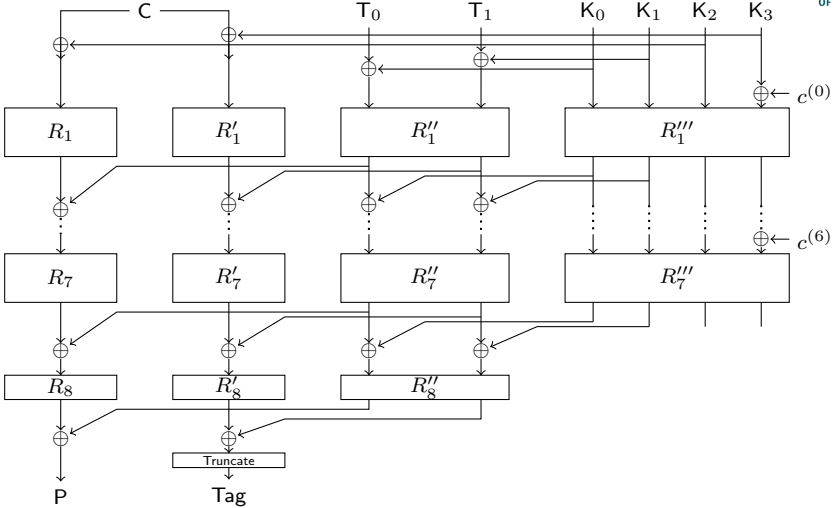
Our New Design – ChiLow



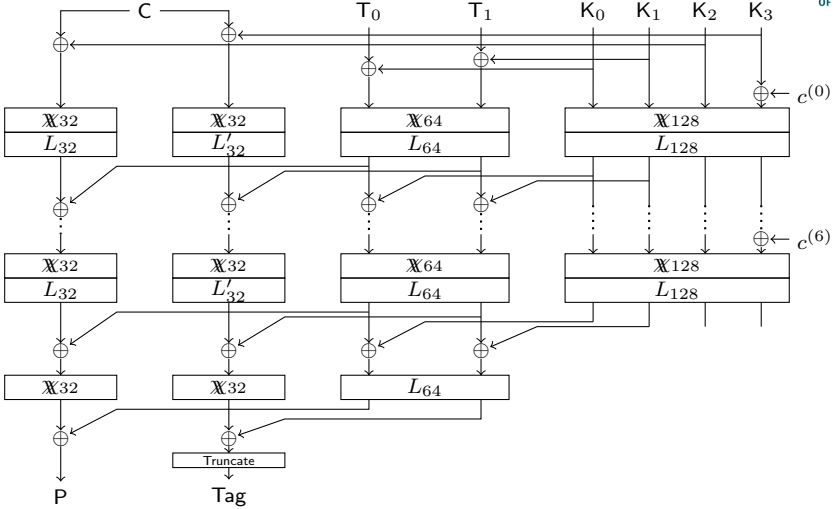
Our New Design – ChiLow



Our New Design – ChiLow



Our New Design – ChiLow



Linear Layer

$$y = L(x) \text{ with } x, y \in \mathbb{F}_2^{128 \text{ or } 64 \text{ or } 32}$$

$$y_i = x_{\alpha i+\beta_0} + x_{\alpha i+\beta_1} + x_{\alpha i+\beta_2}$$

Table: Offsets for the linear maps.

Linear Map	α	β_0	β_1	β_2
L_{32}	11	5	9	12
L'_{32}	11	1	26	30
L_{64}	3	1	26	50
L_{128}	17	7	11	14

Recap χ [Daemen '95]

CASA
Cyber Security in the Age of Large-Scale Adversaries

$$\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$

$$y_i = x_i + \overline{x}_{i+1} x_{i+2}$$

- Widely used (Ascon, SHA-3, etc.)
- Nice properties, including low latency
- Permutation if and only if n is odd
- For us: n is even

Recap χ [Daemen '95]

CASA
Cyber Security in the Age of Large-Scale Adversaries

$$\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$

$$y_i = x_i + \overline{x}_{i+1} x_{i+2}$$

- Widely used (Ascon, SHA-3, etc.)
- Nice properties, including low latency
- Permutation if and only if n is odd
- For us: n is even

Recap χ [Daemen '95]

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

$$\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$

$$y_i = x_i + \overline{x}_{i+1} x_{i+2}$$

- Widely used (Ascon, SHA-3, etc.)
- Nice properties, including low latency
- Permutation if and only if n is odd
- For us: n is even

Recap χ [Daemen '95]

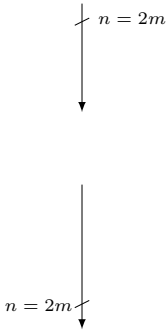
CASA
Cyber Security in the Age of Large-Scale Adversaries

$$\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$

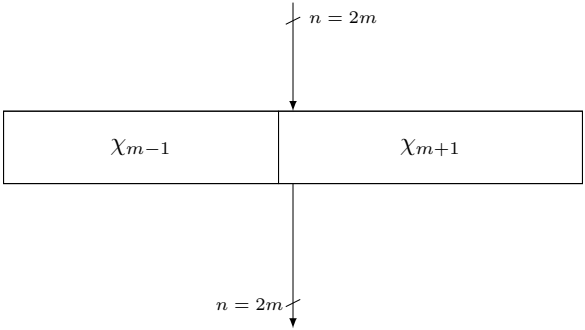
$$y_i = x_i + \overline{x}_{i+1} x_{i+2}$$

- Widely used (Ascon, SHA-3, etc.)
- Nice properties, including low latency
- Permutation if and only if n is odd
- For us: n is even

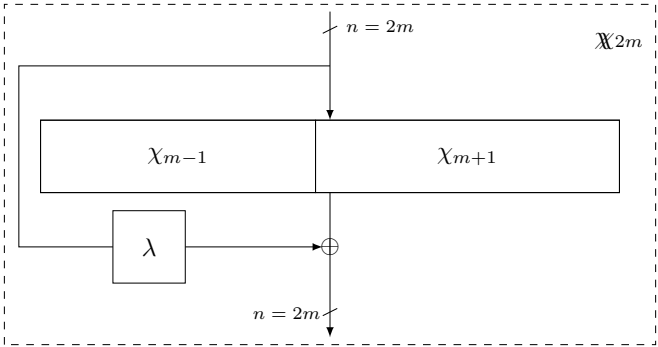
From χ to $\mathbb{X}$



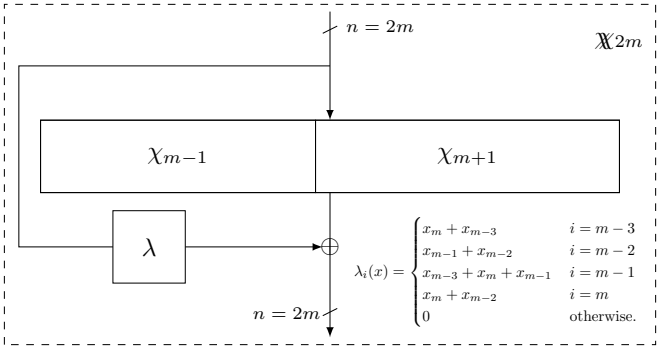
From χ to $\mathcal{X}$



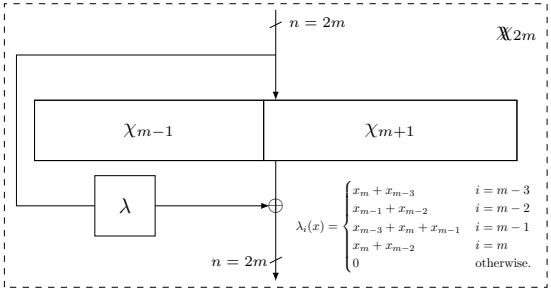
From χ to $\mathbb{X}$



From χ to $\mathbb{X}$



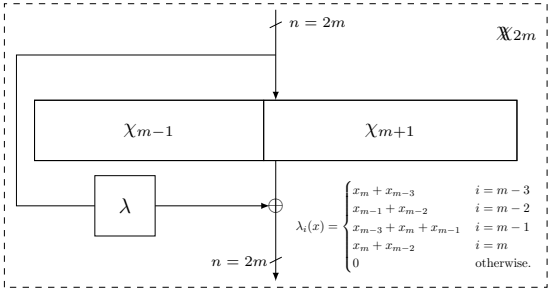
From χ to $\mathbb{X}$



$$(\chi_n)_i = x_i + \overline{x}_{i+1}x_{i+2}$$

$$(\mathbb{X}_{2m})_i(x) = \begin{cases} x_m + \overline{x}_{m-2}x_0 & i = m-3 \\ x_{m-1} + \overline{x}_0 x_1 & i = m-2 \\ \overline{x}_{m-3} + \overline{x}_m\overline{x}_{m+1} & i = m-1 \\ x_{m-2} + \overline{x}_{m+1}x_{m+2} & i = m \\ \chi_{m-1} \text{ or } \chi_{m+1} & \text{otherwise.} \end{cases}$$

From χ to $\mathbb{X}$



$$(\chi_n)_i = x_i + \overline{x}_{i+1}x_{i+2}$$

$$(\mathbb{X}_{2m})_i(x) = \begin{cases} x_m + \overline{x}_{m-2}x_0 & i = m-3 \\ x_{m-1} + \overline{x}_0 x_1 & i = m-2 \\ \overline{x}_{m-3} + \overline{x}_m\overline{x}_{m+1} & i = m-1 \\ x_{m-2} + \overline{x}_{m+1}x_{m+2} & i = m \\ \chi_{m-1} \text{ or } \chi_{m+1} & \text{otherwise.} \end{cases}$$

Theorem

For m even, $\mathbb{X}_{2m}$ is a bijection.

Inverse of χ

CASA
Cyber Security in the Age of Large-Scale Adversaries

Algorithm (Biryukov, Bouillaguet, Khovratovich 2014)

Input: y, ***Output:*** $x = \chi_n^{-1}(y)$
Let $x \leftarrow y$
For $0 \leq i < 3\lfloor \frac{n}{2} \rfloor$*:*
$x_{(n-2)i} \leftarrow x_{(n-2)i} \oplus y_{(n-2)i+2} \cdot y_{(n-2)i+1}$

Theorem (Liu, Sarkar, Meier, Isobe 2022)

The formula of χ_n^{-1} *is*

$$x_i = y_i + \sum_{j=1}^{h} y_{i-2j+1} \prod_{k=j}^{h} \overline{y}_{i-2k}$$

for $i \in [0, n-1]$*. In particular, the degree of* χ_n^{-1} *is* $h+1 = \frac{n+1}{2}$*.*

Inverse of χ

CASA
Cyber Security in the Age of Large-Scale Adversaries

Algorithm (Biryukov, Bouillaguet, Khovratovich 2014)

Input: y, ***Output:*** $x = \chi_n^{-1}(y)$
Let $x \leftarrow y$
For $0 \leq i < 3\lfloor \frac{n}{2} \rfloor$:
$x_{(n-2)i} \leftarrow x_{(n-2)i} \oplus y_{(n-2)i+2} \cdot y_{(n-2)i+1}$

Theorem (Liu, Sarkar, Meier, Isobe 2022)

The formula of χ_n^{-1} *is*

$$x_i = y_i + \sum_{j=1}^{h} y_{i-2j+1} \prod_{k=j}^{h} \overline{y}_{i-2k}$$

for $i \in [0, n-1]$. *In particular, the degree of* χ_n^{-1} *is* $h + 1 = \frac{n+1}{2}$.

Inverse of $\mathcal{X}$

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Suffices to give formulas for x_m, $x_m + x_{m-3}$, x_{m-1}, and x_{m-2}

Lemma (Formula for computing x_m)

For m even and $y = \mathcal{X}_{2m}(x)$, we have

$$x_m = y_{m-3} + \left(\sum_{i=0}^{\frac{m}{2}-2} y_{2i} \prod_{k=1}^{i} \overline{y}_{2k-1} \right) \left(\overline{y}_m + \left(\sum_{i=1}^{\frac{m}{2}-1} y_{2i+m} \prod_{k=1}^{i} \overline{y}_{2k+m-1} \right) + y_{m-2} \prod_{k=1}^{\frac{m}{2}} \overline{y}_{2k+m-1} \right).$$

Conjecture

Every non-trivial component of the inverse of $\mathcal{X}_{2m}$ has algebraic degree m.

Inverse of $\mathbb{X}$

- Suffices to give formulas for x_m, $x_m + x_{m-3}$, x_{m-1}, and x_{m-2}

Lemma (Formula for computing x_m)

For m even and $y = \mathbb{X}_{2m}(x)$, we have

$$x_m = y_{m-3} + \left(\sum_{i=0}^{\frac{m}{2}-2} y_{2i} \prod_{k=1}^{i} \overline{y}_{2k-1} \right) \left(\overline{y}_m + \left(\sum_{i=1}^{\frac{m}{2}-1} y_{2i+m} \prod_{k=1}^{i} \overline{y}_{2k+m-1} \right) + y_{m-2} \prod_{k=1}^{\frac{m}{2}} \overline{y}_{2k+m-1} \right).$$

Conjecture

Every non-trivial component of the inverse of $\mathbb{X}_{2m}$ has algebraic degree m.

Inverse of $\mathbb{X}$

- Suffices to give formulas for x_m, $x_m + x_{m-3}$, x_{m-1}, and x_{m-2}

Lemma (Formula for computing x_m)

For m even and $y = \mathbb{X}_{2m}(x)$, we have

$$x_m = y_{m-3} + \left(\sum_{i=0}^{\frac{m}{2}-2} y_{2i} \prod_{k=1}^{i} \overline{y}_{2k-1} \right) \left(\overline{y}_m + \left(\sum_{i=1}^{\frac{m}{2}-1} y_{2i+m} \prod_{k=1}^{i} \overline{y}_{2k+m-1} \right) + y_{m-2} \prod_{k=1}^{\frac{m}{2}} \overline{y}_{2k+m-1} \right).$$

Conjecture

Every non-trivial component of the inverse of $\mathbb{X}_{2m}$ has algebraic degree m.

Results

CASA
Cyber Security in the Age of Large-Scale Adversaries

Table: Comparison for the Nangate 15nm open cell library.

Cipher	Type	Key/Tweak/Block [bits/bits/bits]	Area [μm^2]	Area [GE]	Latency [ps]	Power [mW]
ChiLow-(32+16)	TBC+PRF	128/64/32	3581.85	18218.25	282.73	0.2521
Scarf	TBC	240/48/10	1096.48	5577.00	216.80	0.0793
Prince	BC	128/-/64	2450.08	12461.75	374.04	0.3433
Qarmav1$_5$-64	TBC	128/64/64	2652.09	13489.25	378.30	0.8172
Orthros	PRF	128/-/128	7372.26	37497.25	354.79	0.8144
Gleeok-128-IP$_{64}$	AE	256/-/128	24616.70	125207.01	382.99	4.1930

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$
  - Prove conjecture
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$
  - Prove conjecture
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$
  - Prove conjecture
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$
  - Prove conjecture
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$ ✓
  - Prove conjecture ✓
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$ ✓
  - Prove conjecture ✓
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$ ✓
  - Prove conjecture ✓
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$ ✓
  - Prove conjecture ✓
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$ ✓
  - Prove conjecture ✓
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Future Work

- $\mathbb{X}$
  - Generalize $\mathbb{X}$ ✓
  - Prove conjecture ✓
  - ...
  - Work in progress
- ChiLow – call to action
  - Cryptanalysis
  - Side-channel attacks/protection
  - Real-world implementation

Thank You!