

# **Gimli: A Lightweight Permutation and Cipher**

## Overview and Technical Analysis

---

Riya Jana

December 9, 2025

Indian Institute of Technology Bhilai

# Outline

Introduction

The Gimli Permutation

The Revised Gimli Permutation

Gimli Toy Version

Cryptanalysis of Gimli

MILP on GIMLI

HARDWARE ANALYSIS on GIMLI

Browney

Comparison

Conclusion

# Introduction

---

# The Rise of Lightweight Cryptography

- **Motivation:** IoT, RFID tags, and embedded microcontrollers require secure yet low-resource cryptography.
- **Challenge:** Classical ciphers consume too much power, memory, and computation.
- **Approach:** Lightweight cryptography provides security with minimal overhead.

## Key Idea

Design efficient, secure primitives specifically optimized for constrained environments.

## Introducing Gimli

---

- Proposed in 2017 by Bernstein, Schwabe, et al.
- 384-bit permutation suitable for CPUs, FPGAs, and ASICs.
- Simple ARX-like structure: rotations, XORs, swaps — no tables.
- Useful for hash functions, PRFs, and authenticated encryption.

**Goal:** Achieve simplicity, security, and cross-platform efficiency.

# The Gimli Permutation

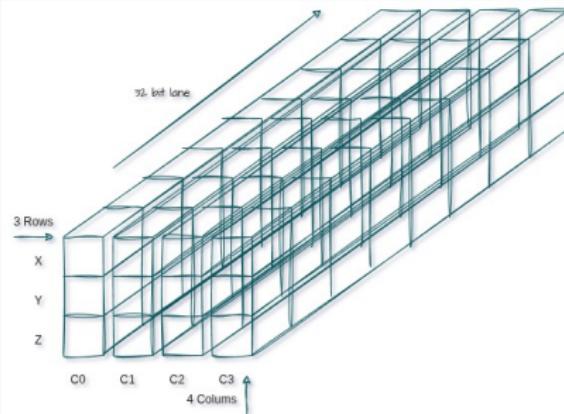
---

# State Layout

Gimli uses a 384-bit state arranged as a  $3 \times 4$  matrix of 32-bit words:

$$S = \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \end{bmatrix}$$

- **Rows:** Logical registers  $x, y, z$  (SIMD-friendly).
- **Columns:** Independent 96-bit lanes processed in parallel.



# Round Function

Each of the 24 rounds includes three components:

1. **Non-linear SP-box** (per 96-bit column):

$$z' = x \text{ XOR } (z \ll 1) \text{ XOR } ((y \text{ AND } z) \ll 2)$$

$$y' = y \text{ XOR } x \text{ XOR } ((x \text{ OR } z) \ll 1)$$

$$x' = z \text{ XOR } y \text{ XOR } ((x \text{ AND } y) \ll 3)$$

2. **Linear Mixing Layer**: Column swaps every 4 rounds:

- Small Swap:  $r \bmod 4 = 0$
- Big Swap:  $r \bmod 4 = 2$

3. **Round Constant**: breaks symmetry

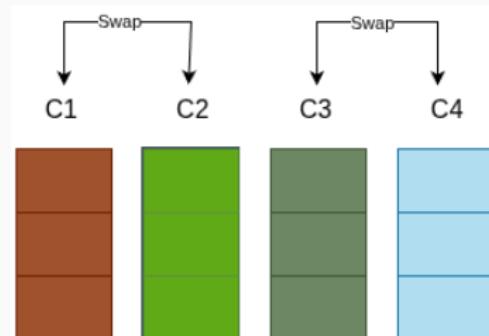
$$s_{0,0} \leftarrow s_{0,0} \oplus (0x9e377900 \oplus r)$$

# Small Big Swaps

Swapping columns improves diffusion across lanes.

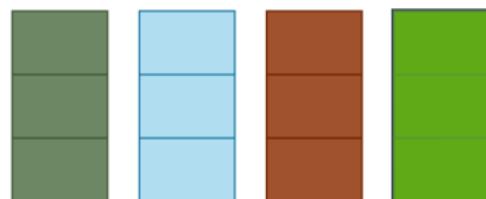
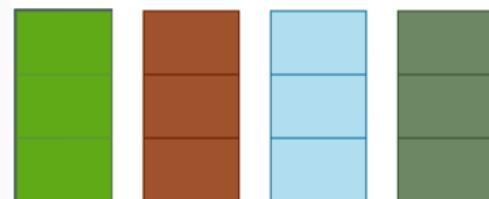
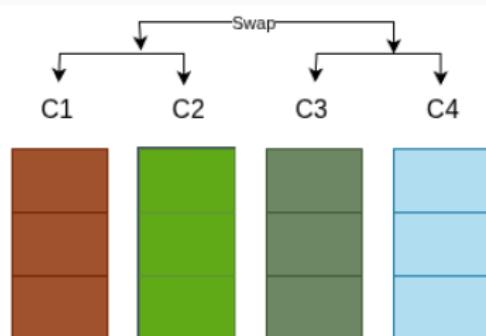
## Small Swap ( $r \bmod 4 = 0$ )

- Swap columns 0 1
- Swap columns 2 3



## Big Swap ( $r \bmod 4 = 2$ )

- Swap columns 0 2
- Swap columns 1 3



## The Revised Gimli Permutation

---

## Revised Gimli Using a 3-Bit S-Box

**Motivation:** Replacing Gimli's original nonlinear word transformation with a compact 3-bit S-box yields multiple advantages:

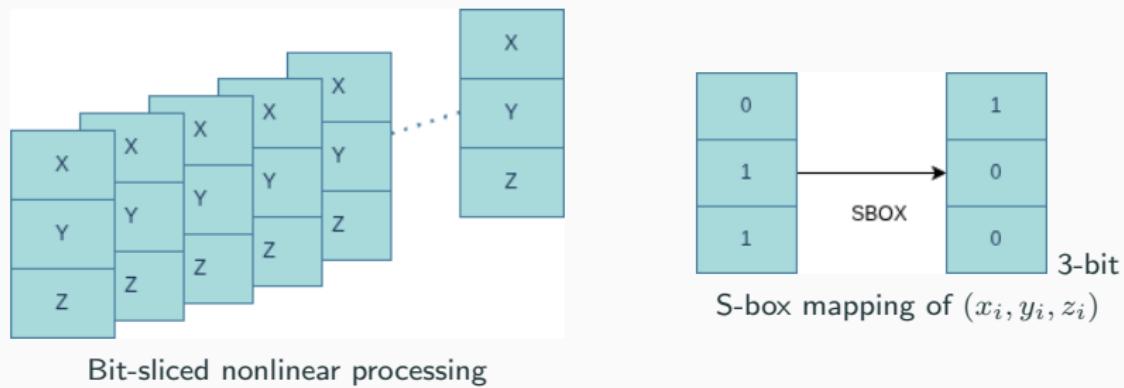
- **Simplified theoretical analysis:** Word-based rotations, AND, OR, and branching are difficult to express in MILP and SAT models. A 3-bit S-box is algebraically compact and fully tabulated.
- **Fine-grained bit tracing:** Each bit-triplet  $(x, y, z)$  is processed independently, allowing precise tracking of diffusion and avalanche behavior.
- **Cryptographic tunability:** S-boxes can be swapped or optimized to achieve better differential or algebraic properties, unlike the rigid ARX nonlinear layer.

**Outcome:** The revised permutation remains structurally consistent with Gimli while dramatically improving tractability for automated security evaluation.

# Simplified Gimli Permutation (24 Rounds)

## Round structure:

- Each round processes state arrays  $(x, y, z)$ .
- Planes are rotated  $(x \leftarrow 24, y \leftarrow 9)$ .
- Each word is sliced to 32 independent bit-tuples.
- Every bit-tuple  $(x_i, y_i, z_i)$  is mapped using the 3-bit S-box.
- SmallSwap and BigSwap preserve Gimli's original column diffusion.
- Round constant ensures symmetry breaking.



# S-Box Analysis and Security Implications

**Nonlinear component:**

$$S = [7, 4, 6, 1, 0, 5, 2, 3], \quad S^{-1} = [4, 3, 6, 7, 1, 5, 2, 0]$$

**Key properties:**

- Balanced outputs and quadratic ANF ensure strong algebraic resistance.
- Differential and boomerang uniformity equal to 2 (optimal for 3-bit bijections).
- Easy DDT, BCT, and integral analysis enables clean reduced-round evaluation.

**Result:** The modified Gimli retains its structural intuition while providing a mathematically transparent nonlinear core that supports both automated cryptanalysis and efficient hardware mapping.

## Gimli Toy Version

---

# Toy Version of the Gimli Permutation

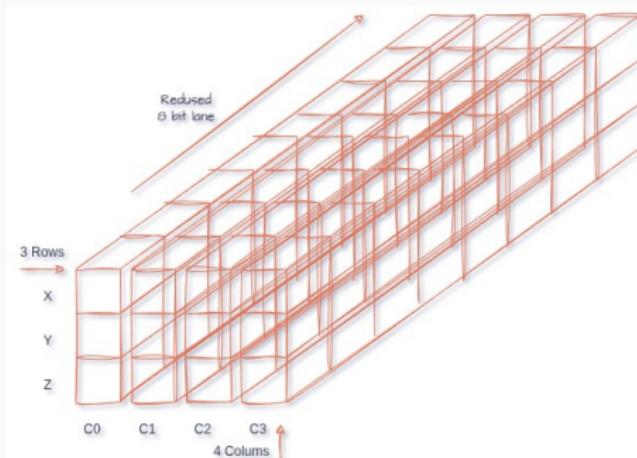
**Motivation:** The toy version is a reduced-scale model of Gimli designed to simplify experimentation and automated cryptanalysis, while retaining its structural characteristics.

## State representation:

Toy state:  $3 \times 4$  matrix of 8-bit words = 96 bits

## Key idea:

- Ideal platform for exploring differential, impossible, and boomerang trails



# Round Structure of Toy Gimli (12 Rounds)

**State:**

$$(x, y, z) \in (\mathbb{F}_2^8)^4, \quad \text{stored as a } 3 \times 4 \text{ byte matrix}$$

**Each round consists of four layers:**

1. **Rotation layer**

$$x \ll 6, \quad y \ll 2$$

Two byte-planes are cyclically rotated to initiate intra-column diffusion.

2. **Nonlinear S-box layer** Every bit-column  $(x_i, y_i, z_i)$  (for all 32 bit-slices) is mapped using

$$S = [7, 4, 6, 1, 0, 5, 2, 3]$$

providing compact nonlinear confusion.

3. **Mixing layer**

$$\text{if } r \bmod 4 = 0 \Rightarrow \text{SmallSwap}, \quad \text{if } r \bmod 4 = 2 \Rightarrow \text{BigSwap}$$

Conditional permutations shuffle columns to spread activity.

4. **Round constant addition**

$$x_0 \leftarrow x_0 \oplus \text{RC}(r)$$

A small constant prevents symmetry and low-weight iterative trails.

# Original Gimli vs Toy Version

Feature	Original Gimli	Toy Version
State size	384 bits	96 bits
Word size	32-bit	8-bit
Rounds	24	12
Nonlinear layer	ARX (word-based)	3-bit S-box
MILP/SAT modeling	Hard	Tractable
Trail search	Very expensive	Exhaustive possible
Integral behavior	Full-state diffusion	Fast to verify
Cryptanalytic use	Real permutation	Educational + reduced

**Interpretation:** The toy permutation preserves the structural philosophy (rotation + substitution + swap) but dramatically reduces modeling complexity, making it suitable for automated reduced-round security evaluation.

# Cryptanalysis of Gimli

---

# Impossible Differential Analysis on toy-Gimli



# Truncated Differential Analysis of Toy-Gimli

## Goal

- Measure diffusion from a 1-bit input difference.
- Observe truncated differential behavior over rounds.

## Input Difference:

$$\Delta = (01\ 00\ 00\ 00, \ 00\ 00\ 00\ 00, \ 00\ 00\ 00\ 00)$$

## Experiment

- Random plaintext  $P_1$
- Paired  $P_2 = P_1 \oplus \Delta$
- Rounds  $r \in \{1, 2, 3, 4\}$
- Compute  
$$\Delta' = E(P_1) \oplus E(P_2)$$
- 1000 trials/round

## Recorded Metrics

- Distinct truncated outputs
- Maximum empirical probability
- Hamming weight distribution

## Results: Rounds 1–4

### Summary Table

Rounds	Unique $\Delta'$	Max Prob.	HW Trend
1	4	25.9%	Mostly HW 1
2	74	8.0%	Low–medium HW
3	275	6.3%	Wide HW spread
4	442	2.6%	Broad HW, near-uniform

### Observations

- # of truncated outputs grows rapidly with rounds.
- Maximum differential probability decays quickly.
- Hamming weights become increasingly dispersed.

# Interpretation and Security Impact

## Diffusion Quality

- **1 round:** highly biased, low diffusion
- **2 rounds:** structure weakens, mixing begins
- **3 rounds:** nonlinear spreading, near-random outputs
- **4 rounds:** truncated differences nearly uniform

## Security Implications

- Truncated distinguishers rely on biased, low-weight output differences. After 3–4 rounds, Toy-Gimli exhibits:
  - large truncated differential spaces
  - low maximum probabilities
  - medium–high Hamming weights

## Conclusion:

Toy-Gimli demonstrates rapid diffusion even in reduced-round form.

Truncated differential attacks become statistically ineffective.

# Differential & Boomerang Analysis

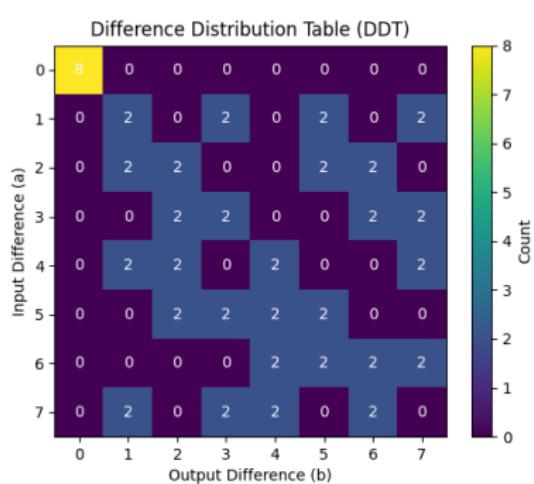
A 3-bit S-box abstraction is used:

$$S = [7, 4, 6, 1, 0, 5, 2, 3]$$

## DDT

- Differential uniformity

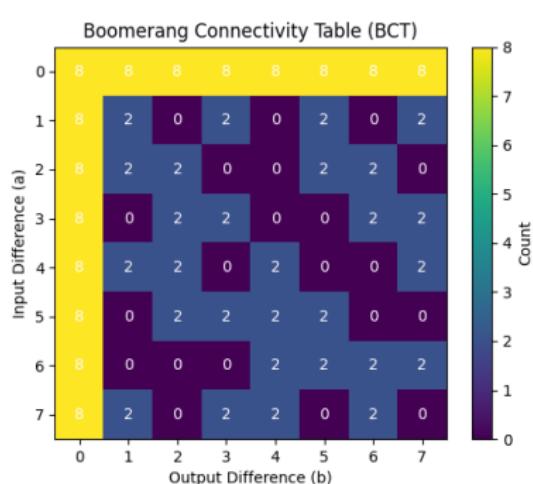
$$\delta_S = 2$$



## BCT

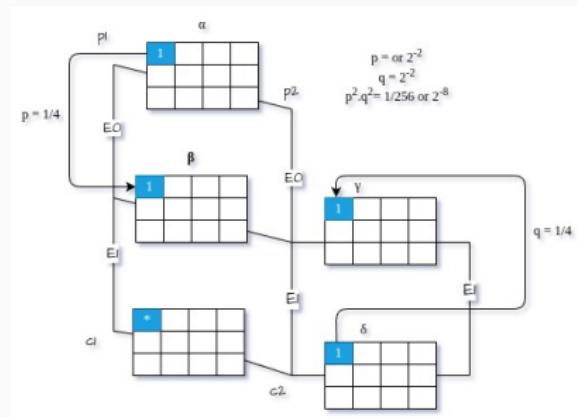
- Boomerang uniformity

$$\beta_S = 2$$



# Boomerang Analysis: 3-Bit S-Box

**Boomerang concept:** A boomerang attack combines two short differential trails, one through  $S$  and one through  $S^{-1}$  forming a boomerang quartet.



hence one valid quartet is expected per 256 random plaintext pairs.

$$(P, P', X, X') = (6, 7, 7, 6), \quad X \oplus X' = 1 = \alpha.$$

# Integral Cryptanalysis

**Idea:** Vary structured subsets of inputs and test whether XOR-sums of outputs cancel.

Rounds	Zero-Sum Found?
6	Yes
7	Yes
8	Yes (2-word variation)
9	No
10	No

## Interpretation

Integral properties vanish after 8 rounds, showing fast diffusion and a strong security margin compared to 24 rounds.

# Higher-Order Differential Analysis

Order	Result	Interpretation
1st Derivative	Non-zero	Nonlinearity present
2nd Derivative	Non-zero	Quadratic interactions
3rd Derivative	Zero	Degree $\leq 2$
4th Derivative	Zero	No higher algebraic leakage
Algebraic Degree	$\deg = 2$	S-box structure

## Interpretations

The third and fourth-order derivatives vanish, proving quadratic algebraic degree and controlled nonlinear dependency.

## Differential and Boomerang Summary

Metric	Value	Implication
Differential Uniformity $\delta_S$	2	Best for 3-bit nonlinear map
Boomerang Uniformity $\beta_S$	2	No rectangle bias
Max Differential Probability	1/4	Acceptable bound
Integral Threshold	8 rounds	Fast diffusion

- Differential and boomerang uniformity are both 2 (optimal for 3-bit S-boxes).
- No dominant differential paths, ensuring robustness against classical and boomerang attacks.
- Fast diffusion across rounds strengthens integral and multi-round security.

# Toy Two-Round Differential–Linear Model

## Cipher Design

- Toy 2-round substitution cipher:  $C = S(S(P))$
- 3-bit Gimli S-box
- No key addition or diffusion between rounds
- Minimal structure isolates DL behavior

## Differential Stage (Round 1)

- Input pair  $(P, P')$  with difference  $\alpha = P \oplus P'$
- First-round outputs:

$$Y = S(P), \quad Y' = S(P')$$

- Differential event:  $Y \oplus Y' = \beta$
- Differential probability:

$$p = \Pr[\beta \mid \alpha] = \frac{2}{8} = 0.25$$

# Linear Stage and DL Combination

## Linear Stage (Round 2)

- Outputs:  $C = S(Y)$ ,  $C' = S(Y')$
- Linear expression:

$$L = \text{parity}(\delta \cdot C) \oplus \text{parity}(\delta \cdot C')$$

- LAT correlation:

$$q = \pm \frac{1}{2}, \quad q^2 = \frac{1}{4}$$

## DL Theory

$$\text{Corr}[DL] = \pm pq^2$$

## Expected Value

$$pq^2 = \frac{1}{4} \cdot \left(\frac{1}{2}\right)^2 = 0.0625$$

Matches observed maximum correlation

# Experimental Results

## Setup

- 112 differential-linear trails tested
- 200,000 chosen plaintext pairs per trail
- A trail is valid if its empirical correlation  $\neq 0$

## Results

- 105 trails behave like random noise
- 7 trails show perfect correlations:  
 $\text{Corr}_{\text{empirical}} = \pm 1$
- Caused by:
  - very small 3-bit state
  - no key mixing and no diffusion between rounds

## Conclusion

- DL mechanism validated:  
 $p$  filtering +  $q^2$  bias
- Perfect correlations are structural, not statistical
- Real ciphers remove them using:
  - strong diffusion
  - round-based key

## MILP on GIMLI

---

# MILP Trail Optimization

Parameter	Value	Comment
Binary Variables	2753	Solver size
Constraints	5121	Boolean modeling
Objective	Minimize active bits	Differential trail
Output Weight (1 Round)	20 bits	Good diffusion
Security	Strong	No weak short trail

- MILP confirms strong nonlinear spreading even from a single active bit.
- High output weight per round prevents low-weight differential trails.
- No shortcut attacks detected through automated optimization modeling.

# Algebraic Normal Form (ANF)

---

ANF expressions of each output bit:

$$X_{\text{out}0} = 1 \oplus A \oplus B \oplus C \oplus BC,$$

$$Y_{\text{out}1} = 1 \oplus A \oplus C \oplus AC \oplus BC,$$

$$Z_{\text{out}2} = 1 \oplus C \oplus AB \oplus AC.$$

Notations:

- Addition = XOR    Multiplication = AND
- Each output is a degree-2 Boolean polynomial

# Algebraic Properties of the S-Box

Output bit	Highest monomials	Degree	Balanced?
$X_{out_0}$	$BC$	2	Yes
$Y_{out_1}$	$AC, BC$	2	Yes
$Z_{out_2}$	$AB, AC$	2	Yes

- All outputs have algebraic degree 2 → good nonlinear resistance.
- Each Boolean function is balanced (Hamming weight 4) → no output bias.
- Compact ANF supports algebraic security proofs and hardware mapping.

# HARDWARE ANALYSIS on GIMLI

---

# S-Box Hardware Cost

Metric	Value	Interpretation
Technology	65 nm CMOS	ASIC-ready
Logic Cells	6	Very compact
Area	$12.6 \mu\text{m}^2$	Lightweight
Delay	170 ps	High-speed
Power	0.46 $\mu\text{W}$	Good for IoT

- Gate-level implementation is extremely compact and area-efficient.
- Delay and power figures make the S-box suitable for embedded and IoT devices.
- Very small hardware footprint supports low-cost ASIC deployment.

# Full Round Hardware Scaling

Metric	Value	Interpretation
S-Boxes per Round	128	Parallel nonlinear layer
Gate Equivalent (GE)	1120 GE	Very low logic cost
Round Power	64 $\mu$ W	IoT-friendly
Round Latency	170 ps	Pipeline compatible
Application	RFID, Sensors, ASICs	Ultra-low area

- Optimal differential and boomerang behavior ensures nonlinear robustness.
- Fast diffusion and high activity eliminate low-weight round trails.
- No structural weakness is observable near the full 24-round permutation.

# Cryptanalytic Summary

Property	Result	Interpretation
Differential Uniformity	2	Optimal for 3-bit S-box
Boomerang Uniformity	2	No weak boomerang rectangles
Integral Order (Toy)	$\leq 8$ rounds	Full diffusion after round 8
Active Bits / Round	20	High nonlinearity and spreading
Degree Growth	Quadratic	Prevents higher-order DC
Security Margin	Strong	No weakness for 24 rounds

**Browney**

---

# MILP Objective and Modeling

---

## Goal:

- Find minimum active nonlinear components in 6 rounds of the Gimli nonlinear layer.

## Modeling:

- State consists of 3 parallel 32-bit branches:  $X, Y, Z$ .
- Binary variables for differential activity.
- Linear constraints model XOR, AND, and bit rotations.
- Boundary condition: a single active input bit.

## Setup:

- 6 rounds, 1440 binary variables, 4609 constraints
- Solver: Gurobi (default)

# Optimization Result

---

## Outcome:

- Minimum total activity: 12 (i.e., 2 per round)
- Only one active bit propagates across all rounds
- $Y$  and  $Z$  remain inactive
- Nonlinear AND terms never activate

## Interpretation:

- Differential propagation behaves linearly via rotation
- Provides a lower bound for resistance of the nonlinear layer

# SAT Encoding Overview for One Round of Gimli

**Objective:** represent one Gimli round as a Boolean SAT instance.

- Gimli state: 12 words of 32 bits
$$(X_0, X_1, X_2, X_3, Y_0, Y_1, Y_2, Y_3, Z_0, Z_1, Z_2, Z_3)$$
- Each word expanded into 32 Boolean variables
- A single round therefore has:  
384 input bits and 384 output bits
- SAT instance = CNF clauses enforcing the correct round transition

# Nonlinear SP-Box Encoding

**Each column  $(x, y, z)$  is updated independently:**

$$Z'_i = x \oplus (z \ll 1) \oplus (y \wedge z \ll 2),$$

$$Y'_i = y \oplus x \oplus (x \vee z \ll 1),$$

$$X'_i = z \oplus y \oplus (x \wedge y \ll 3).$$

**CNF Construction (Tseitin Encoding):**

- AND, OR, XOR gates converted to clauses using auxiliary literals
- Each shifted bit either references a previous bit or constant 0
- No approximation: every Boolean relation is exact

**Result:** SP-box produces a polynomial number of clauses, preserving satisfiability.

# Toy Gimli-Based Hash Construction

## Toy sponge hash:

- Internal state: 12 bytes ( $x, y, z$ ) from the toy Gimli permutation
- Absorption (up to 3 message bytes):

$$x[0] \oplus = m_0, \quad y[0] \oplus = m_1, \quad z[0] \oplus = m_2$$

- Remaining state bytes act as capacity
- After absorption:

$$S' = \text{Gimli}(S, R)$$

- with  $R$  reduced rounds
- Squeezing: 8-bit output

**Idea:** Output is intentionally tiny  $\Rightarrow$  collisions expected.

# Educational Collision Attack

---

$$\text{Collision complexity} \approx \sqrt{2^n} = \sqrt{2^8} = 2^{8/2} = 2^4 = 16$$

## Experimental results ( $R = 2\text{--}12$ ):

- Collisions found for all round counts
- Often within 1 attempt
- Worst case: 17 attempts at  $R = 8$

## Key takeaway:

- Round depth does *not* prevent collisions with 8-bit output
- This does **not** attack real Gimli-Hash
- Real sponge hashes require  $\geq 128$ -bit outputs for security

## Comparison

---

# S-box / Cipher Comparison

**Table 1:** Comparison of Lightweight Cipher Nonlinear Layers Based on Hardware Cost and Algebraic Properties

S. No.	Cipher / S-box	LUT	ANF	DBN	Bit-Width	Algebraic Degree	NAND2 GE
1	Keccak	20.5 GE	20.5 GE	2	5	2	1.44
2	Gimli	8.75 GE	8.75 GE	2	3	2	1.44
3	Qarma v2	26 GE	26 GE	2	4	3	1.44
4	Elephant	23.25 GE	24 GE	2	4	3	1.44
5	Romulus	20.75 GE	20.75 GE	2	4	3	1.44
6	Twinkle	22.25 GE	22.75 GE	2	4	3	1.44
7	Saturnin	24.75 GE	25 GE	2	4	3	1.44

*Although the Gimli S-box has algebraic degree 2, the permutation applies up to 128 S-boxes per round. Therefore, the global algebraic system is large, diffuse, and very hard to solve, making algebraic attacks impractical at the permutation level.*

## Conclusion

---

# Conclusion

---

- **Efficient Design:** ARX-like simplicity with strong diffusion.
- **Robust Security:**
  - Low differential / boomerang uniformity
  - Rapid diffusion in integral tests
  - High algebraic degree growth
- **Security Margin:** All attacks apply only to heavily reduced-round variants.

**No structural vulnerabilities threaten the full 24-round Gimli permutation.**

# Questions?

Thank you.