CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

# Constructing and Deconstructing Intentional Weaknesses in Symmetric Ciphers

**CRYPTO**, 2022

Christof Beierle    Tim Beyne    Patrick Felke    Gregor Leander
Ruhr-Universität Bochum, KU Leuven, University Emden/Leer

RUHR UNIVERSITÄT BOCHUM RUB

KU LEUVEN

University of Applied Sciences HOCHSCHULE EMDEN·LEER

# Backdoors/Intentional Weaknesses

CASA
Cyber Security in the Age of Large-Scale Adversaries

Long-standing interesting topic

- Political: Law Enforcement,...
- Deployed: DES, DualEC, GEA-1...
- Academic: Dedicated BC, SHA-1 variants, MALICIOUS,...

# Backdoors/Intentional Weaknesses

Long-standing interesting topic

- Political: Law Enforcement,...
- Deployed: DES, DualEC, GEA-1...
- Academic: Dedicated BC, SHA-1 variants, MALICIOUS,...

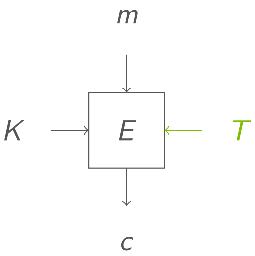
**Disclaimer**

We do not want people to build backdoors but prevent it.

# Backdoors/Intentional Weaknesses

Different Flavors (see [PW20])

- Undetectability
- Untraceability
- Practicability




Achieving all gives public key encryption. We aim at less.

# Our Contribution

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

**Deconstructing**

Explain how the GEA-1 backdoor could have been constructed.

# Our Contribution

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

## Deconstructing

Explain how the GEA-1 backdoor could have been constructed.

## Constructing

Built tweakable ciphers with backdoors. More natural than before.

1. MALICIOUS 2.0
2. GEA-1

# MALICIOUS [PW20]

## Backdoor

A pair of tweaks that give a probability one differential.

## Pros

undetectable, practicable

# MALICIOUS [PW20]

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

**Backdoor**

A pair of tweaks that give a probability one differential.

**Pros**

undetectable, practicable

**Cons**

requires lot of freedom, LowMC-like cipher required, not very natural.

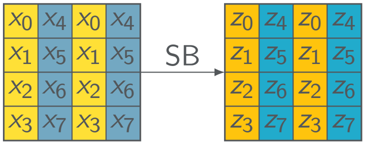
**Our Idea: MALICIOUS 2.0**

Build weakness on invariants instead of differentials

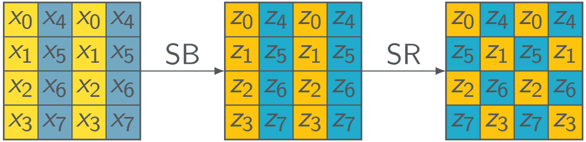
# AES Invariant Space (folklore)

| | | | |
|---|---|---|---|
| $x_0$ | $x_4$ | $x_0$ | $x_4$ |
| $x_1$ | $x_5$ | $x_1$ | $x_5$ |
| $x_2$ | $x_6$ | $x_2$ | $x_6$ |
| $x_3$ | $x_7$ | $x_3$ | $x_7$ |

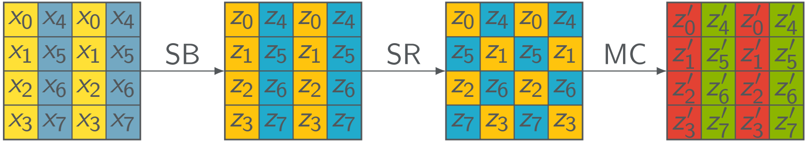
# AES Invariant Space (folklore)



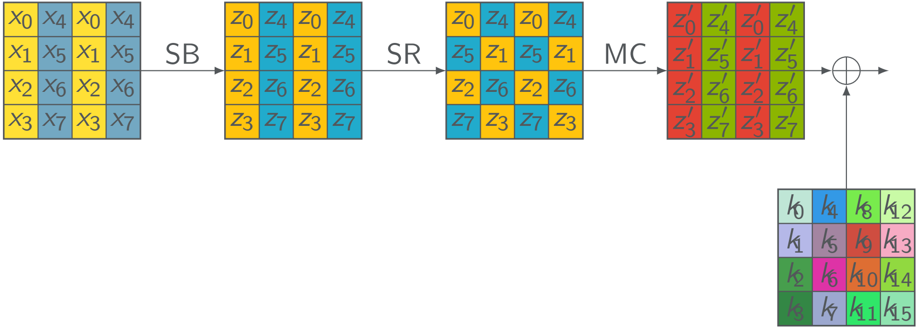
# AES Invariant Space (folklore)



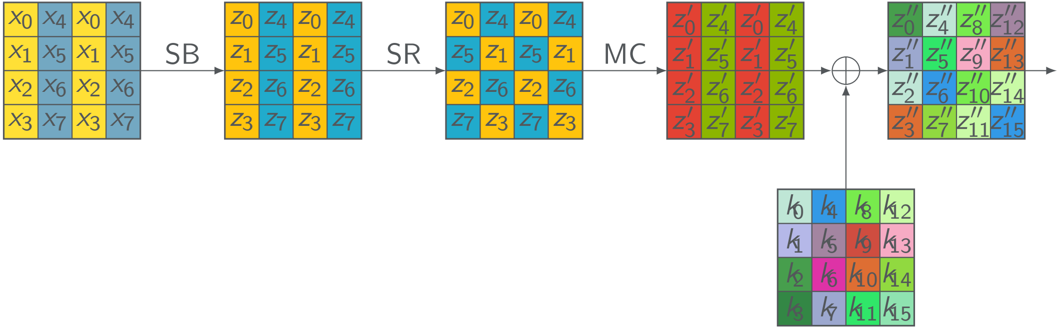
# AES Invariant Space (folklore)



# AES Invariant Space (folklore)



# AES Invariant Space (folklore)

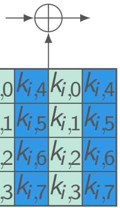


## Modification I

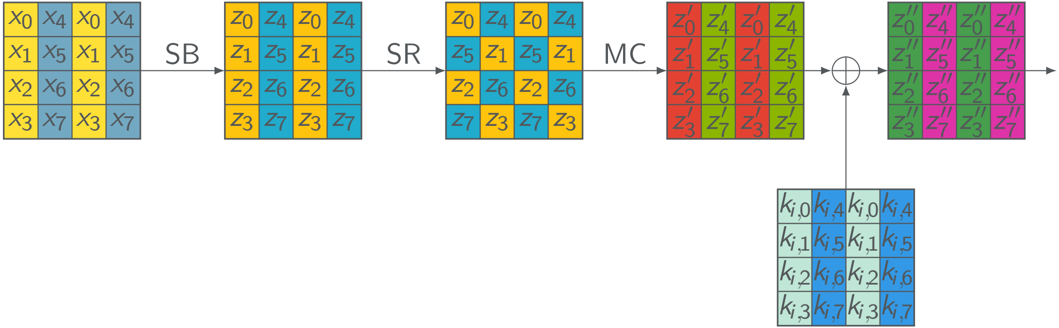


### Modify the Key-Scheduling

Just output symmetric round-keys



# Modification I (Key-Scheduling)

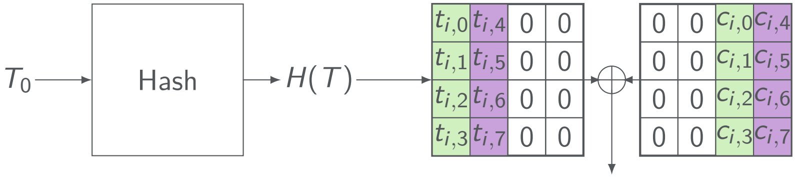


# Modification II: Add a Tweak

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

## Tweak

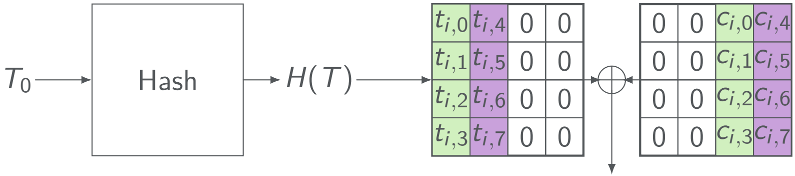
We add a tweak and round-constants.



# Modification II: Add a Tweak

## Tweak

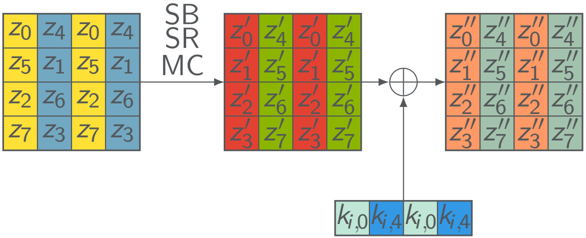
We add a tweak and round-constants.



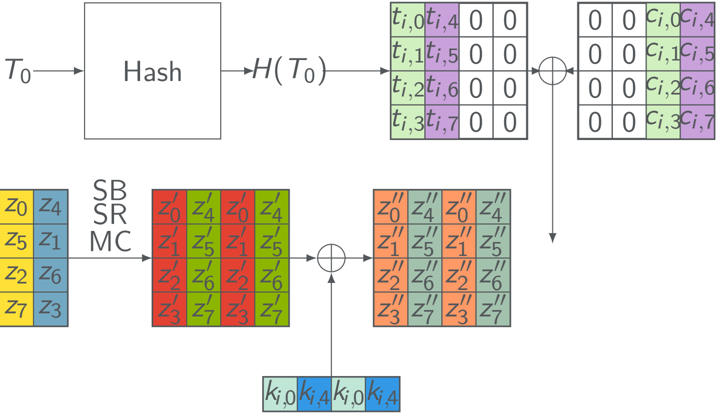

Choose: round constants to make tweak symmetric for $T_0$

# Malicious-AES



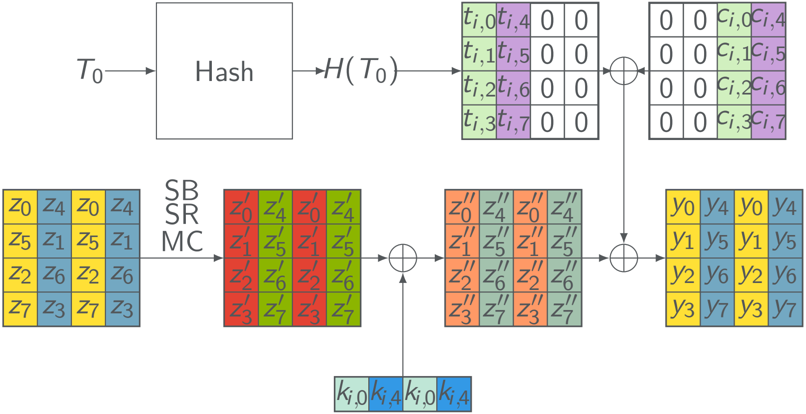



Invariant for any number of rounds!



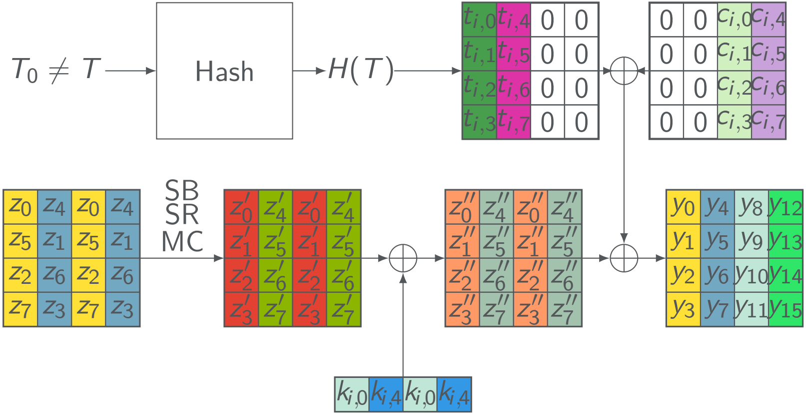

Invariant for any number of rounds!

# Malicious-AES




Invariant for any number of rounds!

# Malicious-AES




Invariant does not work!

# Less Folklore: Boomslang

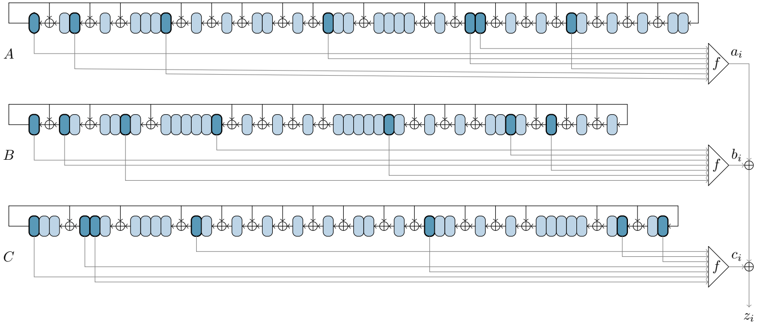
Use nonlinear invariant over two consecutive round functions. Non-trivial to detect.

1. MALICIOUS 2.0
2. GEA-1

# What is GEA-1?

# The Structure of GEA-1 [BDL+21]

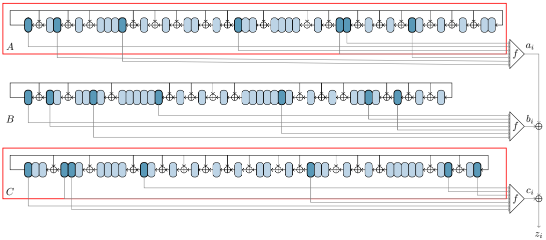
The 64-bit key is (linearly) mapped to a 96-bit internal state



# The Weakness

## Weak Linear Initialization

After the linear initialization process, the joint initial (64-bit) state of registers $A$ and $C$ can only be in a set of $2^{40}$ possible states.



## An Exceptional Property

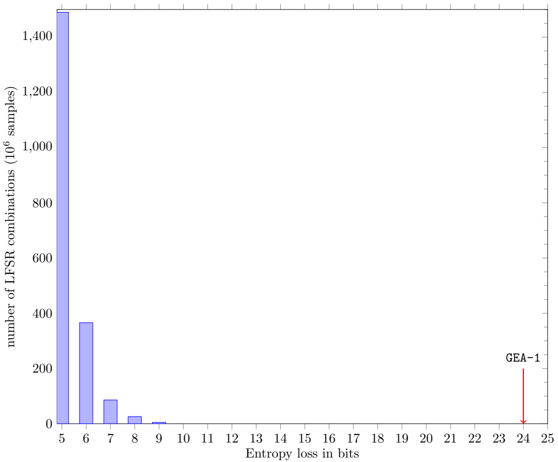
CASA
Cyber Security in the Age of Large-Scale Adversaries

**Question**

Unlucky choice of LFSRs?

- The attack was possible, because the image of the (joint) initialization matrix of two registers has low dimension (here dim 40)
- [BDL+21] checked what happens for two random primitive LFSRs.

# An Exceptional Property



# An Exceptional Property

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

**An intentional weakness**

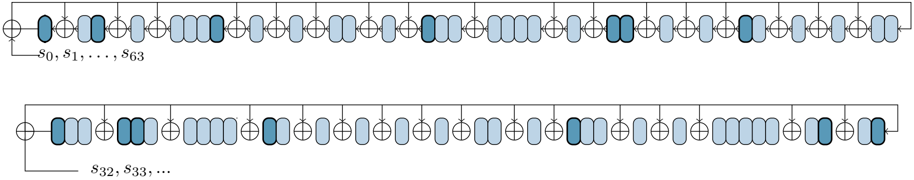
GEA-1 has been weakened on purpose, [BDL+21].

Leads to another question:

**Question**

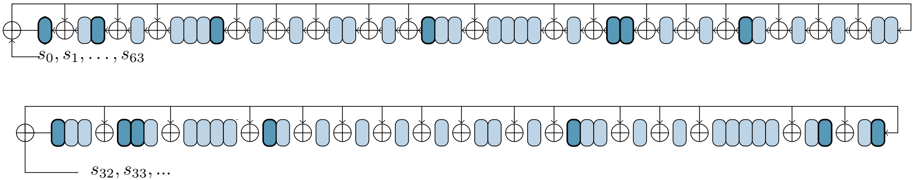
How was this constructed?

# Initialization Details



# Initialization Details

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

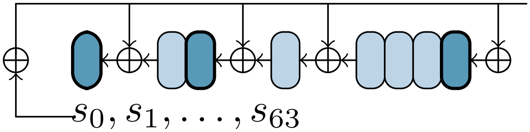



## Small Image ⇔ Large Kernel

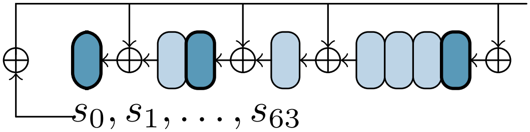
How to choose LFSRs to ensure a large kernel?

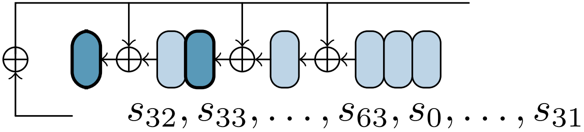
Notation: Feedback-polynomial $g$ and matrix $M_g$
We want large kernel of $s \mapsto (M_{g_a}(s), M_{g_c}(s))$

# Initialization Details: Shift

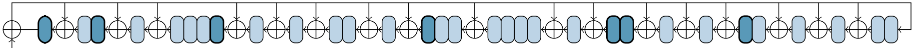


# Initialization Details: Shift



# Rewriting as polynomials



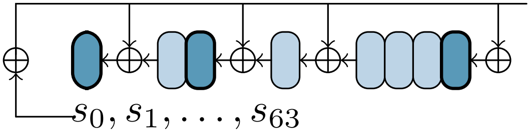

$$(s_0, \ldots, s_{63}) \to p(s) = \sum_i s_i x^i$$

## Link

$$M_g(s) = 0 \Leftrightarrow g | p(s)$$

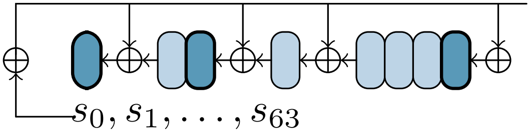
Why? Initialization is just like reducing mod $g$. So $M_g(s) \equiv p(s) \bmod g$

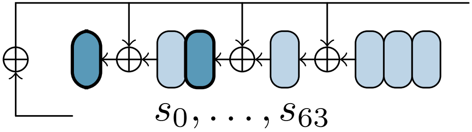
# Initialization Details: Without Shifts



# Initialization Details: Without Shifts

CASA
Cyber Security in the Age of Large-Scale Adversaries



# Without Shifts

CASA
Cyber Security in the Age of Large-Scale Adversaries

**Remember: Link**

$M_g(s) = 0 \Leftrightarrow g | p(s)$

$$M_{g_a}(s) = 0 \text{ and } M_{g_c}(s) = 0$$
$$\Leftrightarrow$$
$$g_a | p(s) \text{ and } g_c | p(s).$$
$$\Leftrightarrow$$
$$g_a \cdot g_c | p(s)$$
$$\Leftrightarrow$$
$$p(s) = 0$$

# Without Shifts

**Remember: Link**

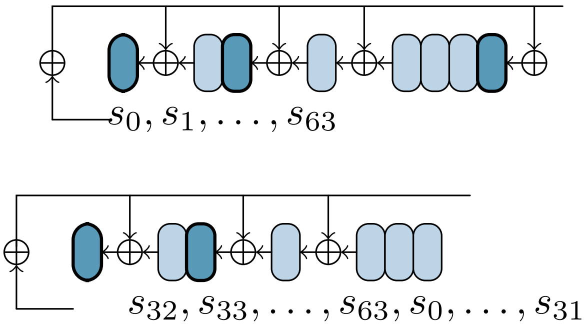
$M_g(s) = 0 \Leftrightarrow g|p(s)$

$$M_{g_a}(s) = 0 \text{ and } M_{g_c}(s) = 0$$
$$\Leftrightarrow$$
$$g_a|p(s) \text{ and } g_c|p(s).$$
$$\Leftrightarrow$$
$$g_a \cdot g_c|p(s)$$
$$\Leftrightarrow$$
$$p(s) = 0$$

Joint kernel is trivial!

## Initialization Details: Shift

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



## With Shifting

### Shifting

$p \to x^{32} p \bmod (x^{64} + 1)$

$$M_{g_a}(s) = 0 \text{ and } M_{g_c}(s >>> 32) = 0$$

$$\Leftrightarrow$$

$$g_a | p(s) \text{ and } g_c | x^{32} p(s) \bmod (x^{64} + 1).$$

# With Shifting

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

### Shifting

$p \to x^{32} p \bmod (x^{64} + 1)$

$$M_{g_a}(s) = 0 \text{ and } M_{g_c}(s >>> 32) = 0$$

$$\Leftrightarrow$$

$$g_a | p(s) \text{ and } g_c | x^{32} p(s) \bmod (x^{64} + 1).$$

### Small Change with Big Effect

Shift enables non-trivial kernel.

# With Shifting

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

**Turn Construction Around**

Given $p(s)$ construct $g_a$ and $g_b$!

## With Shifting

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

### Turn Construction Around

Given $p(s)$ construct $g_a$ and $g_b$!

1. Factorize $p(s)$ (resp. $x^{32}p(s) \bmod (x^{64}+1)$)
2. Hope for primitive factor of degree 33 (resp. 31)

Not too unlikely:

$$\left(\frac{\phi(2^{31}-1)}{31\cdot 2^{31}}\right)\left(\frac{\phi(2^{33}-1)}{33\cdot 2^{33}}\right) \approx \frac{1}{1250}$$

# Final Twist

CASA
Cyber Security in the Age of Large-Scale Adversaries

One element is not enough. We want many!

**Special choice for $p$**

One that implies many.

## GEA-1 Construction?

Procedure works!

- Efficient, even in the 90s.
- Kernel of GEA-1 is of this form.
- Could be weakened below 40 bits
- But not too much
- See paper for details

# GEA-1 Construction?

Procedure works!

- Efficient, even in the 90s.
- Kernel of GEA-1 is of this form.
- Could be weakened below 40 bits
- But not too much
- See paper for details

Thank you very much for your attention!

Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes.
Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2.
In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 155–183. Springer, 2021.

Thomas Peyrin and Haoyang Wang.
The MALICIOUS framework: Embedding backdoors into tweakable block ciphers.
In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 249–278. Springer, 2020.