CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

HAWKEYE

Recovering Symmetric Cryptography from Hardware Circuits

Gregor Leander[1], Christof Paar[2], **Julian Speith[2]**, Lukas Stennes[1]
[1] *Ruhr University Bochum (RUB)*
[2] *Max Planck Institute for Security and Privacy (MPI-SP)*

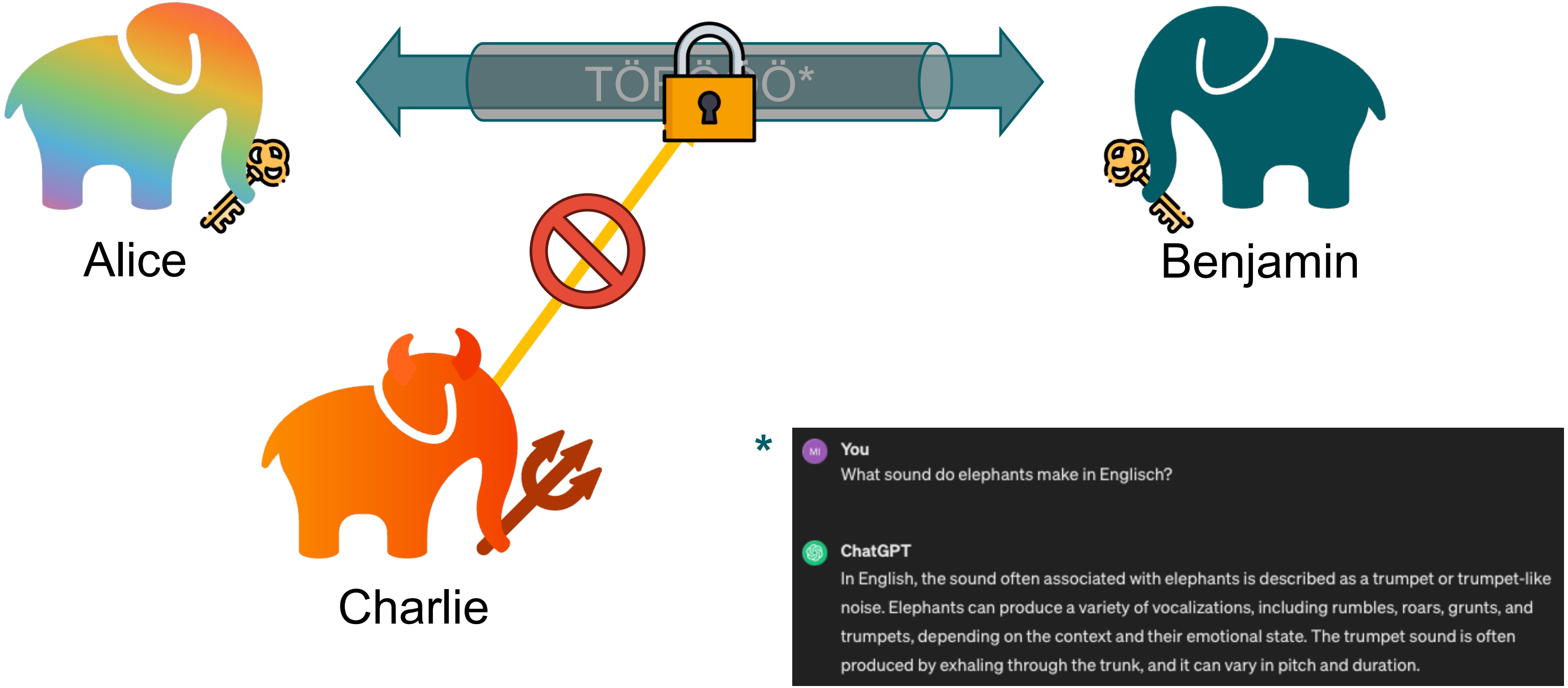
RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

HORST GÖRTZ INSTITUT

SYMMETRIC CRYPTOGRAPHY

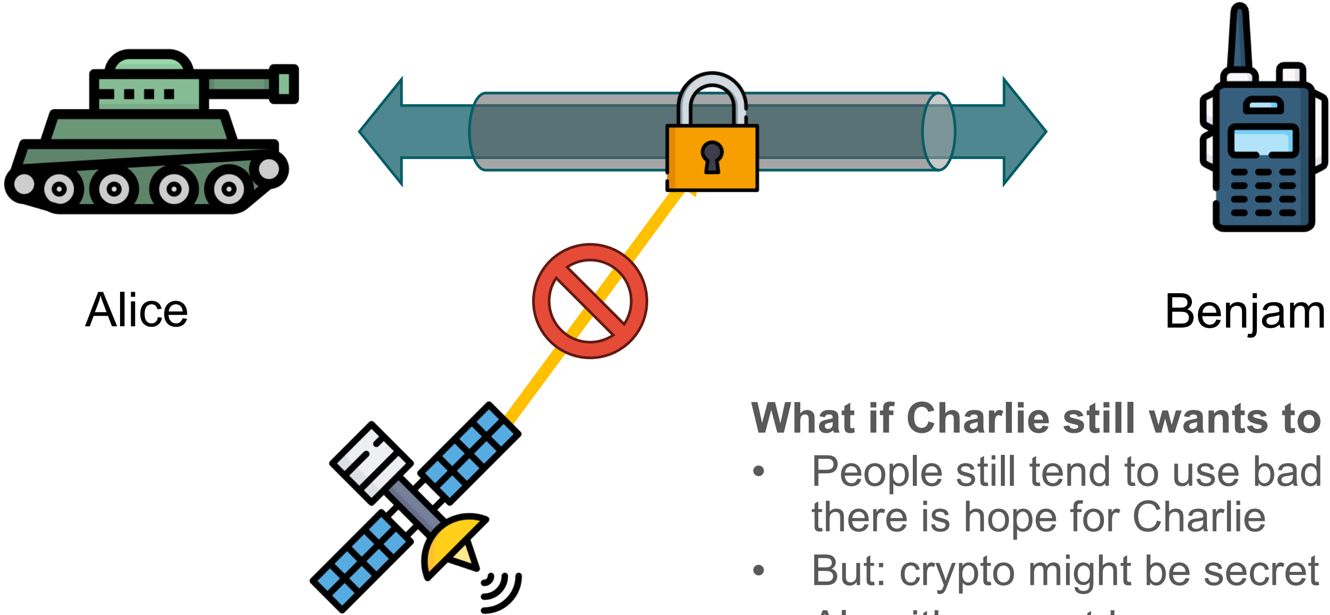


*

You
What sound do elephants make in Englisch?

ChatGPT
In English, the sound often associated with elephants is described as a trumpet or trumpet-like noise. Elephants can produce a variety of vocalizations, including rumbles, roars, grunts, and trumpets, depending on the context and their emotional state. The trumpet sound is often produced by exhaling through the trunk, and it can vary in pitch and duration.

PRACTICAL APPLICATION



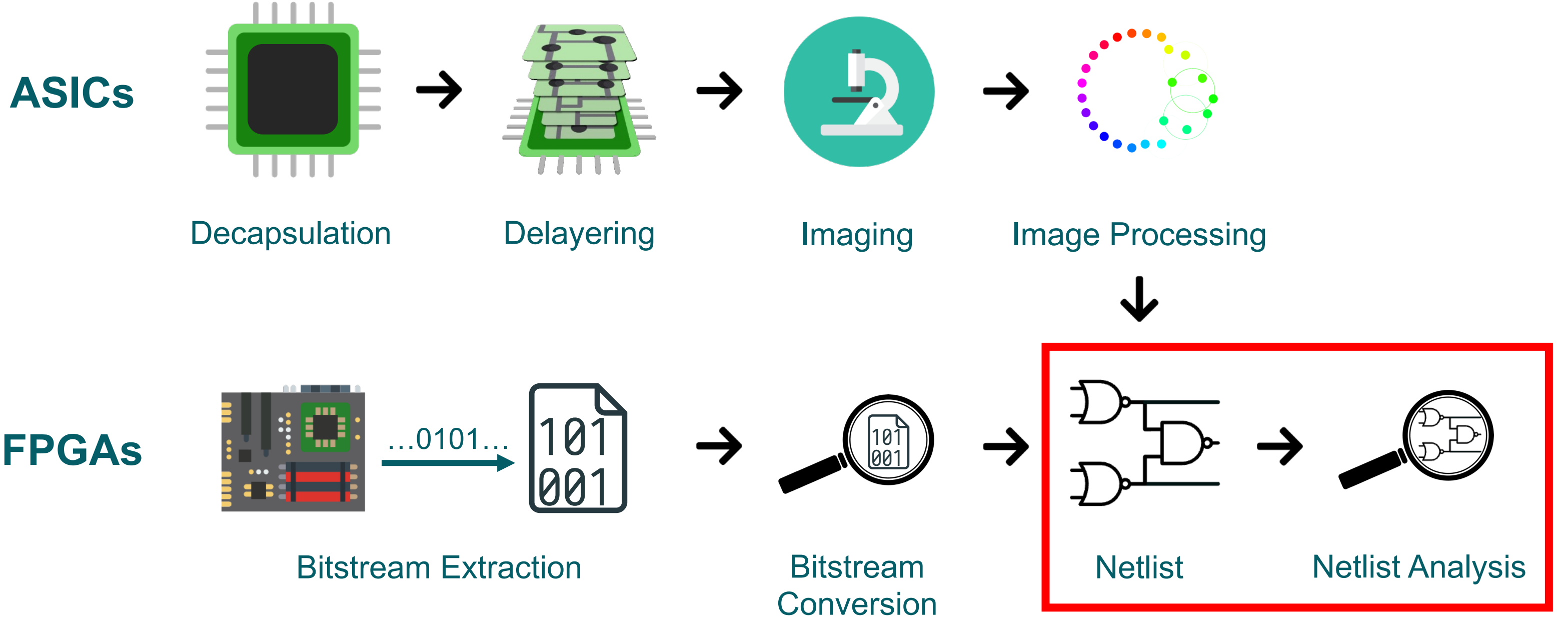
What if Charlie still wants to listen in?

- People still tend to use bad crypto, so there is hope for Charlie
- But: crypto might be secret
- Algorithm must be recovered for subsequent analysis
- But how?

HOW TO FIND (B

- Documents **easy / be**
  - Academic papers, sta
  - Not always available
- Reverse Engineering
  - Software **Where’s** **ENIX’21**
  - Hardware **???**

HRE OVERVIEW



ASICs

Decapsulation → Delayering → Imaging → Image Processing

↓

FPGAs

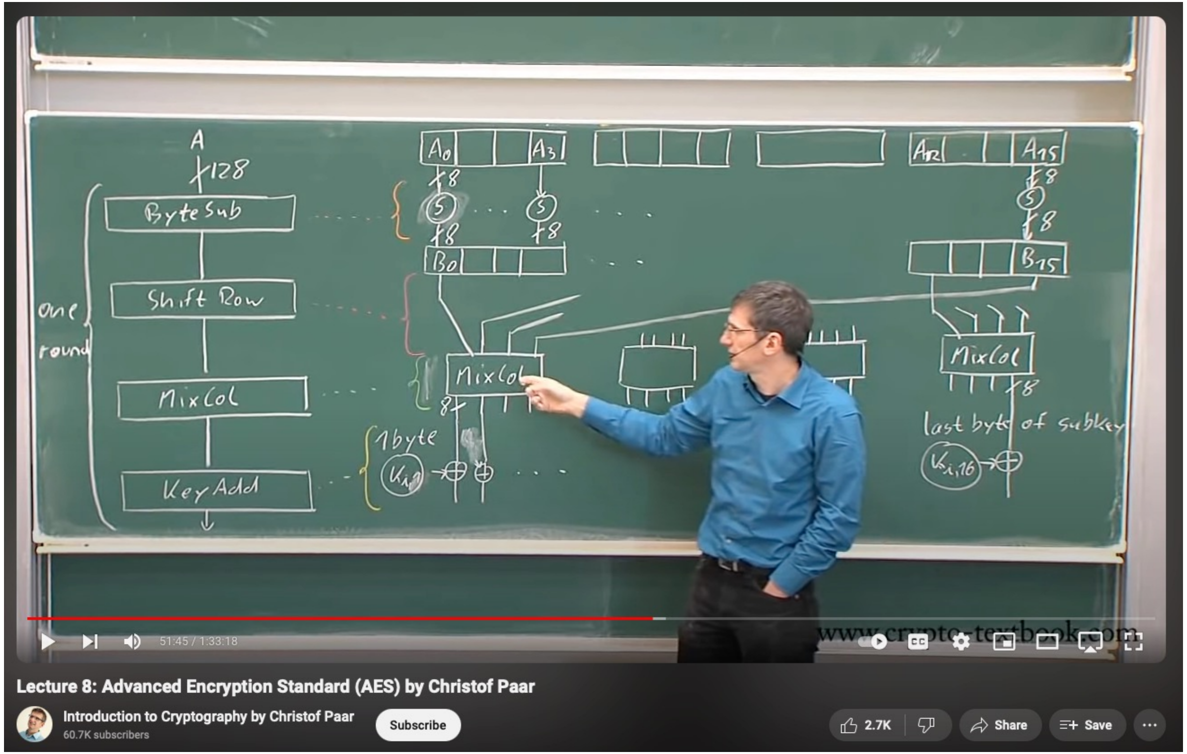
Bitstream Extraction → Bitstream Conversion → Netlist → Netlist Analysis

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Cryptography in Hardware

How does it look like and what makes it special

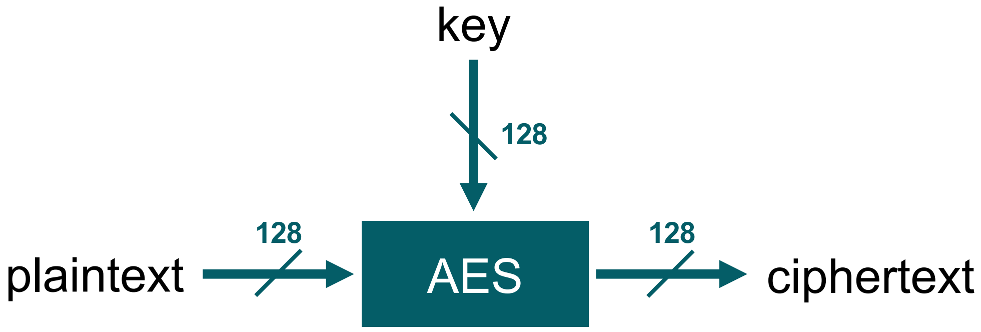
AES



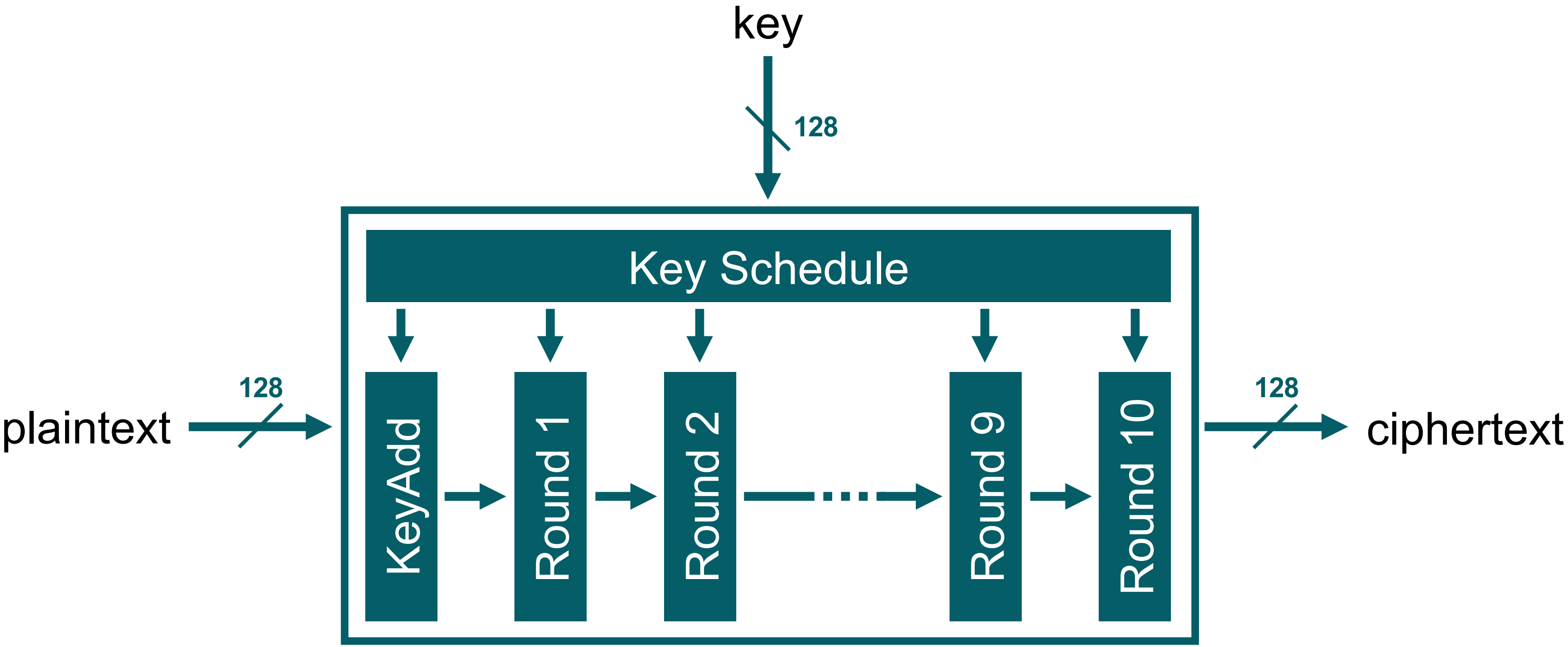
Lecture 8: Advanced Encryption Standard (AES) by Christof Paar

Introduction to Cryptography by Christof Paar
60.7K subscribers

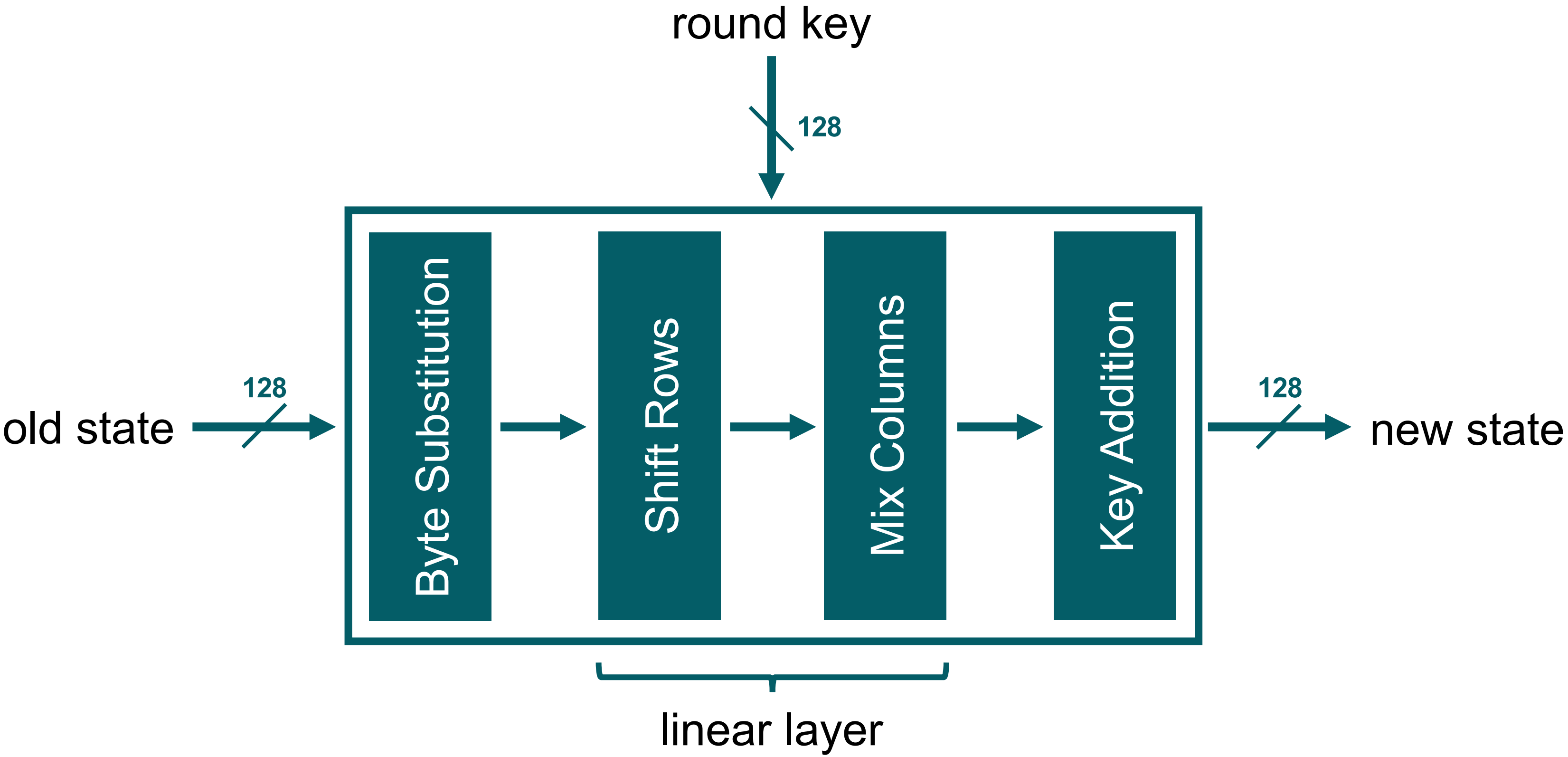
AES



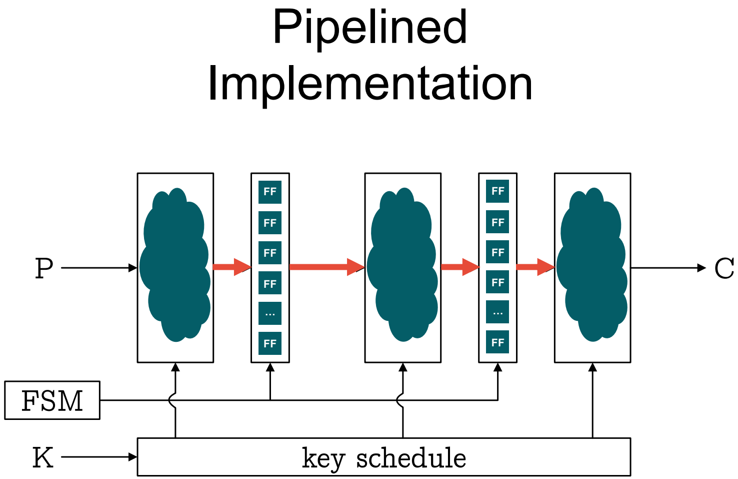
AES

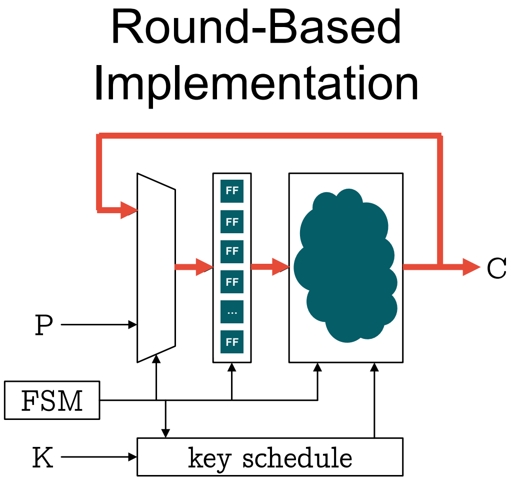

key
128
Key Schedule
plaintext
128
KeyAdd
Round 1
Round 2
Round 9
Round 10
128
ciphertext

AES


round key
128
old state
128
Byte Substitution
Shift Rows
Mix Columns
Key Addition
128
new state
linear layer

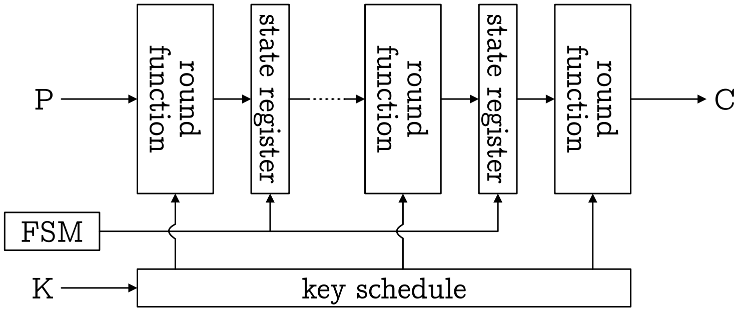
SYMMETRIC CRYPTOGRAPHY IN HARDWARE

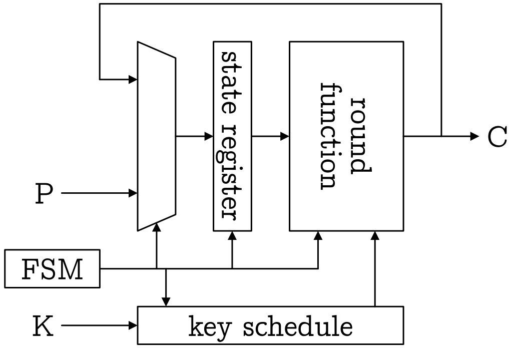




WHAT MAKES SYMMETRIC CRYPTO SPECIAL?

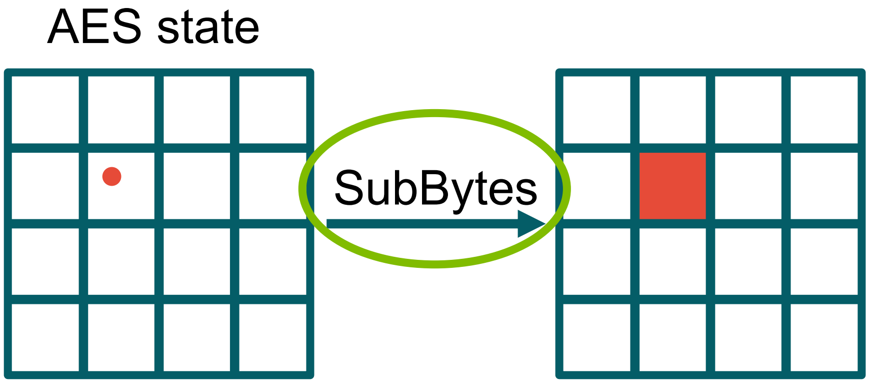
1. FFs in state register influence only state register and ciphertext output
2. State register FFs and ciphertext FFs are distinguishable (believe me)
3. Round function only depends on plaintext, round keys, and FSM control signals





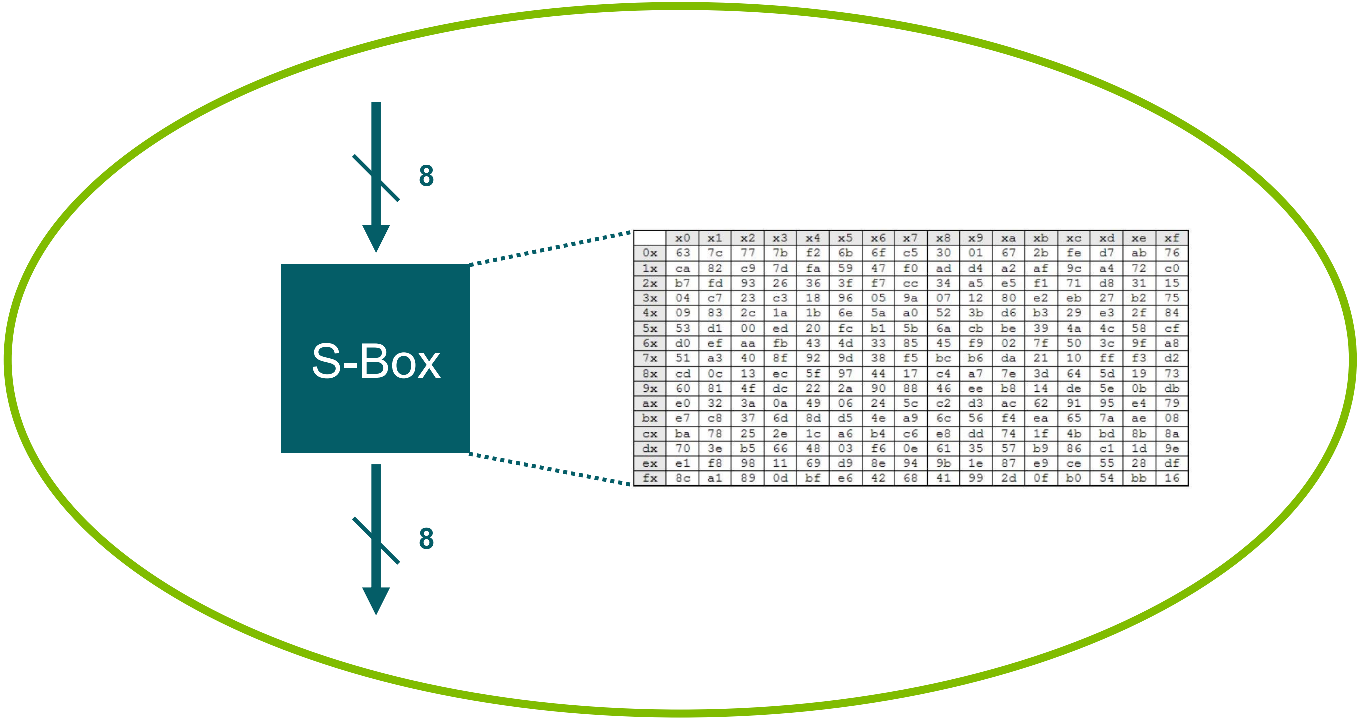
AES

! KeyAdd is omitted



☐ = 1 byte

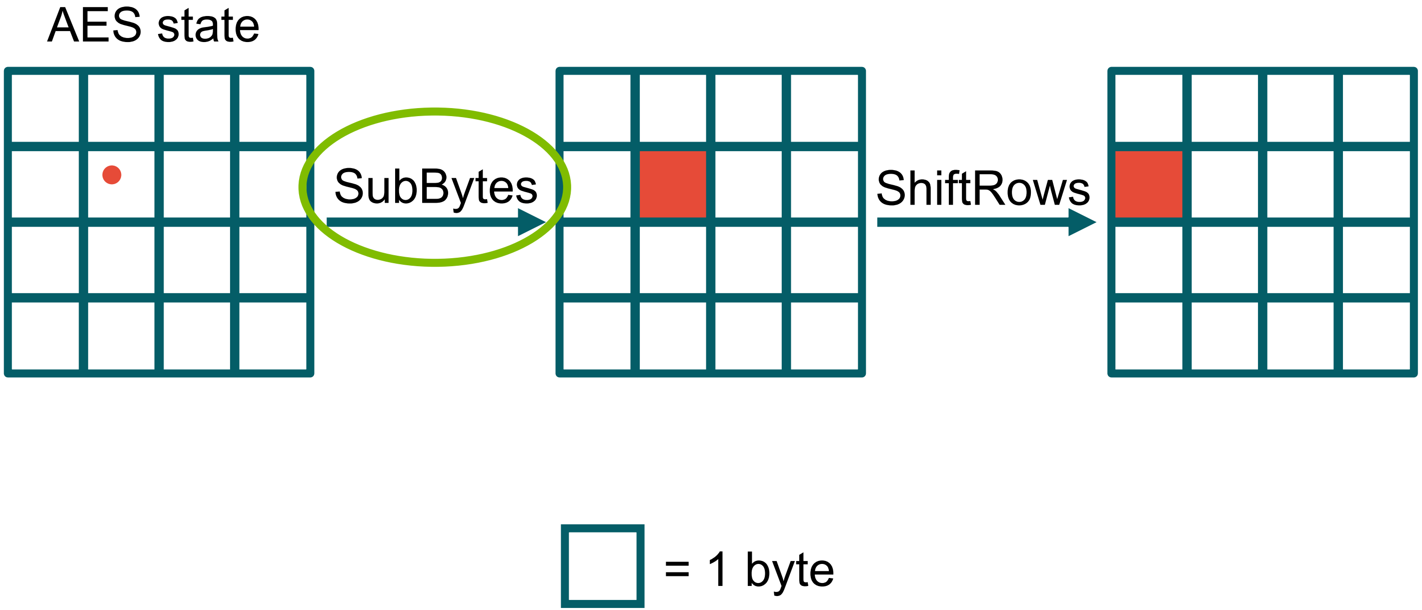
AES



	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES

KeyAdd is omitted



AES state

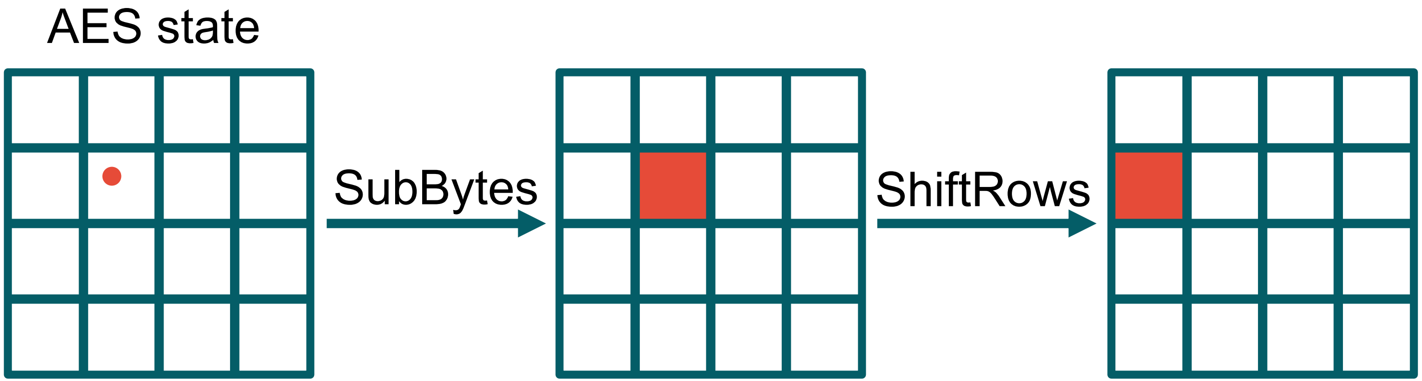
SubBytes

ShiftRows

= 1 byte

AES

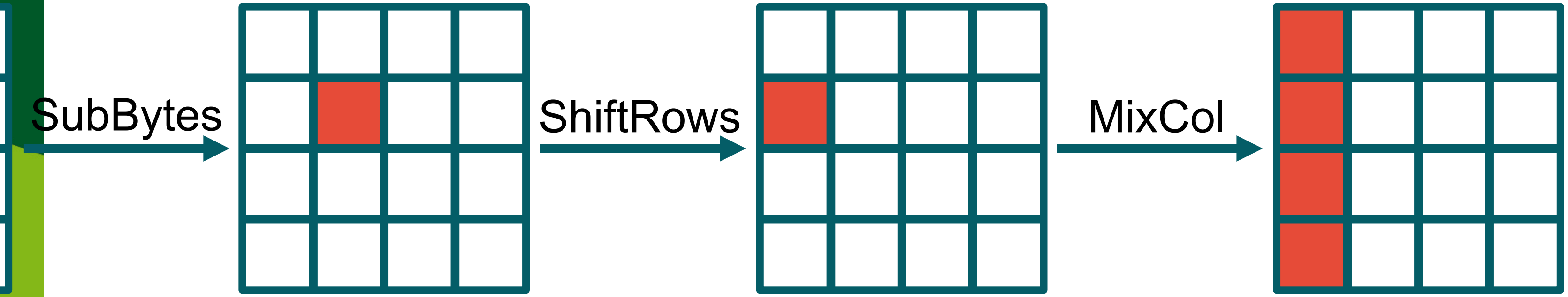
! KeyAdd is omitted



☐ = 1 byte

AES

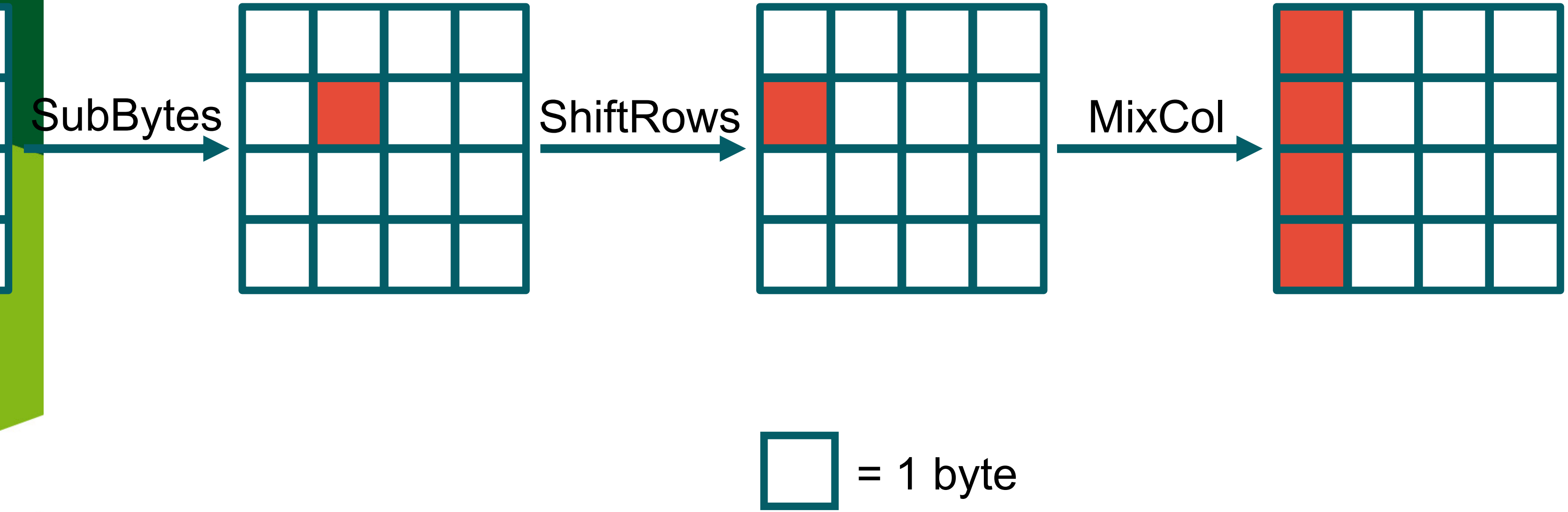
! KeyAdd is omitted



☐ = 1 byte

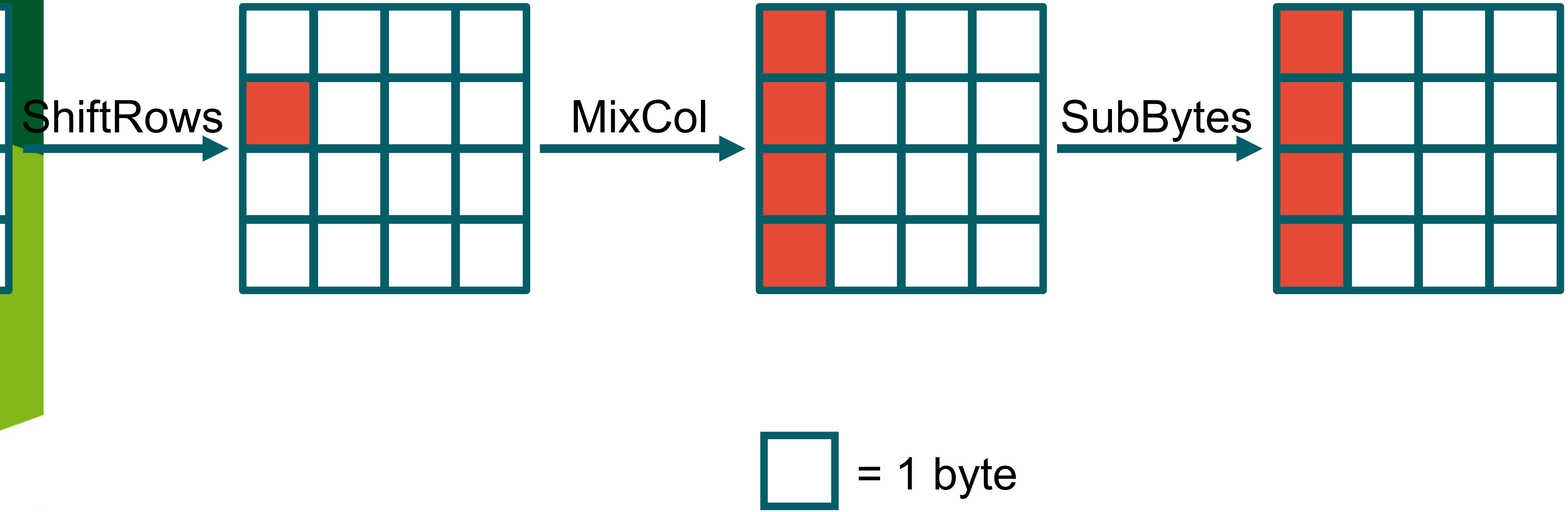
AES

! KeyAdd is omitted



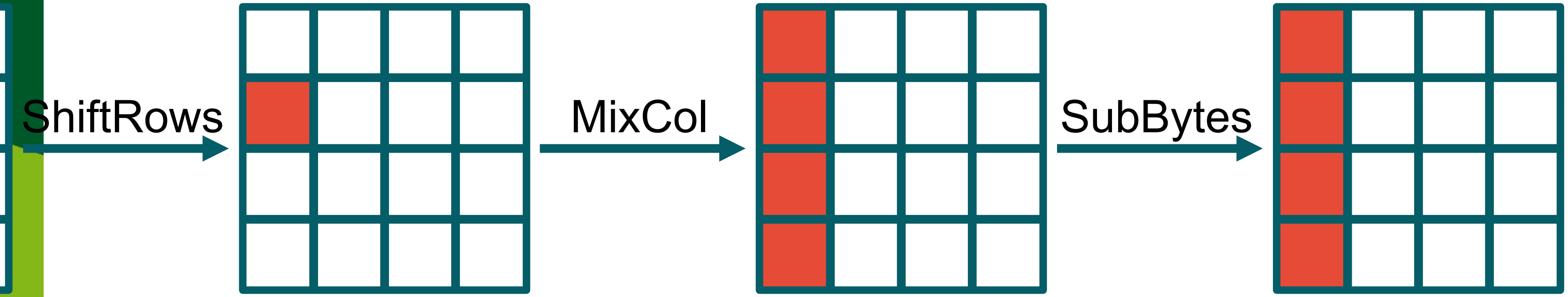
AES

! KeyAdd is omitted



AES

! KeyAdd is omitted

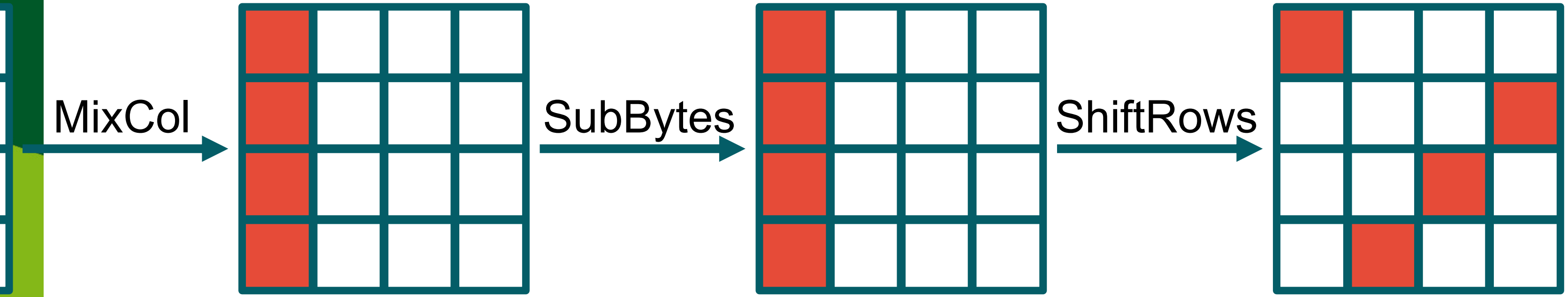


ShiftRows → MixCol → SubBytes

☐ = 1 byte

AES

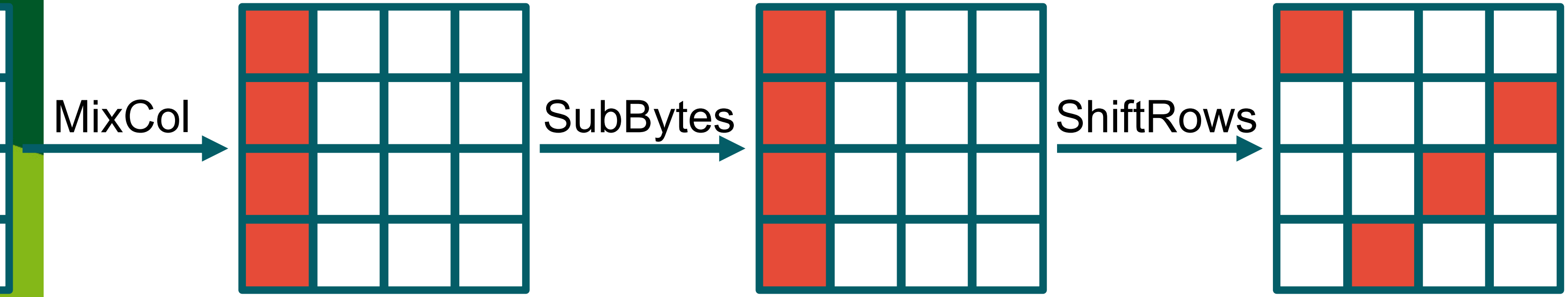
! KeyAdd is omitted



☐ = 1 byte

AES

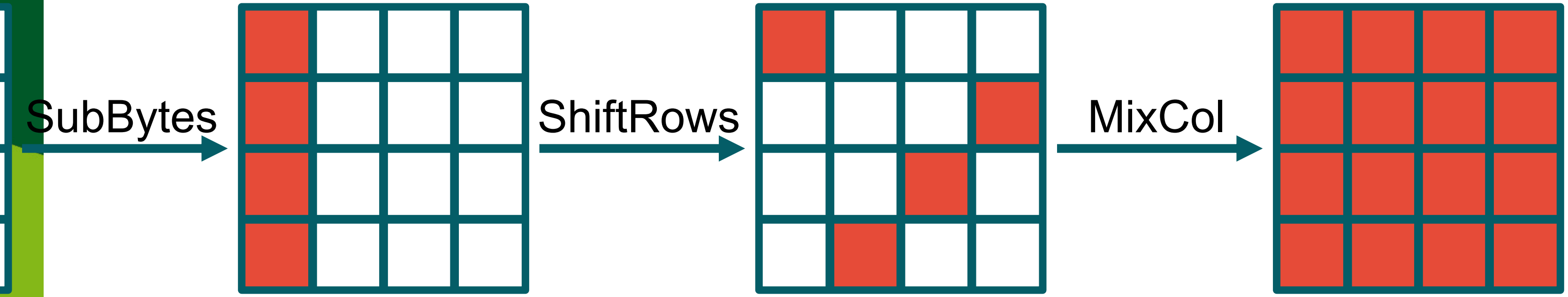
KeyAdd is omitted



☐ = 1 byte

AES

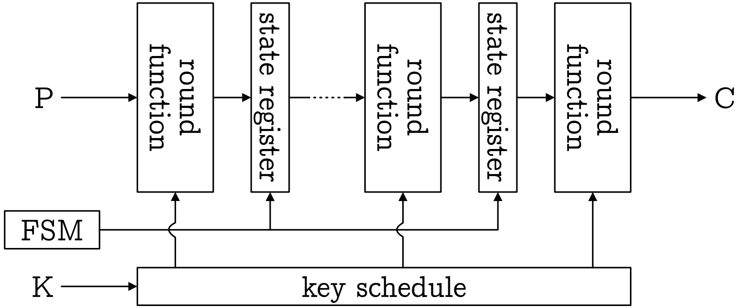
KeyAdd is omitted

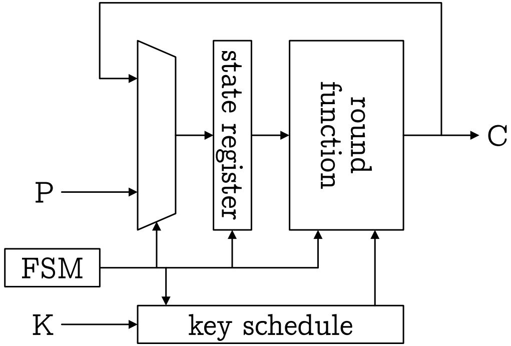


☐ = 1 byte

WHAT MAKES SYMMETRIC CRYPTO SPECIAL?

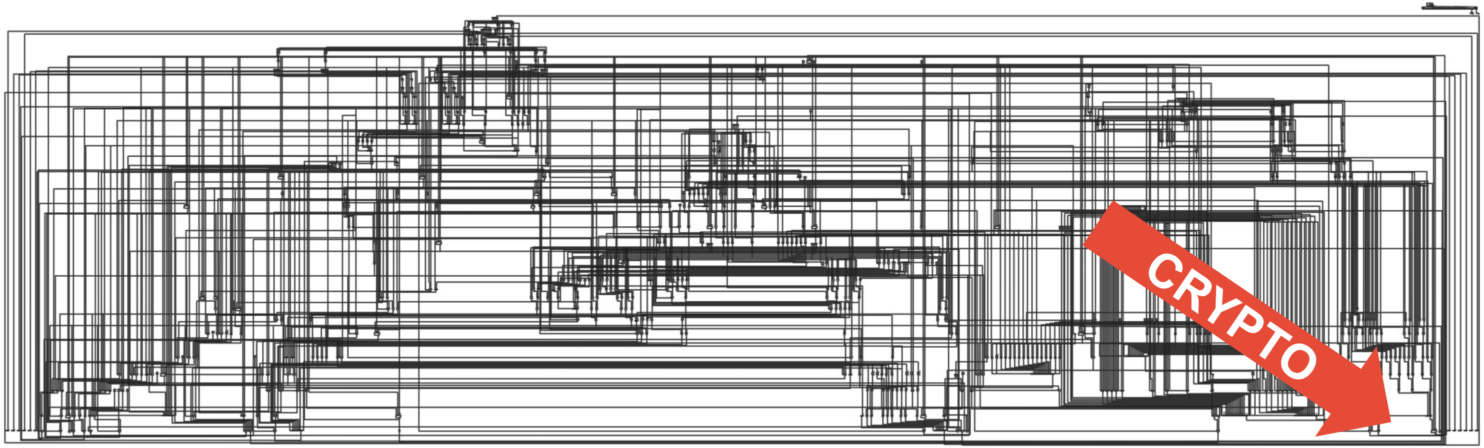
1. FFs in state register influence only state register and ciphertext output
2. State register FFs and ciphertext FFs are distinguishable (believe me)
3. Round function only depends on plaintext, round keys, and FSM control signals
4. Avalanche effect: Bits in first state register influences all bits of later state registers





HAWKEYE: A MULTI-STAGE APPROACH

1. **Structural Candidate Search**
    - We face a potentially huge netlist, only a small piece of it being the crypto implementation
    - Candidate search needs to be freaking fast, so ideally we use only structural properties
    - Relying on known graph algorithms provides significant speed-up



HAWKEYE: A MULTI-STAGE APPROACH

1. **Structural Candidate Search**
    - We face a potentially huge netlist, only a small piece of it being the crypto implementation
    - Candidate search needs to be freaking fast, so ideally we use only structural properties
    - Relying on known graph algorithms provides significant speed-up

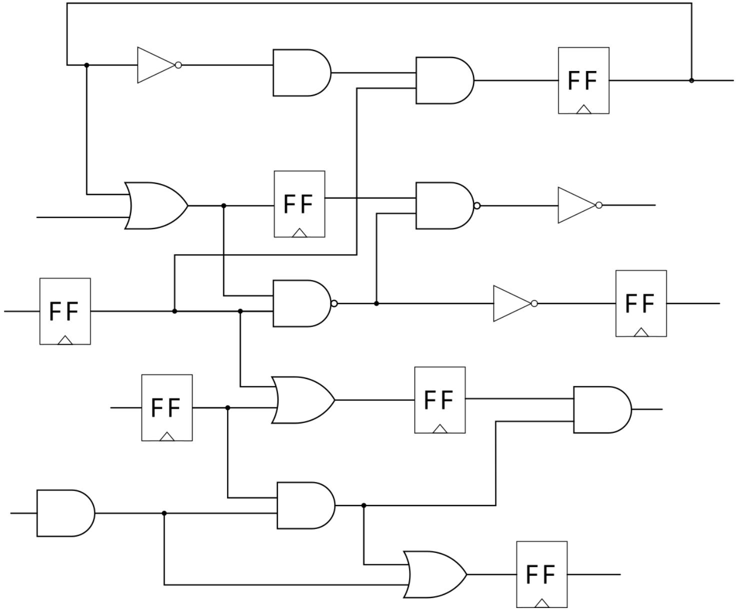
2. **Functional Candidate Analysis**
    - Having found a few rather small candidates, we can switch to functional analysis
    - Goal: extract and analyze the round function by looking at Boolean functions (expensive)
    - If possible: identify cryptographic algorithm by matching against known ciphers

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

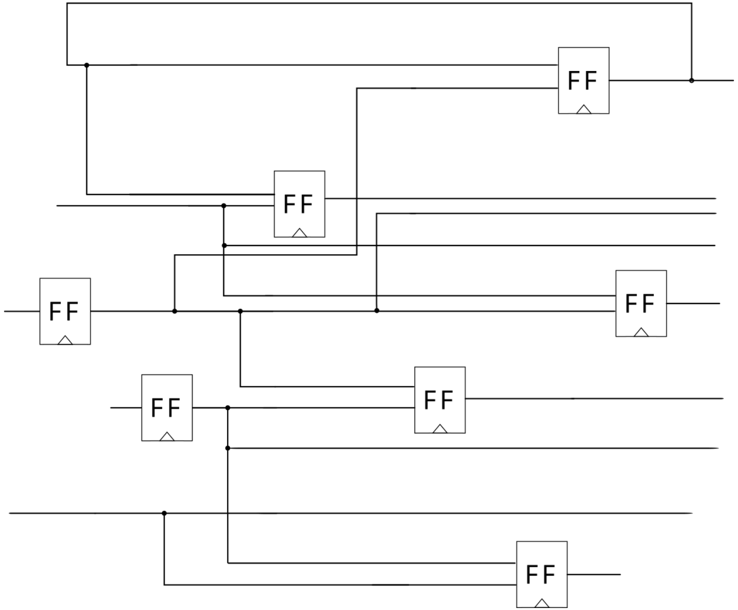
Structural Candidate Search

Using graph algorithms to find cryptographic implementations

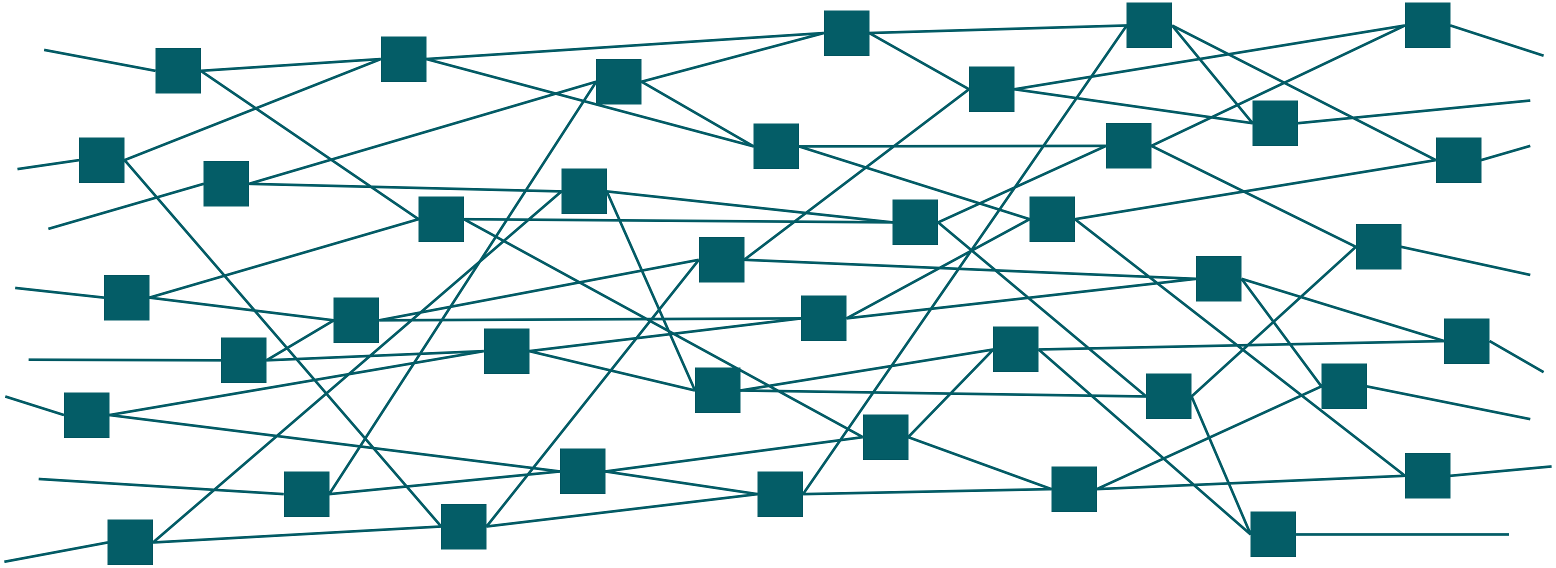
PREPROCESSING



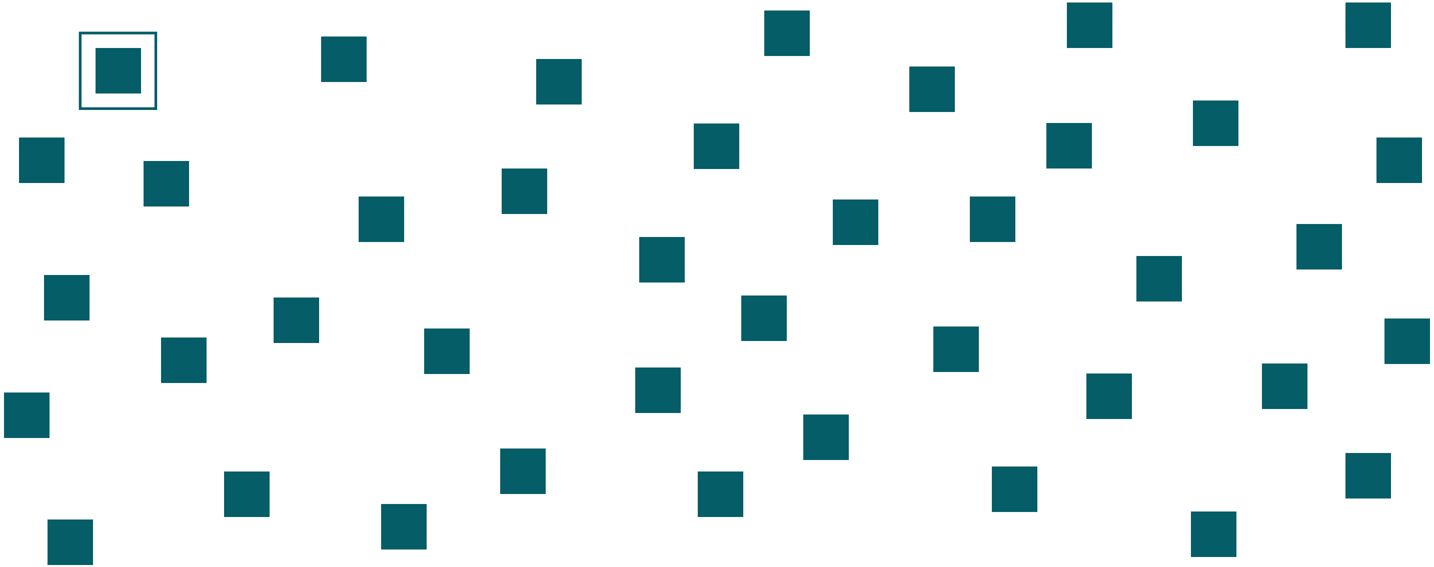
PREPROCESSING



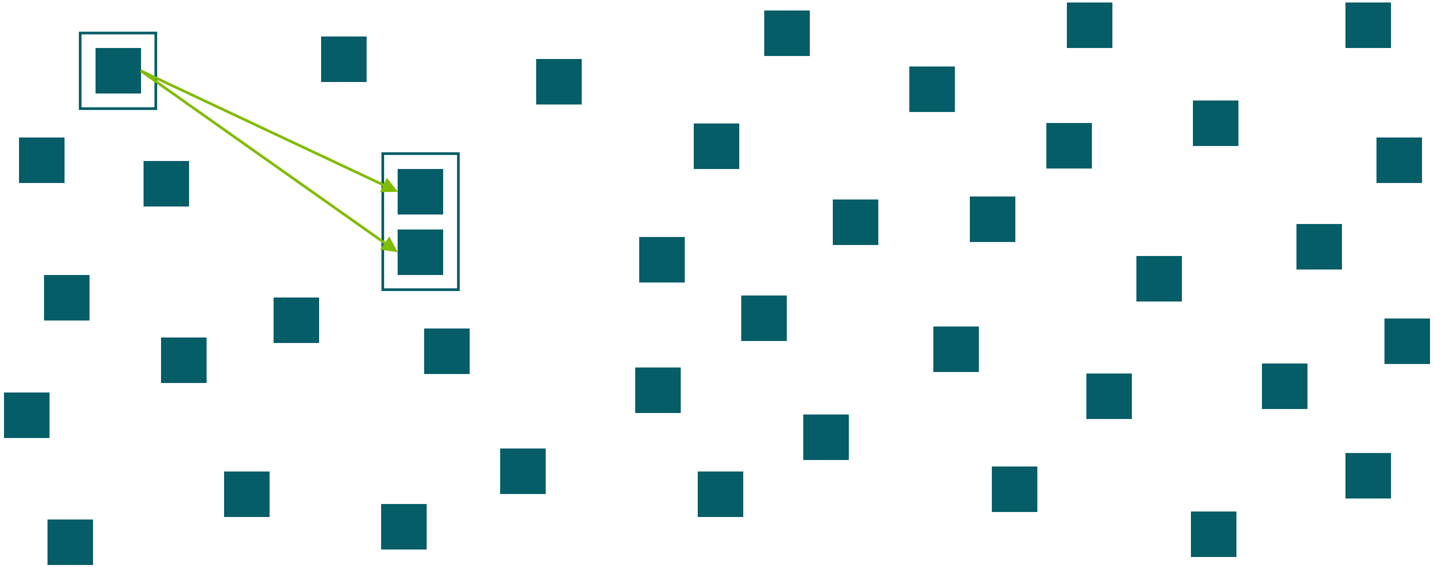
CANDIDATE SEARCH



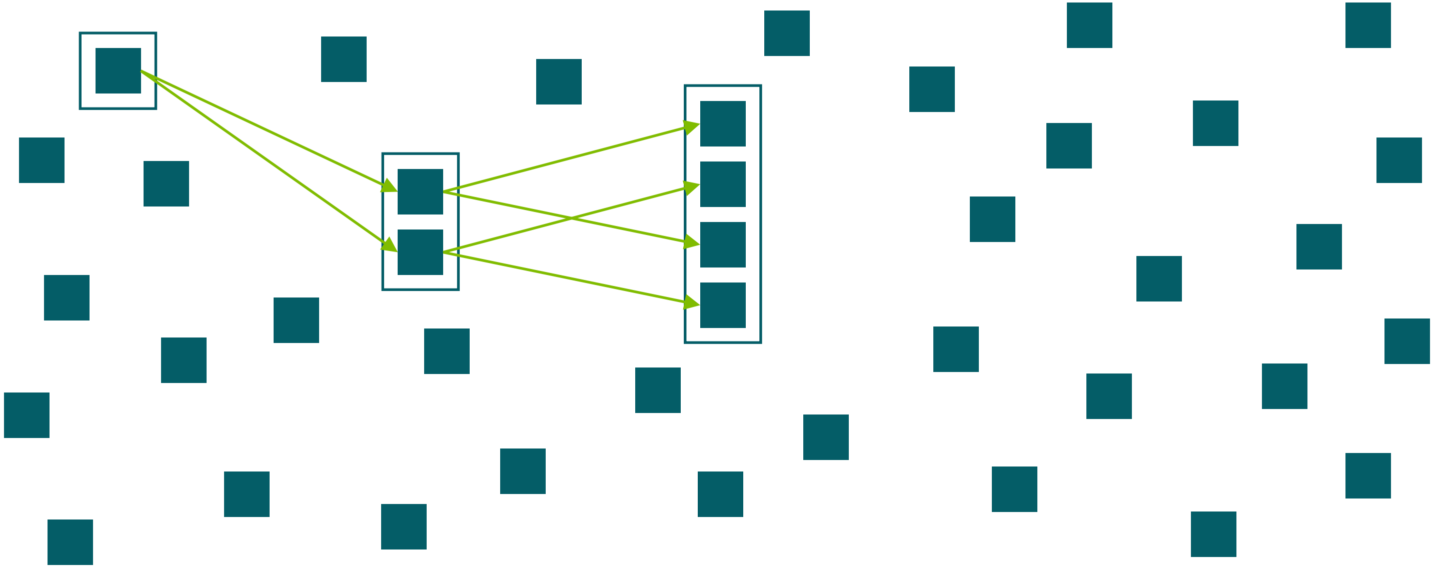
CANDIDATE SEARCH



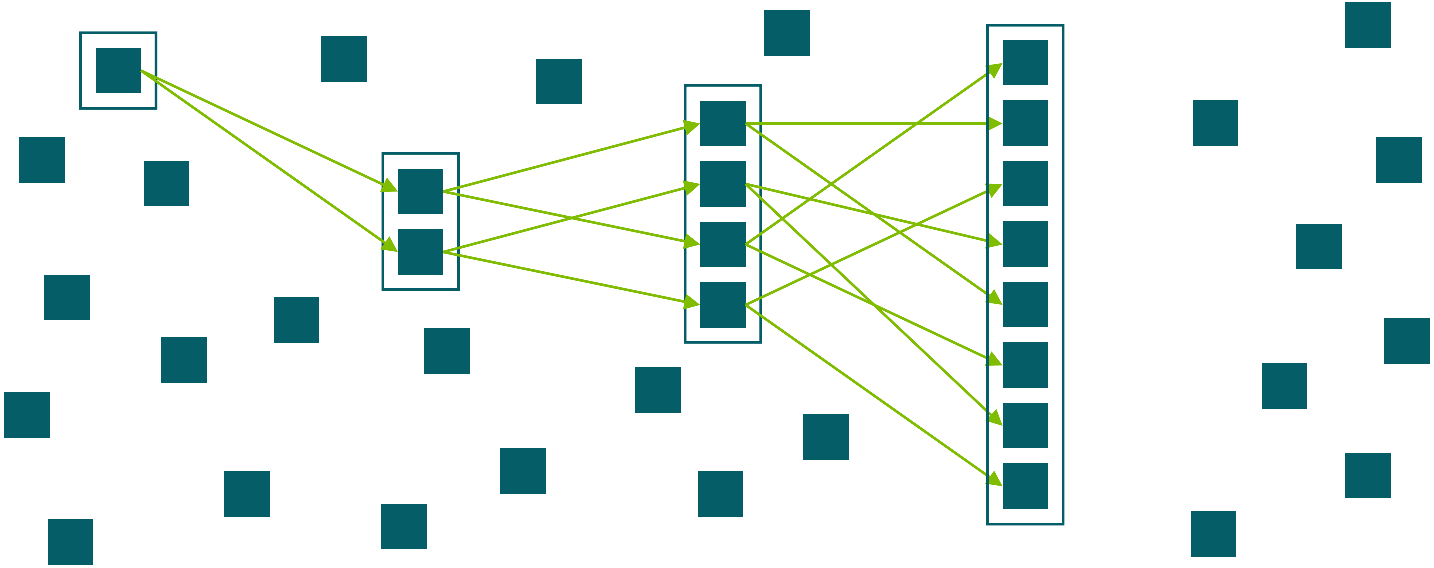
CANDIDATE SEARCH



CANDIDATE SEARCH

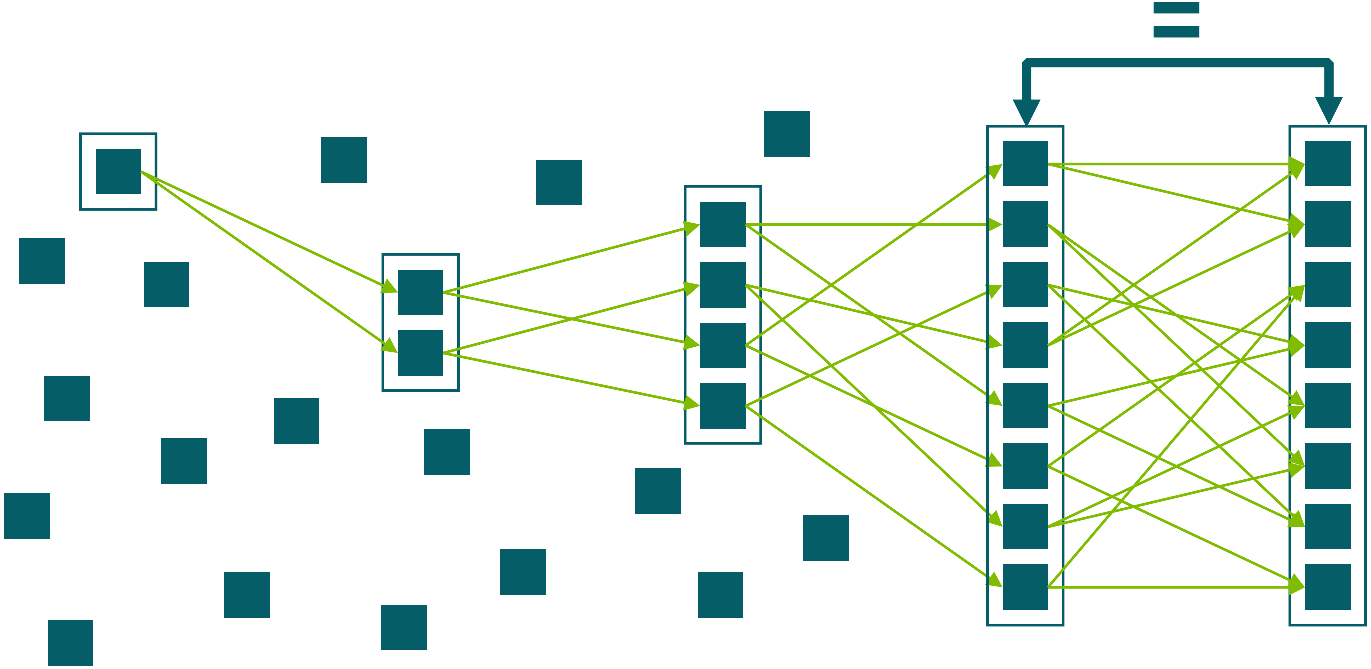


CANDIDATE SEARCH

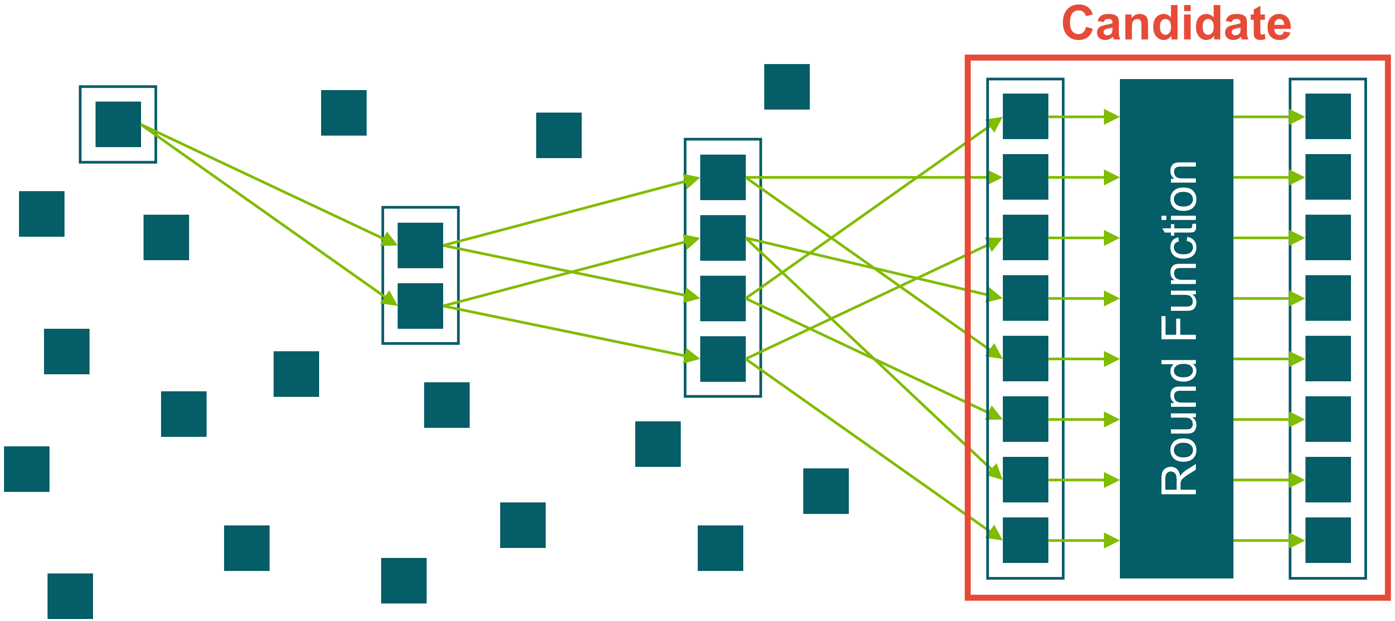


CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

CANDIDATE SEARCH



CANDIDATE SEARCH

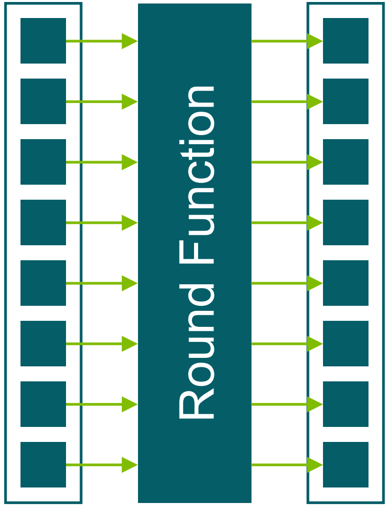


CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

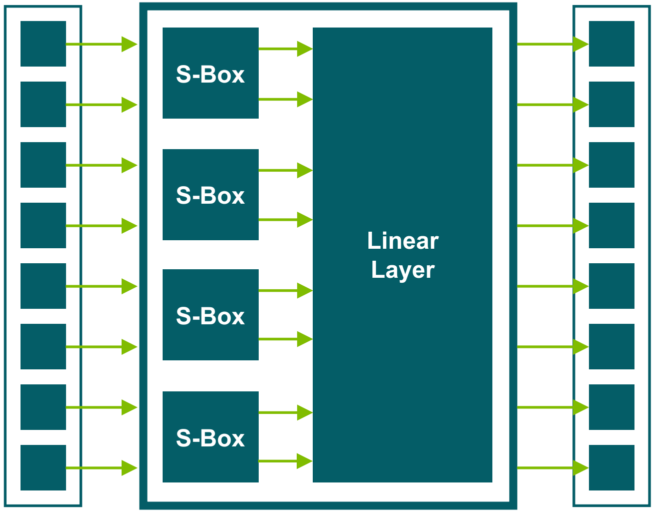
Functional Candidate Analysis

Using functional methods to dissect and identify the round function

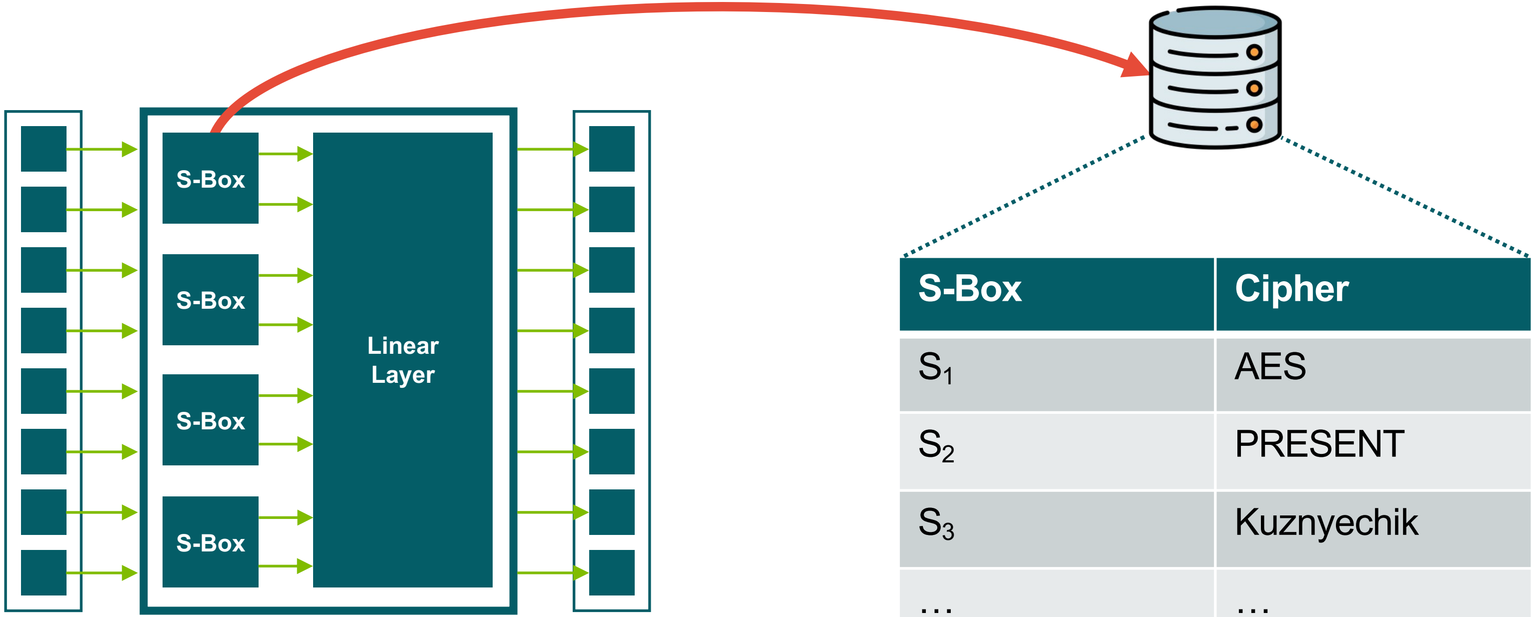
ROUND FUNCTION ANALYSIS



ROUND FUNCTION ANALYSIS



ROUND FUNCTION ANALYSIS



S-Box	Cipher
S_1	AES
S_2	PRESENT
S_3	Kuznyechik
…	…

CASA

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Evaluation

Finding out how well it works

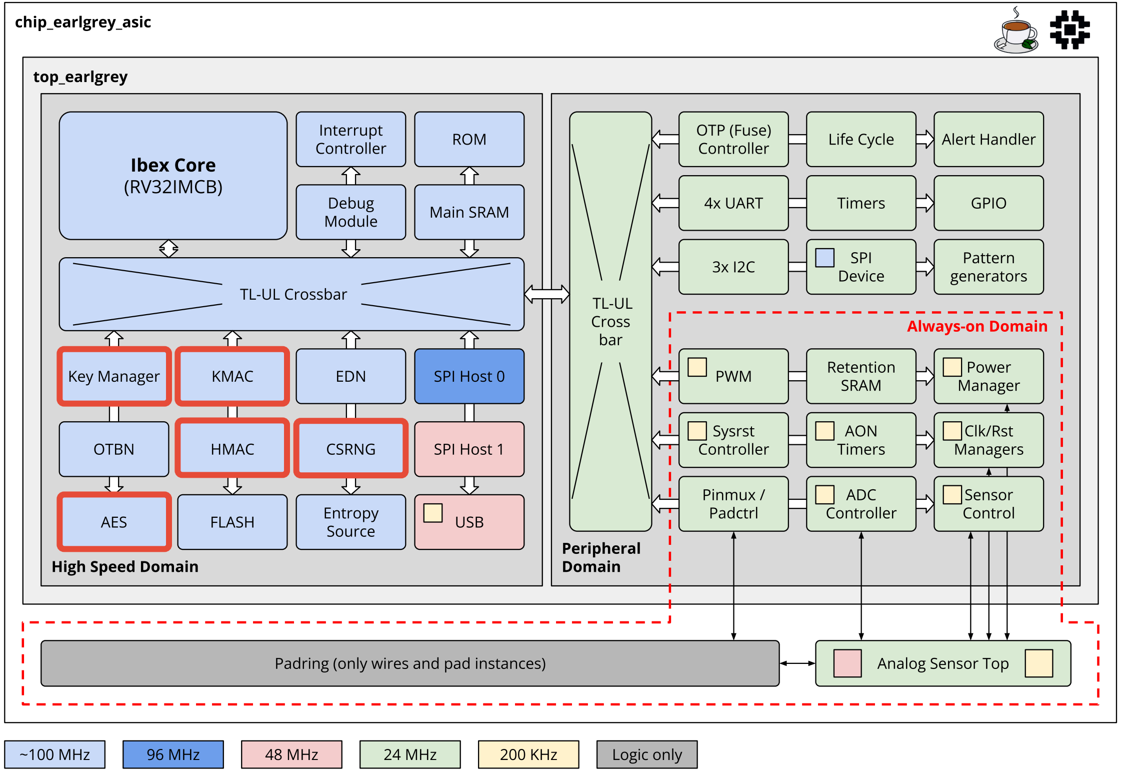
EVALUATION

- Our techniques are based on **heuristics**
- Imperative to **evaluate** the techniques

- Actual hardware reverse engineering is **not an option** (ASIC/FPGA → netlist)
- **Instead:** synthesize open-source hardware designs (hardware design → netlist)
    - OpenTitan: industry-grade security chip
    - Cryptographic accelerators in a small system-on-chip
    - Isolated (non-)cryptographic benchmarks

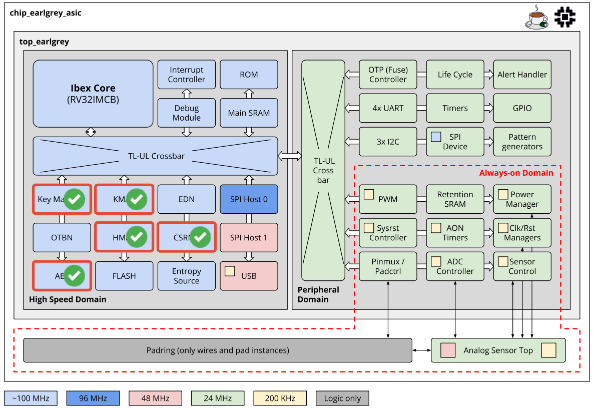
- Implementation is available as artifact as part of our open-source netlist reverse engineering framework **HAL**

OPENTITAN



chip_earlgrey_asic
top_earlgrey
Ibex Core
(RV32IMCB)
Interrupt Controller
ROM
Debug Module
Main SRAM
TL-UL Crossbar
Key Manager
KMAC
EDN
SPI Host 0
OTBN
HMAC
CSRNG
SPI Host 1
AES
FLASH
Entropy Source
USB
High Speed Domain
TL-UL Cross bar
OTP (Fuse) Controller
Life Cycle
Alert Handler
4x UART
Timers
GPIO
3x I2C
SPI Device
Pattern generators
Always-on Domain
PWM
Retention SRAM
Power Manager
Sysrst Controller
AON Timers
Clk/Rst Managers
Pinmux / Padctrl
ADC Controller
Sensor Control
Peripheral Domain
Padring (only wires and pad instances)
Analog Sensor Top
~100 MHz
96 MHz
48 MHz
24 MHz
200 KHz
Logic only

OPENTITAN



Contains 424.341 gates

After 44 seconds on Apple M2:

No.	#FFs	Crypto?	Description
1	640	✓	partial Keccak state
2	128	✓	AES state
3	256	✓	AES round key
4	256	✓	SHA-2 state
5	256	✓	Xoshiro256++ state
6	192	✓	PRESENT state and key
7	64	✓	PRINCE output
8	64	✓	LFSR of PRNG within analog sensors
9	64	✓	key manager clearing PRNG
10	64	✓	AES clearing PRNG
11	40	✓	LFSR of PRNG in memory controller
12	40	✓	LFSR of PRNG in memory controller

KNOWN CIPHERS

Name
3DES
AES-128$_r$
AES-128$_p$
ASCON
CRAFT
DES
GIFT
LED-64
LED-128
Magma
Midori
Piccolo
PRESENT-80
PRESENT-128
SHA-256
SHA-3
SIMON-128
SKINNY-64

- Finds almost all ciphers in FPGA and ASIC netlists
- Runtime is in the seconds
- Even finds some ciphers that we did not expect it to find
- Only very few false positives

CONCLUSION & FUTURE WORK

Recap:

- HAWKEYE is optimized for SPN, ARX, and Feistel ciphers
- It reliably locates all kinds of ciphers, even in a large industry-grade SoC
- Detection is fast and usually requires at most a few minutes

Future Work / Please Reach Out:

- Symmetric cryptography based on shift registers
- Side-channel protected implementations
- Actually finding unknown cryptography
- **If you have a real-world device to look at, please reach out to us!**

THE END

If you want to know more:

- HAWKEYE has been published as an academic paper at IACR Crypto’24
- The open-source implementation of HAWKEYE is available as a plugin to our netlist reverse engineering framework HAL

HARRIS 2025 Workshop:

- We host a hardware reverse engineering workshop on March 17-18, 2025
- Located in Bochum, Germany
- Last year: 130 participants from industry, government, and academia

Paper

HAL

HARRIS

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

RUHR-UNIVERSITÄT BOCHUM
Horst-Görtz-Institut für IT-Sicherheit
Exzellenzcluster CASA
MC 0.75 | Universitätsstr. 150 | 44780 Bochum | Germany
www.casa.rub.de | www.hgi.rub.de

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM RUB

HORST GÖRTZ INSTITUT