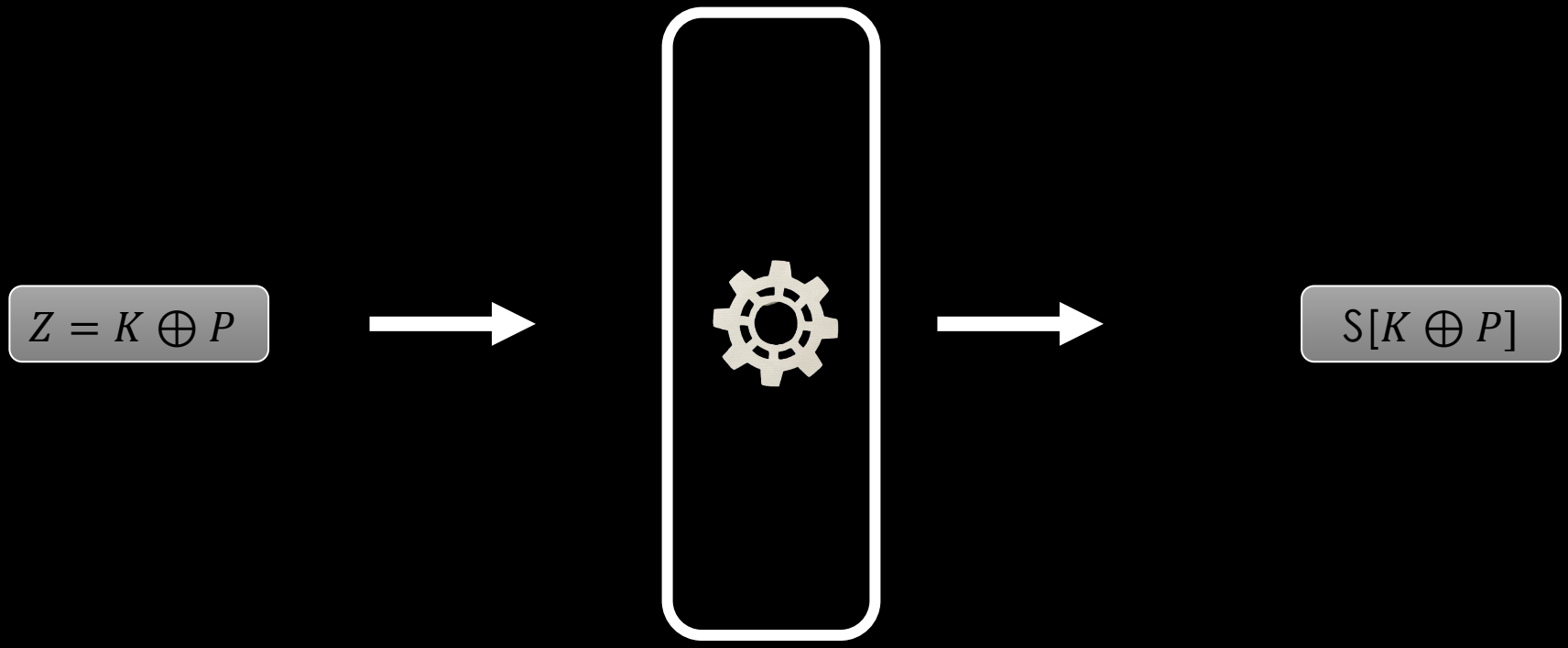
# HOW TO SMASH THE SMAESH CHES CHALLENGE ?

## BEING HONEST OR EVIL…

Valence Cristiani | Ches 2023

NinjaLab

# BEING AN HONEST GUY



# BEING AN HONEST GUY

$Z = K \oplus P$

```
T1 = U0 + U3
T2 = U0 + U5
T3 = U0 + U6
T4 = U3 + U5
T5 = U4 + U6
T6 = T1 + T5
T7 = U1 + U2
```

```
T8 = U7 + T6
T9 = U7 + T7
T10 = T6 + T7
T11 = U1 + U5
T12 = U2 + U5
T13 = T3 + T4
T14 = T6 + T11
```

```
T15 = T5 + T11
T16 = T5 + T12
T17 = T9 + T16
T18 = U3 + U7
T19 = T7 + T18
T20 = T1 + T19
T21 = U6 + U7
```

```
T22 = T7 + T21
T23 = T2 + T22
T24 = T2 + T10
T25 = T20 + T17
T26 = T3 + T16
T27 = T1 + T12
```

Figure 5: Top linear transform in forward direction.

```
T23 = U0 + U3
T22 = U1 # U3
T2 = U0 # U1
T1 = U3 + U4
T24 = U4 # U7
R5 = U6 + U7
T8 = U1 # T23
```

```
T19 = T22 + R5
T9 = U7 # T1
T10 = T2 + T24
T13 = T2 + R5
T3 = T1 + R5
T25 = U2 # T1
R13 = U1 + U6
```

```
T17 = U2 # T19
T20 = T24 + R13
T4 = U4 + T8
R17 = U2 # U5
R18 = U5 # U6
R19 = U2 # U4
Y5 = U0 + R17
```

```
T6 = T22 + R17
T16 = R13 + R19
T27 = T1 + R18
T15 = T10 + T27
T14 = T10 + R18
T26 = T3 + T16
```

Figure 6: Top linear transform in reverse direction.

$S[K \oplus P]$

```
M1 = T13 x T6
M2 = T23 x T8
M3 = T14 + M1
M4 = T19 x D
M5 = M4 + M1
M6 = T3 x T16
M7 = T22 x T9
M8 = T26 + M6
M9 = T20 x T17
M10 = M9 + M6
M11 = T1 x T15
M12 = T4 x T27
M13 = M12 + M11
M14 = T2 x T10
M15 = M14 + M11
M16 = M3 + M2
```

```
M17 = M5 + T24
M18 = M8 + M7
M19 = M10 + M15
M20 = M16 + M13
M21 = M17 + M15
M22 = M18 + M13
M23 = M19 + T25
M24 = M22 + M23
M25 = M22 x M20
M26 = M21 + M25
M27 = M20 + M21
M28 = M23 + M25
M29 = M28 x M27
M30 = M26 x M24
M31 = M20 x M23
M32 = M27 x M31
```

```
M33 = M27 + M25
M34 = M21 x M22
M35 = M24 x M34
M36 = M24 + M25
M37 = M21 + M29
M38 = M32 + M33
M39 = M23 + M30
M40 = M35 + M36
M41 = M38 + M40
M42 = M37 + M39
M43 = M37 + M38
M44 = M39 + M40
M45 = M42 + M41
M46 = M44 x T6
M47 = M40 x T8
M48 = M39 x D
```

```
M49 = M43 x T16
M50 = M38 x T9
M51 = M37 x T17
M52 = M42 x T15
M53 = M45 x T27
M54 = M41 x T10
M55 = M44 x T13
M56 = M40 x T23
M57 = M39 x T19
M58 = M43 x T3
M59 = M38 x T22
M60 = M37 x T20
M61 = M42 x T1
M62 = M45 x T4
M63 = M41 x T2
```

Sbox tower fileds implementation

# BEING AN HONEST GUY

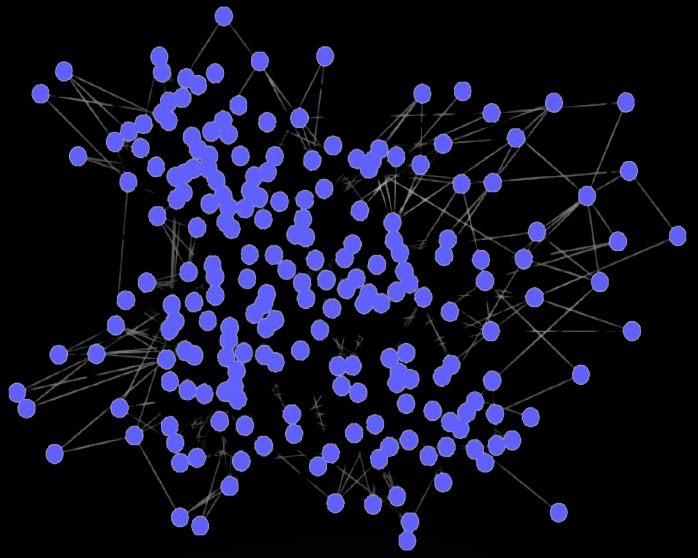
| | | | |
|---|---|---|---|
| T1 = U0 + U3 | T8 = U7 + T6 | T15 = T5 + T11 | T22 = T7 + T21 |
| T2 = U0 + U5 | T9 = U7 + T7 | T16 = T5 + T12 | T23 = T2 + T22 |
| T3 = U0 + U6 | T10 = T6 + T7 | T17 = T9 + T16 | T24 = T2 + T10 |
| T4 = U3 + U5 | T11 = U1 + U5 | T18 = U3 + U7 | T25 = T20 + T17 |
| T5 = U4 + U6 | T12 = U2 + U5 | T19 = T7 + T18 | T26 = T3 + T16 |
| T6 = T1 + T5 | T13 = T3 + T4 | T20 = T1 + T19 | T27 = T1 + T12 |
| T7 = U1 + U2 | T14 = T6 + T11 | T21 = U6 + U7 | |

Figure 5: Top linear transform in forward direction.

| | | | |
|---|---|---|---|
| T23 = U0 + U3 | T19 = T22 + R5 | T17 = U2 # T19 | T6 = T22 + R17 |
| T22 = U1 # U3 | T9 = U7 # T1 | T20 = T24 + R13 | T16 = R13 + R19 |
| T2 = U0 # U1 | T10 = T2 + T24 | T4 = U4 + T8 | T27 = T1 + R18 |
| T1 = U3 + U4 | T13 = T2 + R5 | R17 = U2 # U5 | T15 = T10 + T27 |
| T24 = U4 # U7 | T3 = T1 + R5 | R18 = U5 # U6 | T14 = T10 + R18 |
| R5 = U6 + U7 | T25 = U2 # T1 | R19 = U2 # U4 | T26 = T3 + T16 |
| T8 = U1 # T23 | R13 = U1 + U6 | Y5 = U0 + R17 | |

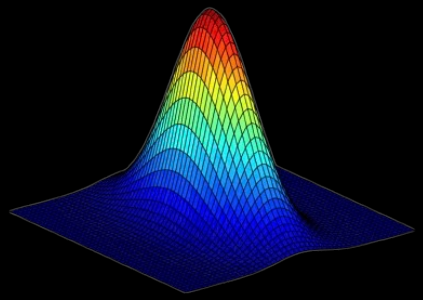
Figure 6: Top linear transform in reverse direction.

| | | | |
|---|---|---|---|
| M1 = T13 x T6 | M17 = M5 + T24 | M33 = M27 + M25 | M49 = M43 x T16 |
| M2 = T23 x T8 | M18 = M8 + M7 | M34 = M21 x M22 | M50 = M38 x T9 |
| M3 = T14 + M1 | M19 = M10 + M15 | M35 = M24 x M34 | M51 = M37 x T17 |
| M4 = T19 x D | M20 = M16 + M13 | M36 = M24 + M25 | M52 = M42 x T15 |
| M5 = M4 + M1 | M21 = M17 + M15 | M37 = M21 + M29 | M53 = M45 x T27 |
| M6 = T3 x T16 | M22 = M18 + M13 | M38 = M32 + M33 | M54 = M41 x T10 |
| M7 = T22 x T9 | M23 = M19 + T25 | M39 = M23 + M30 | M55 = M44 x T13 |
| M8 = T26 + M6 | M24 = M22 + M23 | M40 = M35 + M36 | M56 = M40 x T23 |
| M9 = T20 x T17 | M25 = M22 x M20 | M41 = M38 + M40 | M57 = M39 x T19 |
| M10 = M9 + M6 | M26 = M21 + M25 | M42 = M37 + M39 | M58 = M43 x T3 |
| M11 = T1 x T15 | M27 = M20 + M21 | M43 = M37 + M38 | M59 = M38 x T22 |
| M12 = T4 x T27 | M28 = M23 + M25 | M44 = M39 + M40 | M60 = M37 x T20 |
| M13 = M12 + M11 | M29 = M28 x M27 | M45 = M42 + M41 | M61 = M42 x T1 |
| M14 = T2 x T10 | M30 = M26 x M24 | M46 = M44 x T6 | M62 = M45 x T4 |
| M15 = M14 + M11 | M31 = M20 x M23 | M47 = M40 x T8 | M63 = M41 x T2 |
| M16 = M3 + M2 | M32 = M27 x M31 | M48 = M39 x D | |



Build the ~~huge and horrible~~ graph from the equations

Make more than 4000 Gaussian templates (2 for each node since it's masked)



Apply belief propagation algorithm (SASCA) and recover the key

# BEING AN HONEST GUY

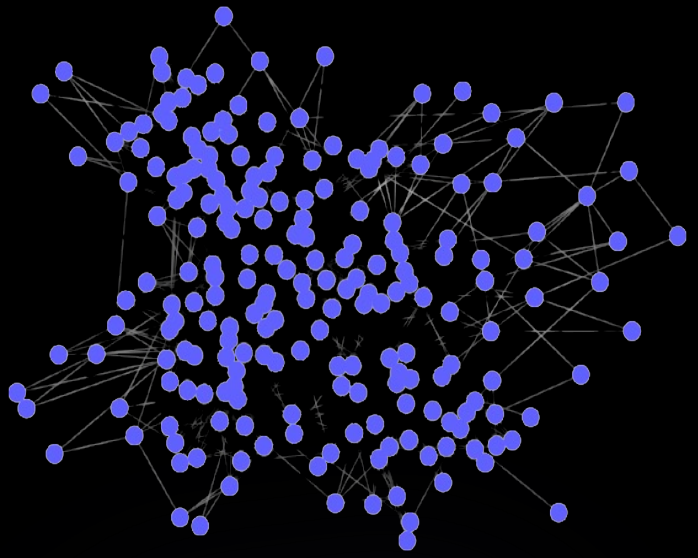
| | | | |
|---|---|---|---|
| T1 = U0 + U3 | T8 = U7 + T6 | T15 = T5 + T11 | T22 = T7 + T21 |
| T2 = U0 + U5 | T9 = U7 + T7 | T16 = T5 + T12 | T23 = T2 + T22 |
| T3 = U0 + U6 | T10 = T6 + T7 | T17 = T9 + T16 | T24 = T2 + T10 |
| T4 = U3 + U5 | T11 = U1 + U5 | T18 = U3 + U7 | T25 = T20 + T17 |
| T5 = U4 + U6 | T12 = U2 + U5 | T19 = T7 + T18 | T26 = T3 + T16 |
| T6 = T1 + T5 | T13 = T3 + T4 | T20 = T1 + T19 | T27 = T1 + T12 |
| T7 = U1 + U2 | T14 = T6 + T11 | T21 = U6 + U7 | |

Figure 5: Top linear transform in forward direction.

| | | | |
|---|---|---|---|
| T23 = U0 + U3 | T19 = T22 + R5 | T17 = U2 # T19 | T6 = T22 + R17 |
| T22 = U1 # U3 | T9 = U7 # T1 | T20 = T24 + R13 | T16 = R13 + R19 |
| T2 = U0 # U1 | T10 = T2 + T24 | T4 = U4 + T8 | T27 = T1 + R18 |
| T1 = U3 + U4 | T13 = T2 + R5 | R17 = U2 # U5 | T15 = T10 + T27 |
| T24 = U4 # U7 | T3 = T1 + R5 | R18 = U5 # U6 | T14 = T10 + R18 |
| R5 = U6 + U7 | T25 = U2 # T1 | R19 = U2 # U4 | T26 = T3 + T16 |
| T8 = U1 # T23 | R13 = U1 + U6 | Y5 = U0 + R17 | |

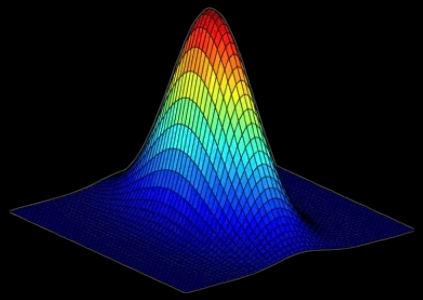
Figure 6: Top linear transform in reverse direction.

| | | | |
|---|---|---|---|
| M1 = T13 x T6 | M17 = M5 + T24 | M33 = M27 + M25 | M49 = M43 x T16 |
| M2 = T23 x T8 | M18 = M8 + M7 | M34 = M21 x M22 | M50 = M38 x T9 |
| M3 = T14 + M1 | M19 = M10 + M15 | M35 = M24 x M34 | M51 = M37 x T17 |
| M4 = T19 x D | M20 = M16 + M13 | M36 = M24 + M25 | M52 = M42 x T15 |
| M5 = M4 + M1 | M21 = M17 + M15 | M37 = M21 + M29 | M53 = M45 x T27 |
| M6 = T3 x T16 | M22 = M18 + M13 | M38 = M32 + M33 | M54 = M41 x T10 |
| M7 = T22 x T9 | M23 = M19 + T25 | M39 = M23 + M30 | M55 = M44 x T13 |
| M8 = T26 + M6 | M24 = M22 + M23 | M40 = M35 + M36 | M56 = M40 x T23 |
| M9 = T20 x T17 | M25 = M22 x M20 | M41 = M38 + M40 | M57 = M39 x T19 |
| M10 = M9 + M6 | M26 = M21 + M25 | M42 = M37 + M39 | M58 = M43 x T3 |
| M11 = T1 x T15 | M27 = M20 + M21 | M43 = M37 + M38 | M59 = M38 x T22 |
| M12 = T4 x T27 | M28 = M23 + M25 | M44 = M39 + M40 | M60 = M37 x T20 |
| M13 = M12 + M11 | M29 = M28 x M27 | M45 = M42 + M41 | M61 = M42 x T1 |
| M14 = T2 x T10 | M30 = M26 x M24 | M46 = M44 x T6 | M62 = M45 x T4 |
| M15 = M14 + M11 | M31 = M20 x M23 | M47 = M40 x T8 | M63 = M41 x T2 |
| M16 = M3 + M2 | M32 = M27 x M31 | M48 = M39 x D | |



Build the ~~huge and horrible~~ graph from the equations

Make more than 4000 Gaussian templates (2 for each node since it's masked)



290k traces

Apply belief propagation algorithm (SASCA) and get the key

## BEING AN HONEST GUY

# But it…

- Requires to understand a lot of theory (graphs, BP algorithm, dealing with the loops etc…)
- Is very long
- Does not even guarantee to win

## BEING AN HONEST GUY

# But it…

- Requires to understand a lot of theory (graphs, BP algorithm, dealing with the loops etc…)
- Is very long
- Does not even guarantee to win

One need a 0 trace attack !

# BEING A BAD GUY

*Let's use another side-channel ? Power leakage is so old shcool…*

The evaluation framework may leak some information


| | | | | |
|---|---|---|---|---|
| Inazawa | A7_d2 | 225000 | ✗ | 127.7 |

**Upper bound of $\log_2(KeyRank)$**

Aggregating many well-crafted submissions may allow to extract enough information on the key → 60 bits is enough !

# BEING AN BAD GUY

*How many submissions?*

- Uniform probability for all bytes except one
- Return a different score for each of the 256 values with a uniform spacing (ex: 1, 2 … , 256)

Obfuscate this behind a neural network…

- Upload the submission and store the $\log_2(KeyRank)$

↓

Avergage of **4.9** bits of information per submissions

4.9 x 13 = 63.7

**Require 13 submissions !**

# BEING A BAD GUY

Read it backwards…

*I created a new account named* ***Sec-artorez***

| | | | | |
|---|---|---|---|---|
| Hawai | A7_d2 | 200000 | ✗ | 128.0 |
| Everest | A7_d2 | 210000 | ✗ | 126.7 |
| Dubai | A7_d2 | 220000 | ✗ | 123.8 |
| Inazawa | A7_d2 | 225000 | ✗ | 127.7 |
| Bahamas | A7_d2 | 215000 | ✗ | 127.8 |
| Zanzibar | A7_d2 | 200000 | ✗ | 127.0 |
| Antarctica | A7_d2 | 180000 | ✗ | 127.3 |
| Capri | A7_d2 | 205000 | ✗ | 128.0 |
| Faliraki | A7_d2 | 220000 | ✗ | 125.2 |
| Gaios | A7_d2 | 180000 | ✗ | 127.9 |
| Jakarta | A7_d2 | 189000 | ✗ | 125.0 |
| Kuala Lumpur | A7_d2 | 230000 | ✗ | 123.3 |

- First letter is a reminder for the concerned byte
- Space the submission by ~ 2 days…

*Local analysis reveals that the we gained 66.1 bits. Means that we should have :*

$$\log_2(KeyRank) = 61.9$$

- Aggregate the results and mount the final attack.

*And…*

# BEING A BAD GUY

Number of traces

| | | | | | |
|---|---|---|---|---|---|
| One_Shot | A7_d2 | 1 | ✅ | 61.9 | **Current challenger!** |

*The SMAesH challenge has been SMASHED*