Beer-recovery attack

Jean-Philippe Aumasson Dmitry Khovratovich

KECCAK

SHA-3 candidate

KECCAK

SHA-3 candidate

Sponge with permutation KECCAK-*f*[1600]

KECCAK

SHA-3 candidate

Sponge with permutation KECCAK-*f*[1600]

No external cryptanalysis

KECCAK

SHA-3 candidate

Sponge with permutation KECCAK-*f*[1600]

No external cryptanalysis

A Trappist 25-beer award

KECCAK

SHA-3 candidate

Sponge with permutation KECCAK-*f*[1600]

No external cryptanalysis

A Trappist 25-beer award

So we start...

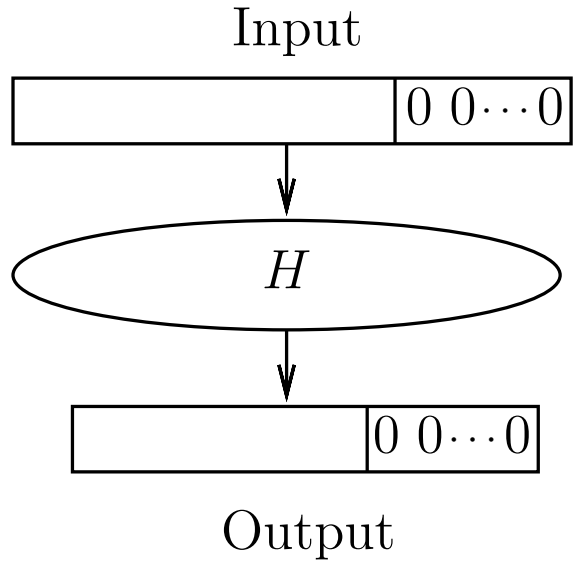
CICO problem for KECCAK-f[1600]

KECCAK-f[1600]: $\{0,1\}^{1600} \mapsto \{0,1\}^{1600}$

18 rounds

Constrained Input – Constrained Output (CICO) problem:

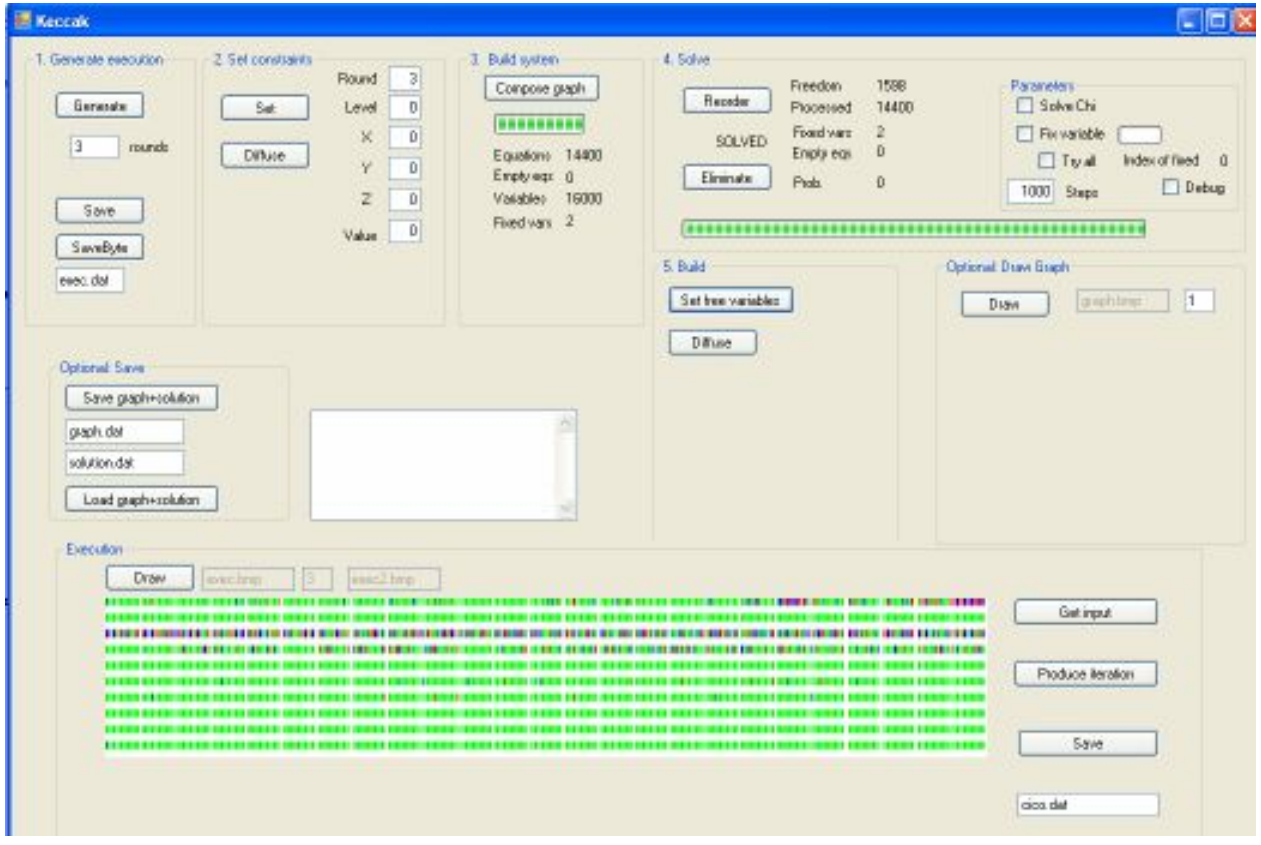
- Fix $X, Y \subset \{0,1\}^{1600}$
- Find many $x \in X,\ y \in Y$: $f(x) = y$
- Hard if X and Y are small



Triangulation tool

- View the transformation as a system of equations
- Fix some input and output bits to 0
- Find solutions with complexity 1

Three rounds (of 18) can be attacked



The tool is online: `https://cryptolux.uni.lu/mediawiki/uploads/0/03/Keccak-tool.zip`

Algebraic analysis

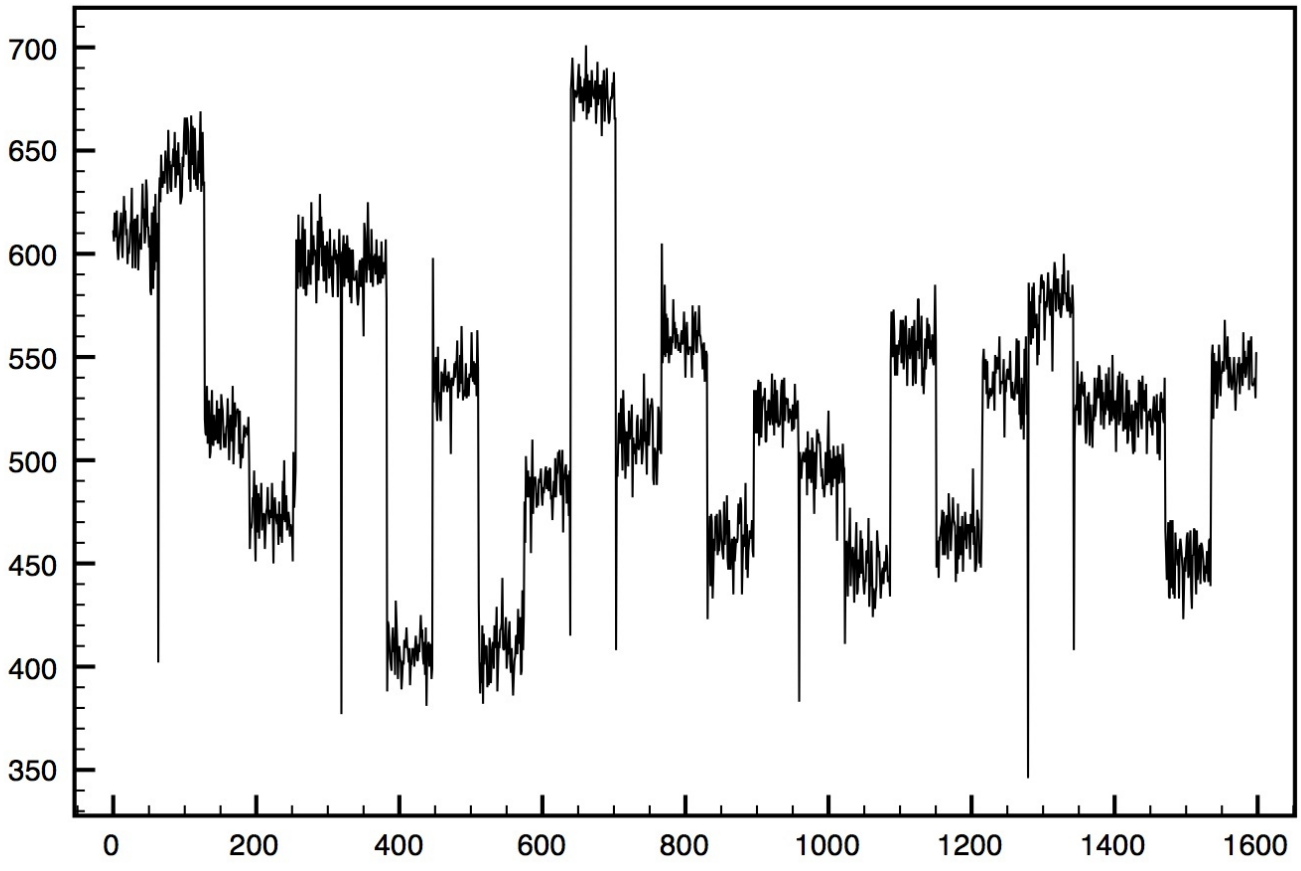
Bounds b on the degree given in the spec

($\Rightarrow$ cube tester in 2^{b+1} possible)

Our result: heterogeneous algebraic structure even for small cubes

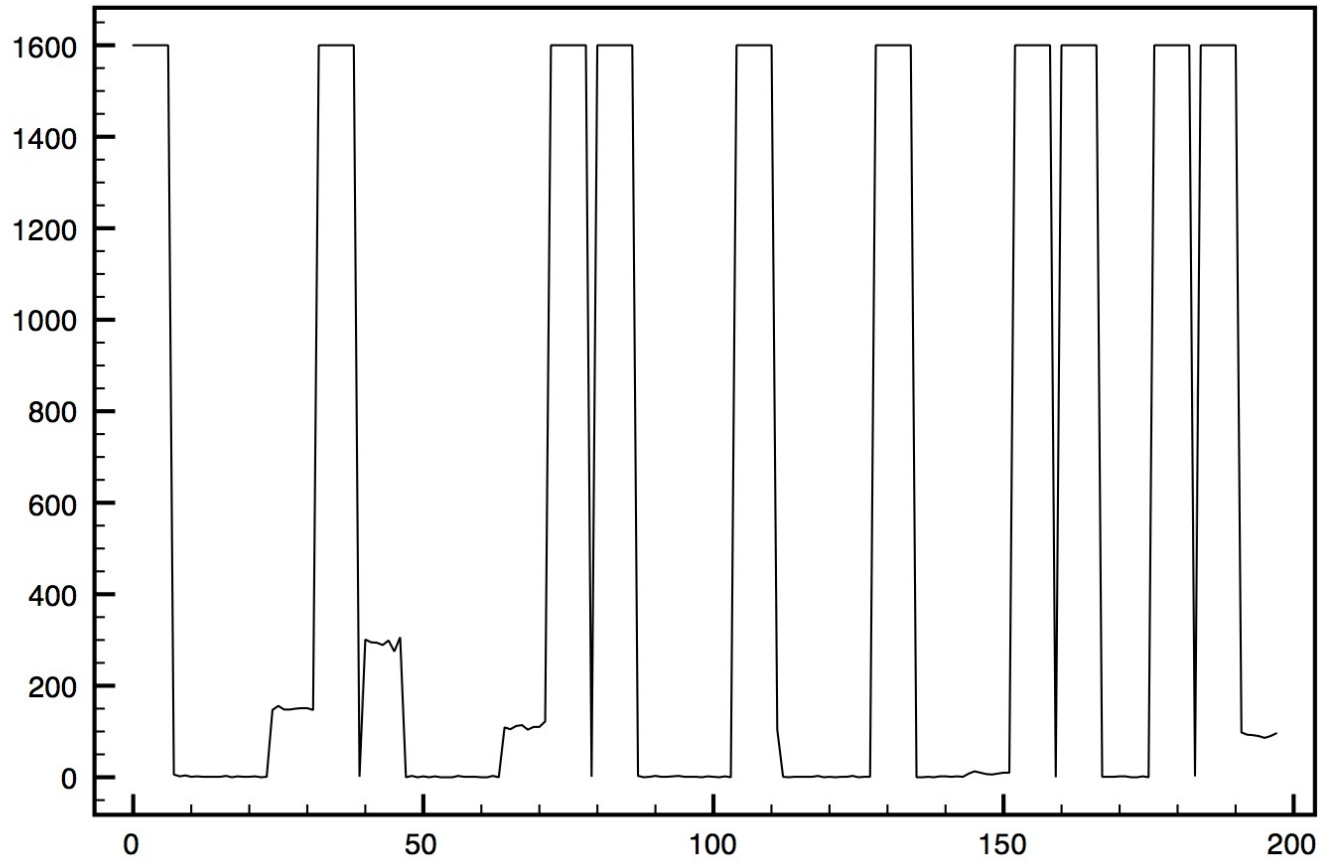
3 rounds, degree-2 cubes

#components attacked = cube position



4 rounds, degree-9 cubes

#components attacked = cube position



KECCAK's doc conjectures 13 rounds enough against distinguishers

Need 11 rounds for maximal degree...

Open problem: how many rounds for a homogenous (reduced-degree) structure?

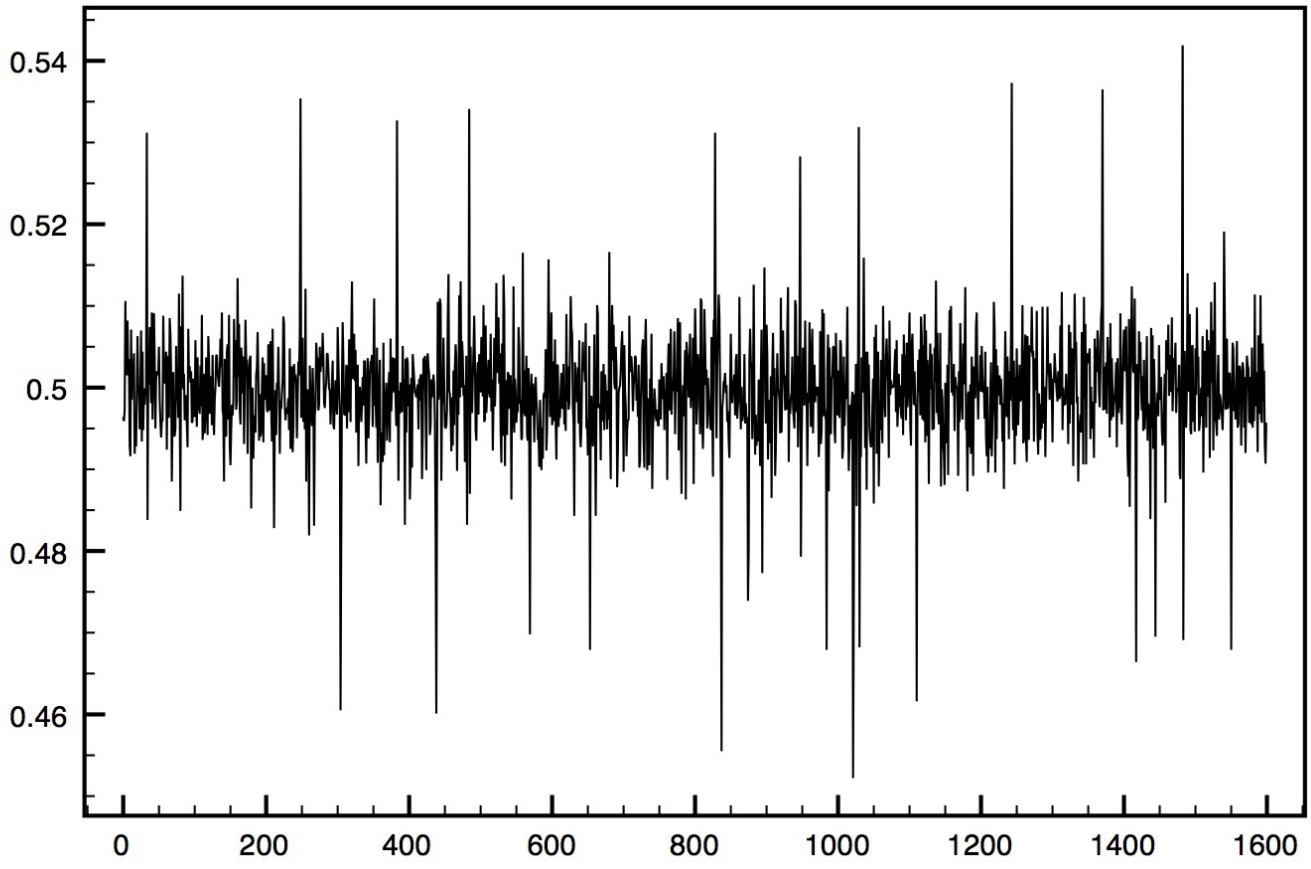
Truncated differentials

First find $\Delta_{\text{in}} \mapsto \Delta_{\text{out}}$ for θ^{-1}
with Hamming weight $|\Delta_{\text{in}}| = 1$, $|\Delta_{\text{out}}| \approx 1600/2$

(conjectured optimal in the documentation)

Used to find probability-1 truncated differential on 3 rounds

On four rounds, still large biases



Conclusions

Inverse permutation more difficult to attack

- Faster diffusion
- Prob-1 differentials on 1 round only

Results consistent with the designers' analysis

Good security margin

The paper is online
`http://131002.net/data/papers/AK09.pdf`