On some algebraic properties of Keccak

Christina Boura, Anne Canteaut and Christophe De Cannière

DTU, Inria and Google

http://www-rocq.inria.fr/secret/Anne.Canteaut/

Keccak & SHA-3 Day, 27 March 2013

Outline

1. Motivations: algebraic properties of a cryptographic primitive
2. Algebraic properties of Keccak-f
   - due to the use of a small Sbox
   - due to the use of a quadratic Sbox
3. Conclusions

Algebraic properties

of a cryptographic primitive

Random behaviour of cryptographic primitives

Cryptographic primitives should behave like random functions.

A distinguishing property may lead to some attacks

e.g., finding the plaintext among a few possibilities.

Security proofs of many constructions assume random building blocks

e.g., in [Bertoni et al. 08]: *A padded sponge construction calling a random transformation, $\mathcal{S}'[\mathcal{F}]$, is $(t_D, t_S, N, \varepsilon)$-indistinguishable from a random oracle, for any $t_D, t_S = O(N^2), N < 2c$ and any ε with $\varepsilon > f_T(N)$.*

This does not mean that a non-random behaviour of the inner transformation leads to a distinguisher for the construction .

Does Keccak-f behave like a random permutation of $\mathbb{F}_2^{1600}$?

Algebraic normal form of a function.

$f : \mathbf{F}_2^n \to \mathbf{F}_2$ has a unique polynomial representation in $\mathbf{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
	0	0	1	1	1	0	0	1	0	0	1	1	1	0	0	1	0	0	1	1	1	0	0	1	0	0	1	1	1	0	0	1
	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1
χ	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	1	1	1	1	1	1	1
	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

$$\chi(x_1, \ldots, x_5) = \begin{pmatrix} x_1x_3 + x_2 + x_3 \\ x_2x_4 + x_3 + x_4 \\ x_3x_5 + x_4 + x_5 \\ x_1x_4 + x_5 + x_1 \\ x_2x_5 + x_1 + x_2 \end{pmatrix}$$

ANF of a random function

Uniform distribution over all functions:

equivalent to the uniform distribution over all ANFs.

$\longrightarrow$ each monomial appears with probability $\frac{1}{2}$.

Uniform distribution over all permutations:

open problem.

- all coordinates of a permutation of $\mathbf{F}_2^n$ have degree at most $(n-1)$.
- almost all permutations of $\mathbf{F}_2^n$ have degree $(n-1)$ [Wells 69], [Das 02], [Konyagin-Pappalardi 02]

Some attacks exploiting a non-random ANF

Algebraic attacks.
The attacker can write the equations defining the primitive and try to solve the polynomial system.

Cube attacks [Dinur-Shamir 09].
The factor of some monomial depends linearly on the key bits.

Higher-order differential cryptanalysis [Lai 94][Knudsen 94].
If F has degree $d < n$, all derivatives of order $(d+1)$ vanish:

$$D_{a_1} D_{a_2} \dots D_{a_{d+1}} F(x) = \bigoplus_{v \in \langle a_1, \dots, a_{d+1} \rangle} F(x+v) = 0 \,.$$

Zero-sums [Knudsen-Rijmen 07][Aumasson-Meier 09]

Definition. Let $F : \mathbf{F}_2^n \to \mathbf{F}_2^n$.

A zero-sum for F of size K is a subset $\{x_1, \ldots, x_K\} \subset \mathbf{F}_2^n$ such that

$$\bigoplus_{i=1}^{K} x_i = \bigoplus_{i=1}^{K} F(x_i) = 0.$$

Zero-sums [Knudsen-Rijmen 07][Aumasson-Meier 09]

Definition. Let $F : \mathbf{F}_2^n \to \mathbf{F}_2^n$.

A zero-sum for F of size K is a subset $\{x_1, \ldots, x_K\} \subset \mathbf{F}_2^n$ such that

$$\bigoplus_{i=1}^{K} x_i = \bigoplus_{i=1}^{K} F(x_i) = 0.$$

Proposition. [Boura-Canteaut 10]

For any function F, there exists at least a zero-sum of size ≤ 5.

Zero-sums [Knudsen-Rijmen 07][Aumasson-Meier 09]

Definition. Let $F : \mathbf{F}_2^n \to \mathbf{F}_2^n$.

A zero-sum for F of size K is a subset $\{x_1, \ldots, x_K\} \subset \mathbf{F}_2^n$ such that

$$\bigoplus_{i=1}^{K} x_i = \bigoplus_{i=1}^{K} F(x_i) = 0.$$

Definition. Let P be a permutation from $\mathbf{F}_2^n$ into $\mathbf{F}_2^n$.

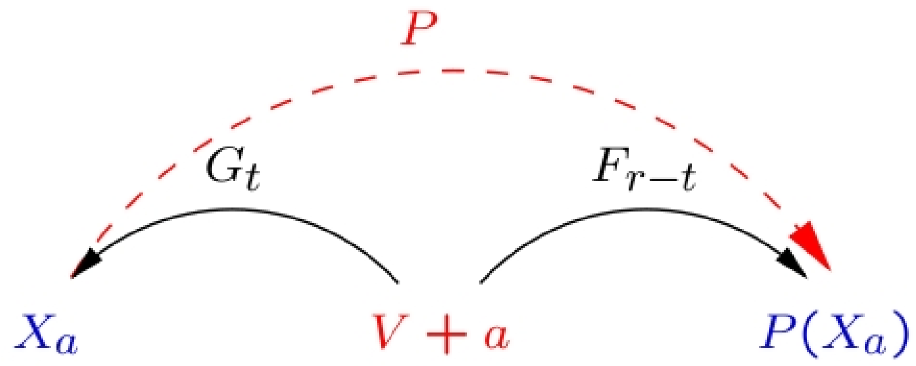
A zero-sum partition for P of size $K = 2^k$ is a collection of 2^{n-k} disjoint zero-sums.

Exploiting a low-degree [Aumasson-Meier 09]

We decompose P into $P = F_{r-t} \circ G_t^{-1}$.

Let $V \subset \mathbf{F}_2^n$ with $\dim V > \max(\deg(F_{r-t}), \deg(G_t))$.

$$X_a = (G_t(a+V))$$



$$\bigoplus_{x \in X_a} x = \bigoplus_{z \in V} G_t(a+z) = 0$$

$$\bigoplus_{x \in X_a} P(x) = \bigoplus_{z \in V} F_{r-t}(a+z) = 0$$

Algebraic properties of Keccak-f

Trivial bounds

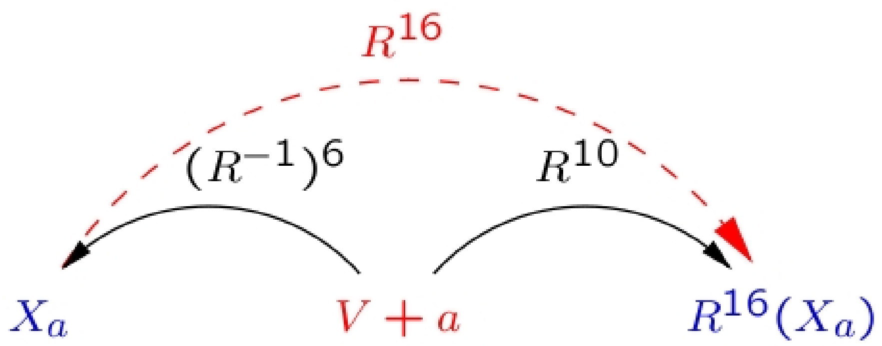
24 rounds of a permutation R of degree 2 over $\mathbf{F}_2^{1600}$

$\rightarrow$ after r rounds, $\deg(R^r) \leq 2^r$.

What is usually expected

- full degree after 11 rounds
- existence of zero-sum partitions up to 16 rounds:

$$\deg(R^{10}) \leq 2^{10} \text{ and } \deg((R^{-1})^6) \leq 3^6$$



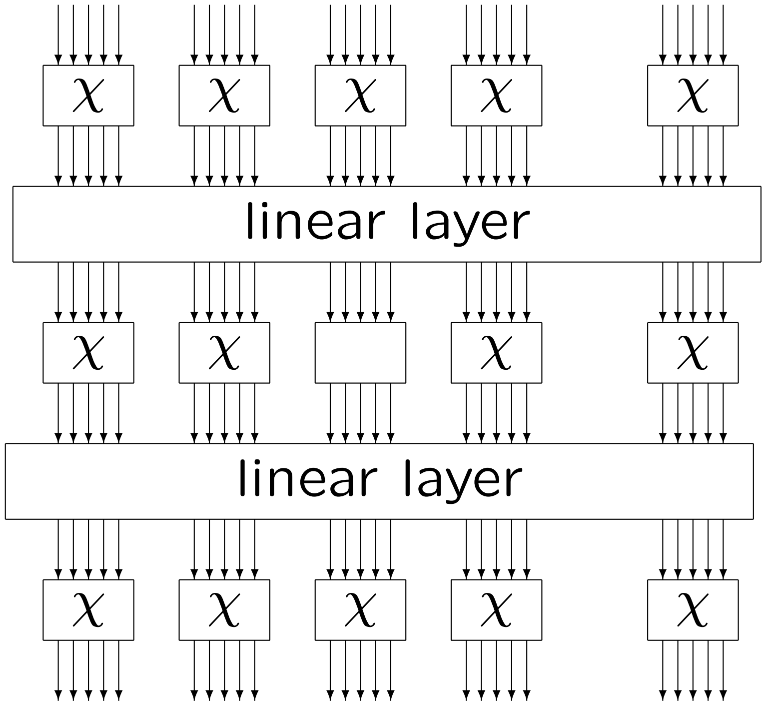
Experiments on Keccak-f[25] [Daemen et al. 08]

number of rounds r	1	2	3	4	5	6
trivial bound	2	4	8	16	24	24
exact value of $\deg R^r$	2	4	8	16	22	24

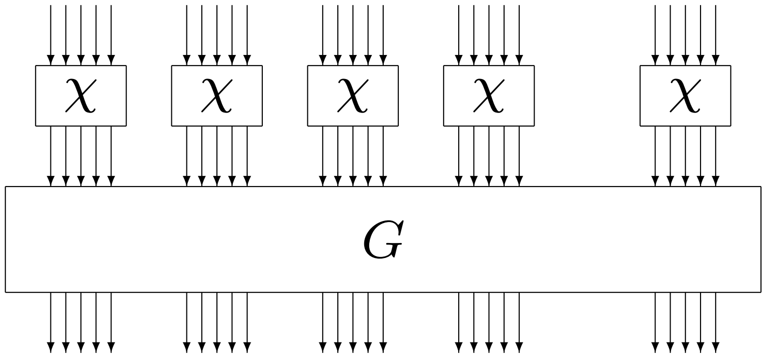
For the inverse function:

number of rounds r	1	2	3	4	5	6
trivial bound	3	9	24	24	24	24
exact value of $\deg(R^{-1})^r$	3	9	17	21	23	24

Using the particular form of the nonlinear layer



Using the particular form of the nonlinear layer



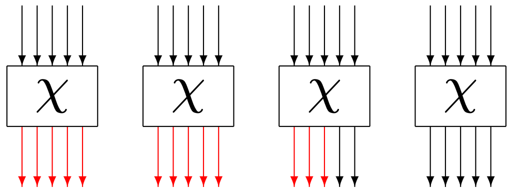
Problem: Find the maximal degree of the product of d output coordinates of the Sbox layer.

Degree of the product π of d output coordinates

A fundamental parameter:

$\boldsymbol{\delta_k}$ = maximal degree of the product of $\boldsymbol{k}$ coordinates of $\boldsymbol{\chi}$

Example: $\boldsymbol{d = 13}$



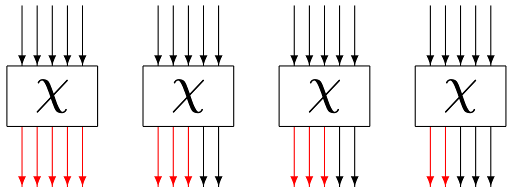
$$\deg \pi \leq 2\delta_5 + \delta_3$$

Degree of the product π of d output coordinates

A fundamental parameter:

δ_k = maximal degree of the product of k coordinates of χ

Example: $d = 13$



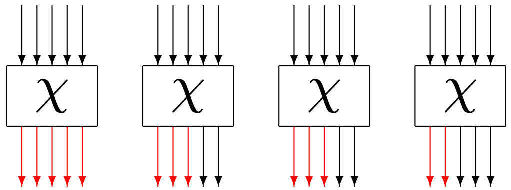
$$\deg \pi \leq \delta_5 + 2\delta_3 + \delta_2$$

Degree of the product π of d output coordinates

A fundamental parameter:

δ_k = maximal degree of the product of k coordinates of χ

Example: $d = 13$



$$\deg \pi \leq \max_{(x_1,\ldots,x_5)} (x_1\delta_1 + \ldots + x_5\delta_5)$$

with $x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 = d$.

Bound on δ_k

δ_k = maximal degree of the product of k coordinates of χ

For χ:

k	1	2	3	4	5
δ_k	2	4	5	5	5

Proposition. If S is a permutation of $\mathbf{F}_2^n$,

$$\delta_k = n \text{ if and only if } k = n$$

Bound on δ_k

δ_k = maximal degree of the product of k coordinates of χ

For χ:

k	1	2	3	4	5
δ_k	2	4	4	4	5

Proposition. If S is a permutation of $\mathbf{F}_2^n$,

$$\delta_k = n \text{ if and only if } k = n$$

A new bound

Theorem. Let $F = (S, \ldots, S)$ where S is a permutation of $\mathbf{F}_2^{n_0}$. Then,

$$\deg(G \circ F) \leq n - \frac{n - \deg G}{\gamma(S)}$$

where

$$\gamma(S) = \max_{1 \leq k \leq n_0 - 1} \frac{n_0 - k}{n_0 - \delta_k(S)} .$$

For Keccak-f

$$\gamma(\chi) = \max_{1 \leq k \leq 4} \frac{5 - k}{5 - \delta_k(\chi)}$$

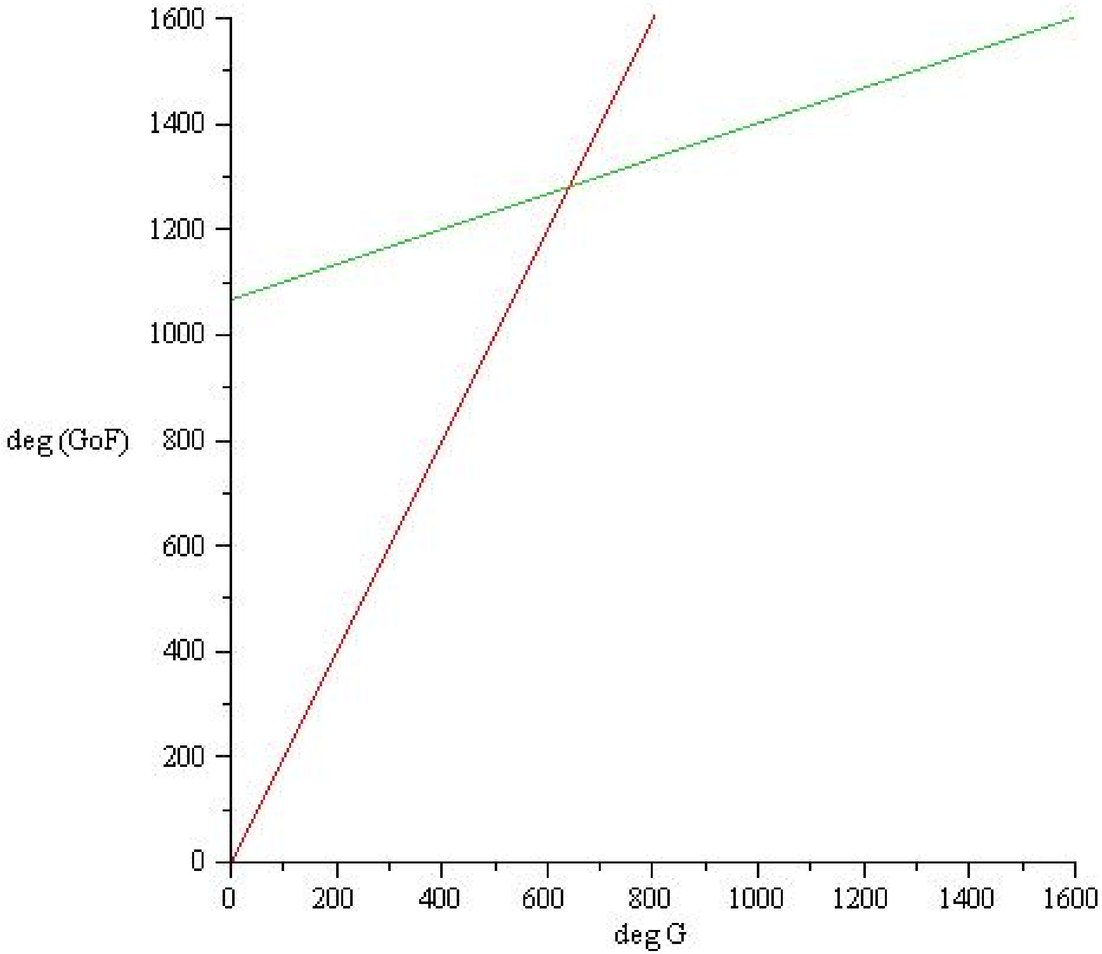
k	1	2	3	4	5
$\delta_k(\chi)$	2	4	4	4	5

$$\gamma(\chi) \leq \max\left(\frac{4}{3}, \frac{3}{1}, \frac{2}{1}, \frac{1}{1}\right) = 3$$

We deduce

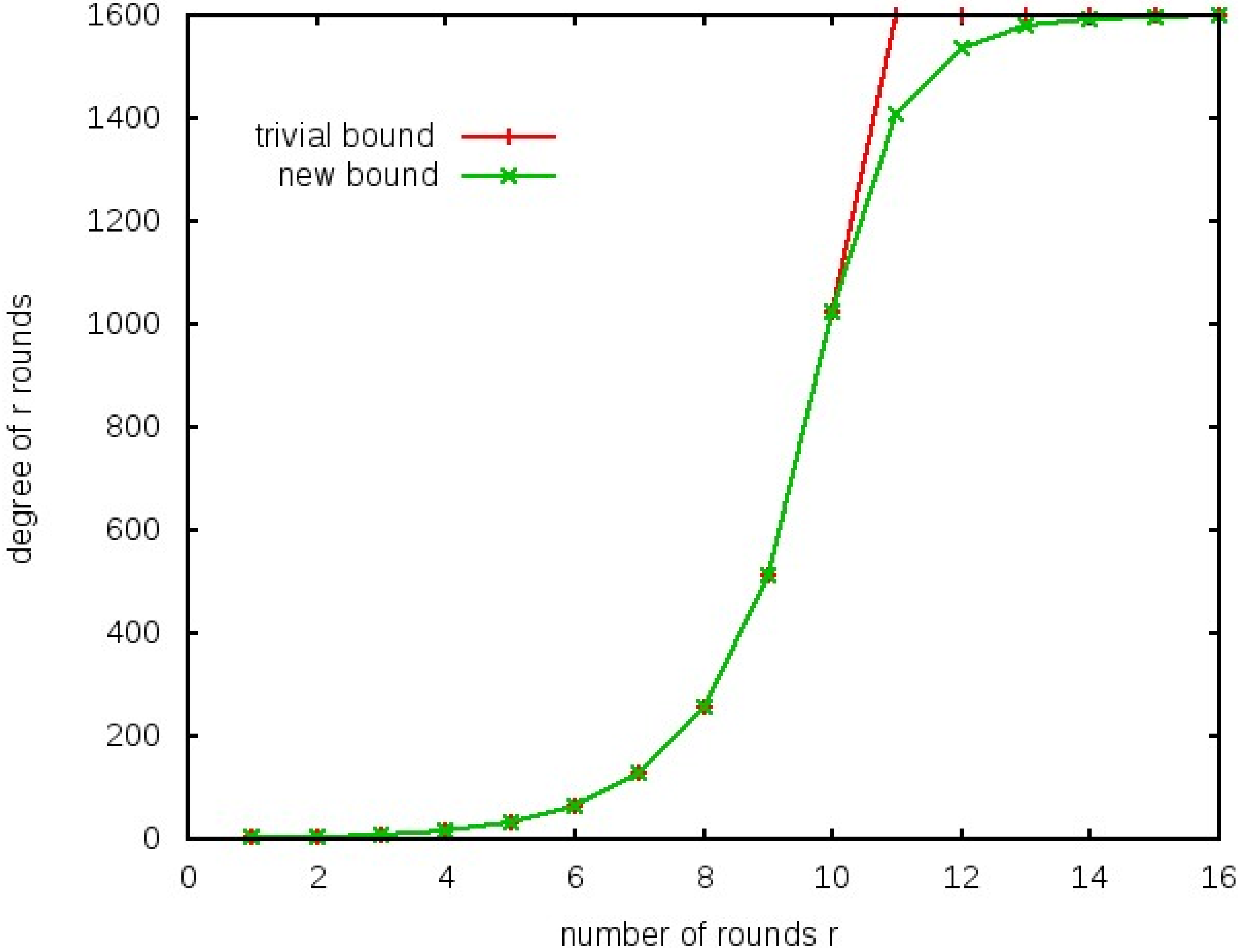
$$\deg(G \circ F) \leq n - \frac{n - \deg G}{3}$$

For Keccak-f



1600
1400
1200
1000
deg (GoF)
800
600
400
200
0
0
200
400
600
800
1000
1200
1400
1600
deg G

Bound on the degree of r rounds of Keccak-f



For the inverse of Keccak-f

Similar bound:

$$\gamma(\chi^{-1}) \le \max_{1 \le k \le 4} \frac{5-k}{5-\delta_k(\chi^{-1})}$$

For χ^{-1}:

k	1	2	3	4	5
$\delta_k(\chi^{-1})$	3	4	4	4	5

Observation [Duan-Lai 11]:

$$\delta_2(\chi^{-1}) = 3$$

Influence of the degree of the inverse

Theorem. Let F be a permutation of $\mathbf{F}_2^n$.
Then, $\delta_\ell(F) < n - k$ if and only if $\delta_k(F^{-1}) < n - \ell$.

For Keccak-f:

$\delta_1(\chi) = 2 < 5 - 2$ implies $\delta_2(\chi^{-1}) < 5 - 1 = 4$.

More generally:

$\delta_1(F^{-1}) = \deg F^{-1} < n - (n - 1 - \deg F^{-1})$ iff $\delta_{n-1-\deg F^{-1}}(F) < n - 1$

i.e., the product of any $(n - 1 - \deg F^{-1})$ coordinates of F has degree at most $(n - 2)$.

A new bound

Theorem. Let $F = (S, \ldots, S)$ where S is a permutation of $\mathbf{F}_2^{n_0}$. Then,

$$\deg(G \circ F) \leq n - \frac{n - \deg G}{\gamma(S)}$$

where

$$\gamma(S) = \max_{1 \leq k \leq n_0 - 1} \frac{n_0 - k}{n_0 - \delta_k(S)} .$$

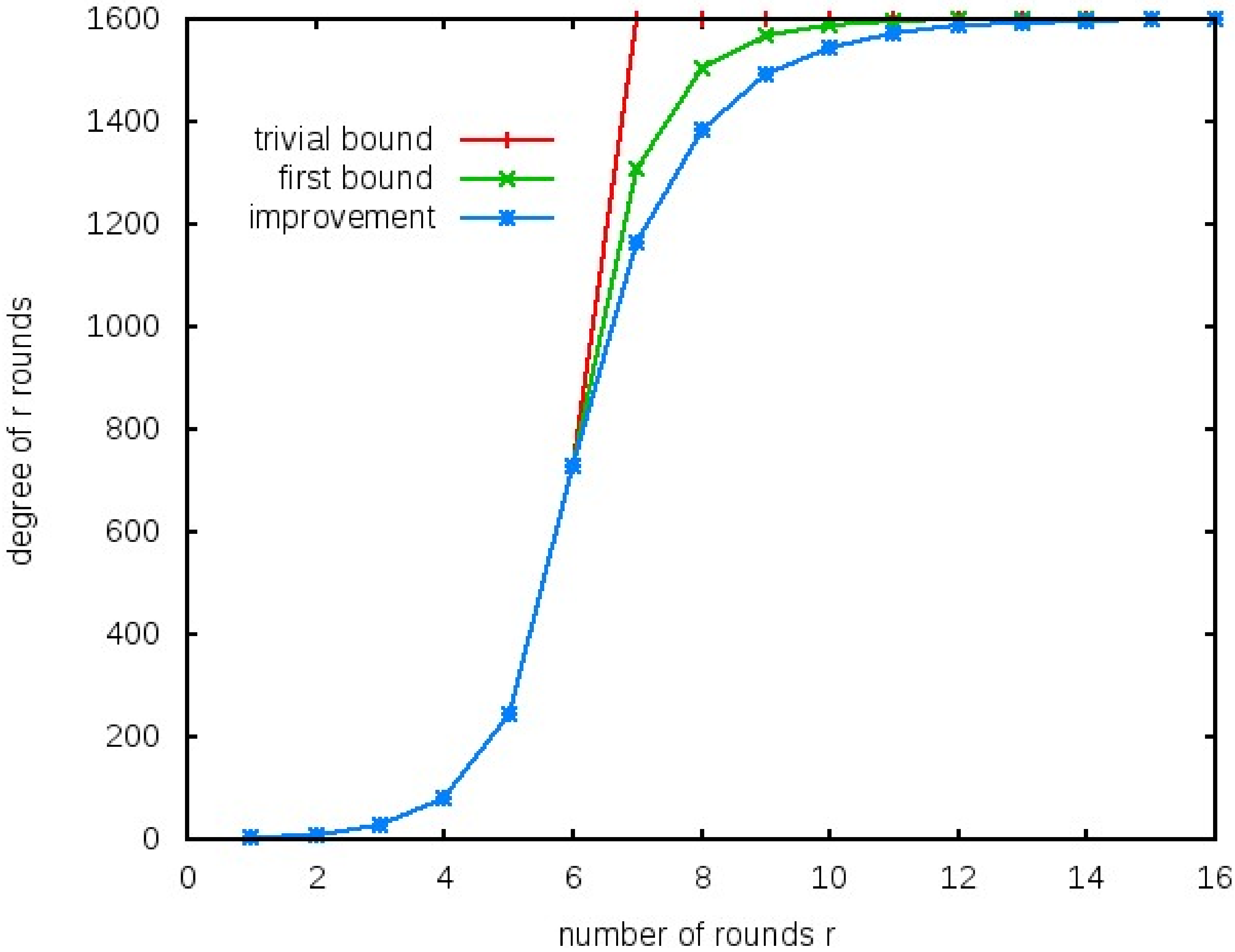
In particular,

$$\gamma(S) \leq \max\left(\frac{n_0 - 1}{n_0 - \deg S}, \frac{n_0}{2} - 1, \deg S^{-1}\right).$$

For the inverse of Keccak-f:

$$\gamma(\chi^{-1}) \leq 2$$

Bound on the degree of r rounds of the inverse



Zero-sum partitions for Keccak-f

- $\mathbf{12}$ rounds forwards have degree at most $\mathbf{1536}$
- $\mathbf{11}$ rounds backwards have degree at most $\mathbf{1572}$

We find several zero-sum partitions of size $\mathbf{2^{1575}}$ for Keccak-$\boldsymbol{f}$.

Conclusions

Zero-sum partitions can be used to gain Belgian beers

Congratulations to the winners of the third KECCAK cryptanalysis prize

16 February 2010

We are happy to announce that **Christina Boura** and **Anne Canteaut** are the winners of the third KECCAK cryptanalysis prize for their paper entitled *A zero-sum property for the KECCAK-f permutation with 18 rounds*. We are currently arranging practical details with the winners to give them the awarded Lambic-based beers and book. *Congratulations to them!*

We will soon announce a new prize with a new deadline.

Does it invalidate the proof?

Theorem. [Bertoni et al. 08] For the sponge construction with capacity c calling an ideal permutation $\mathcal{F}$ of $\mathbf{F}_2^n$, the advantage of any distinguisher totalling at most N calls to $\mathcal{F}$ and $\mathcal{F}^{-1}$ is

$$Adv \leq \frac{N(N+1)}{2^{c+1}} - \frac{N(N-1)}{2^{n+1}}\,.$$

$\longrightarrow$ This result still holds if the inner permutation has a given structural property involving more than $2^{\frac{c+1}{2}}$ input-output pairs.

Comparison with the experiments on Keccak-$f[25]$

number of rounds r	1	2	3	4	5	6
trivial bound	2	4	8	16	24	24
exact value of $\mathbf{deg}\, R^r$	2	4	8	16	22	24
$\min\left(2^r, 25 - \frac{25 - \deg(R^{r-1})}{3}\right)$	2	4	8	16	22	24

For the inverse function:

number of rounds r	1	2	3	4	5	6
trivial bound	3	9	24	24	24	24
exact value of $\mathbf{deg}(R^{-1})^r$	3	9	17	21	23	24
$\min\left(3^r, 25 - \frac{25 - \deg((R^{-1})^{r-1})}{2}\right)$	3	9	17	21	23	24