# Bounds in Shallows and in Miseries

Céline Blondeau Andrey Bogdanov Gregor Leander

ESC 2013

# The Title

## Shakespeare “The Tragedy of Julius Caesar”

Omitted, all the voyage of their life
Is bound in shallows and in miseries

# Outline

# Grøstl

(moves the bytes in each column to eight different columns), it is guaranteed that for Grøstl there are at least $9^2 = 81$ active s-boxes in any four-round differential trail [24, Theorem 9.5.1]. Note that this holds for Grøstl-256 as well as for Grøstl-512. Hence, there are at least $2 \cdot 81 = 162$ and $3 \cdot 81 = 243$ active s-boxes in any eight-round, respectively twelve-round differential trail. This, combined with the maximum difference propagation probability of the s-box of $2^{-6}$, means that the probabilities of any differential trail (assuming independent rounds) over eight and twelve rounds (for either $P$ or $Q$) are expected to be at most $2^{-6 \cdot 162} = 2^{-972}$, respectively $2^{-1458}$. Therefore, in a classical differential attack where one specifies a differential trail for every round for both $P$ and $Q$, there is only a very small chance that this would lead to a successful attack for Grøstl-256 and Grøstl-512.

In the collision attack [78] on Grindahl-256 [53], the low probability of any difference propagation through the s-box is circumvented by ignoring the actual values of differences, and instead only considering whether a byte is active or not. Since in Grindahl, a message block overwrites

# Photon

linear and differential cryptanalysis.

**Table 2.** Upper bounds on the best differential path probability, best differential probability, best linear appro probability and best linear hull probability for 4 rounds and for the full version of the five PHOTON internal perm

| | $P_{100}$ | | $P_{144}$ | | $P_{196}$ | | $P_{256}$ | | $P_{288}$ | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 4 rds | full | 4 rds | full | 4 rds | full | 4 rds | full | 4 rds | f |
| differential path probability | $2^{-72}$ | $2^{-216}$ | $2^{-98}$ | $2^{-294}$ | $2^{-128}$ | $2^{-384}$ | $2^{-162}$ | $2^{-486}$ | $2^{-294}$ | $2^{}$ |
| differential probability | $2^{-50}$ | | $2^{-72}$ | | $2^{-98}$ | | $2^{-128}$ | | $2^{-246}$ | |
| linear approx. probability | $2^{-72}$ | $2^{-216}$ | $2^{-98}$ | $2^{-294}$ | $2^{-128}$ | $2^{-384}$ | $2^{-162}$ | $2^{-486}$ | $2^{-294}$ | $2^{}$ |
| linear hull probability | $2^{-50}$ | | $2^{-72}$ | | $2^{-98}$ | | $2^{-128}$ | | $2^{-246}$ | |

"Note that such a reasoning assumes that random subkeys are added each round"

# Spongent

Table 4: Longest differential characteristics holding with probability in the range of $2^{-b}$ (under independency assumption)

| | # rounds | ASN | Prob |
|---|---|---|---|
| SPONGENT-88/80/8 | 17 | 34 | $2^{-88}$ |
| SPONGENT-88/176/88 | 27 | 103 | $2^{-268}$ |
| SPONGENT-128/128/8 | 20 | 56 | $2^{-137}$ |
| SPONGENT-128/256/128 | 42 | 146 | $2^{-385}$ |
| SPONGENT-160/160/16 | 20 | 66 | $2^{-179}$ |
| SPONGENT-160/160/80 | 44 | 88 | $2^{-242}$ |
| SPONGENT-160/320/160 | 48 | 192 | $2^{-480}$ |
| SPONGENT-224/224/16 | 44 | 88 | $2^{-242}$ |
| SPONGENT-224/224/112 | 26 | 133 | $2^{-343}$ |
| SPONGENT-224/448/224 | - | - | - |
| SPONGENT-256/256/16 | 30 | 108 | $2^{-276}$ |
| SPONGENT-256/256/128 | 31 | 150 | $2^{-392}$ |
| SPONGENT-256/512/256 | 85 | 256 | $2^{-768}$ |

# State-of-the-art

## State-of-the-art

Designs often state bounds without interpreting them (in a specified model).

## Lack of Understanding?

Easy to derive bounds. Interpreting bounds seems more unclear.

# This Work

**This work**

Shed some light on the meaning of those bounds.

What we do not deal with:

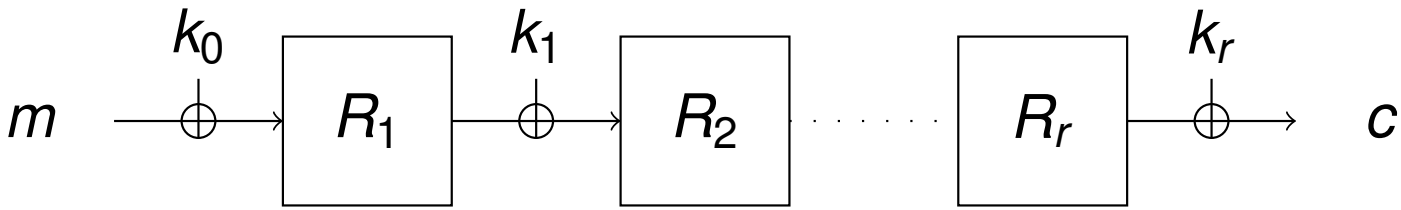
- Differentials
- truncated characteristics
- showing weaknesses in designs.

# (At Least) Two Points To Clarify

- Independency?
- Implication of the bounds?

# Independency (I)

Situation better understood in the case of key-alternating block ciphers.



# Independency (II)

Well established model:

**Cipher-Model**

Assuming independent round keys. The number of pairs fulfilled by a characteristic with probability $p$ is given by

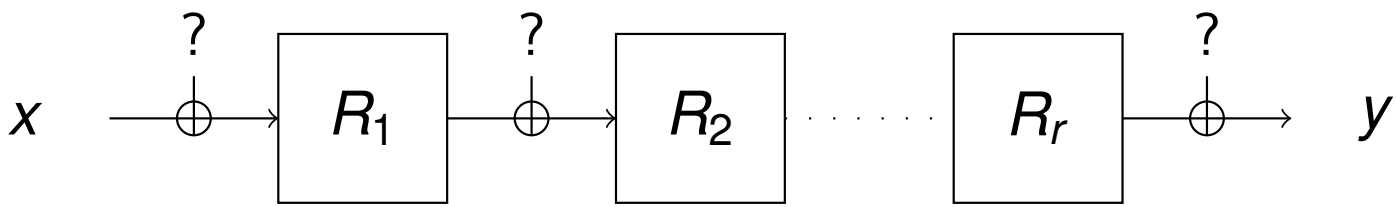
$$X \sim \mathcal{B}(p, N)$$

$$N = 2^{n-1}, n \text{ block-size}$$

Answer to the question: What is the ratio of keys such that a given characteristic is fulfilled by $t$ pairs?

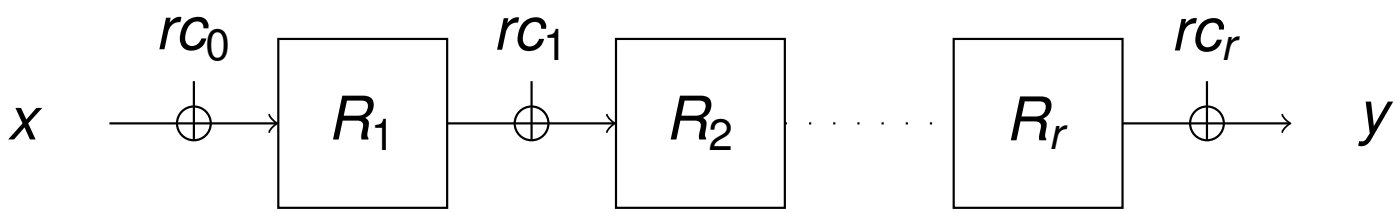
# Independency (III)

Adapting to fixed permutations:



# Independency (III)

Adapting to fixed permutations:



# Independency (II)

Well established model:

**Fixed-Permutation-Model**

Assuming independent round constants. The number of pairs fulfilled by a characteristic with probability $p$ is given by

$$X \sim \mathcal{B}(p, N)$$

$$N = 2^{n-1}, n \text{ block-size}$$

Answer to the question: What is the ratio of round-constants such that a given characteristic is fulfilled by $t$ pairs?

# Implication of the Bounds

With the above model:

## Any Given Characteristic

Given a bound $p$. The probability that any given characteristic is fulfilled by less then $B$ pairs is bounded by

$$\Pr(X < B) = \sum_{t=0}^{B-1} \binom{N}{t} p^t (1-p)^{N-t}$$

## Example (Grøstl's P)

The probability that any given characteristic is fullfiled by no pair is $\approx 1$.

More precisely: $> 1 - 2^{-461}$.

# Implication of the Bounds

But:

**Fixed Permutation**

There always exist characteristics fulfilled by at least one pair!

**Question**

What is the maximal number of pairs fulfilled by a characteristic?

Reciprocally:

**Design Goal**

There is no characteristic fulfilled by more than one (two, three) pair(s).

# Implication of the Bounds

**Strongest Design Goal**

There is no characteristic fulfilled by more than one pair.

**Question**

How small has the bound to be to achieve this goal?

# Outline

# Design Goal

**Strongest Design Goal**

There is no characteristic fulfilled by more than one pair.

How to achieve this? What bound is needed?

**Assumption**

Characteristics are independent.

# Differential Characteristic Spectrum

Bound alone not enough:

**Definition (Differential Characteristic Spectrum)**

The sequence of pairs $(p_i, A_i)$ where

- $p_i$ is the probability
- $A_i$ the number of char. with prob. $p_i$.
- $p_{i+1} < p_i$

Relation:

$$\sum_i A_i p_i = 2^{n-1}$$

# Differential Characteristic Spectrum

**Theorem**

*Under the above Assumptions:*

$$\Pr(\textit{ at most } B \textit{ pairs for any char.}) = \prod_i \Pr(X_i \leq B)^{A_i}$$

*where* $X_i \sim \mathcal{B}(p_i, N)$.

Problem: We cannot compute the (complete) spectrum!

# Differential Characteristic Spectrum

Problem: We cannot compute the (complete) spectrum!

**Solution**

Cut it!

Remember:

$$\sum_i A_i p_i = 2^n$$

# Example: Cutting The Spectrum

| $p_i$ | $A_i$ |
|---|---|
| $2^{-16}$ | 1 |
| $2^{-17}$ | 10 |
| $2^{-18}$ | 44 |
| $2^{-19}$ | 125 |
| $2^{-20}$ | 343 |
| $\vdots$ | $\vdots$ |

$\rightarrow$

| $p_i$ | $A_i$ |
|---|---|
| $2^{-16}$ | 1 |
| $2^{-17}$ | 10 |
| $2^{-18}$ | 44 |
| $2^{-19}$ | 1572728 |

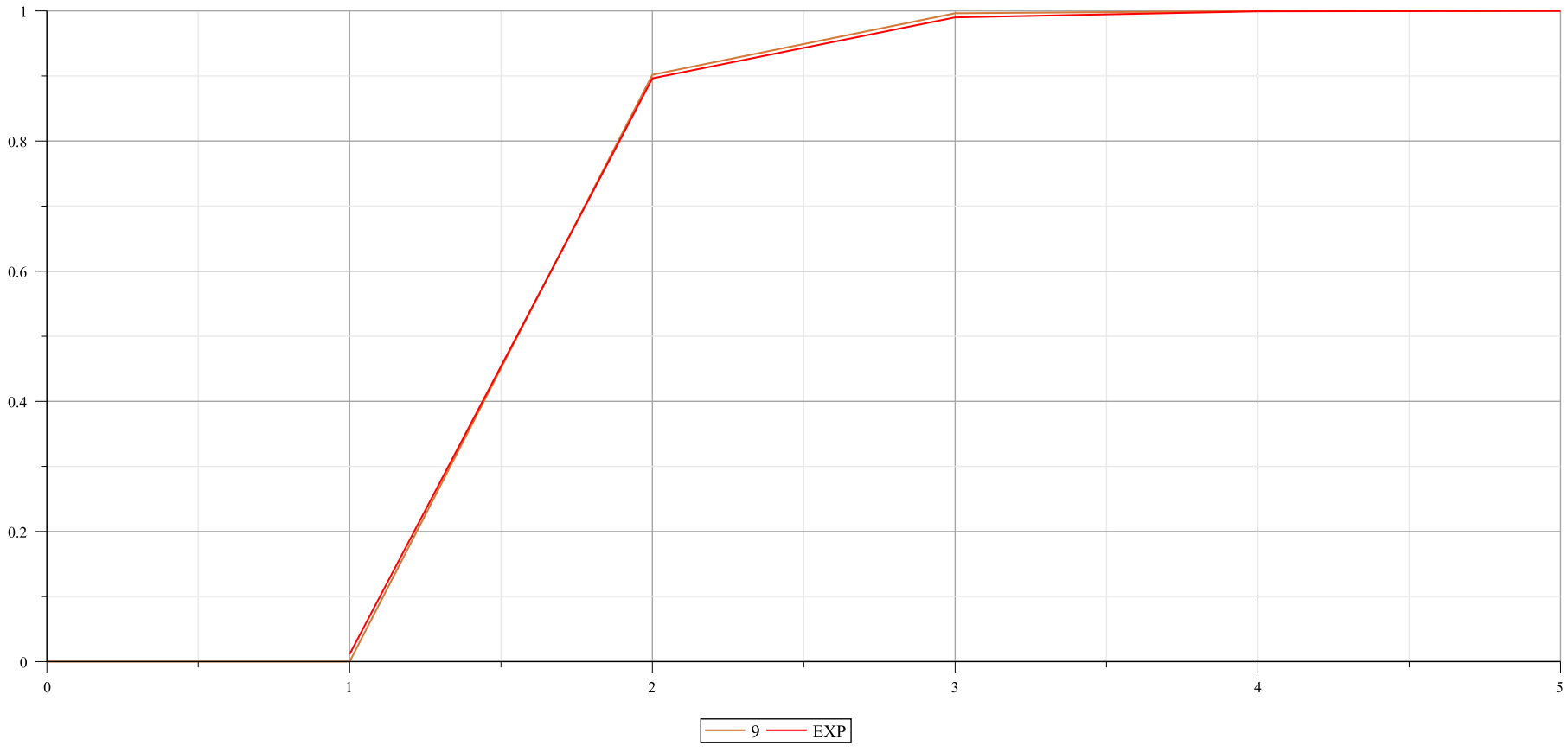
# Cuts Are Okay

**Theorem (Cuts Are Okay)**

$$\Pr(\textit{ at most B pairs for any char.})$$
$$\geq \Pr(\textit{ at most B pairs for any char. for any cut spectrum})$$

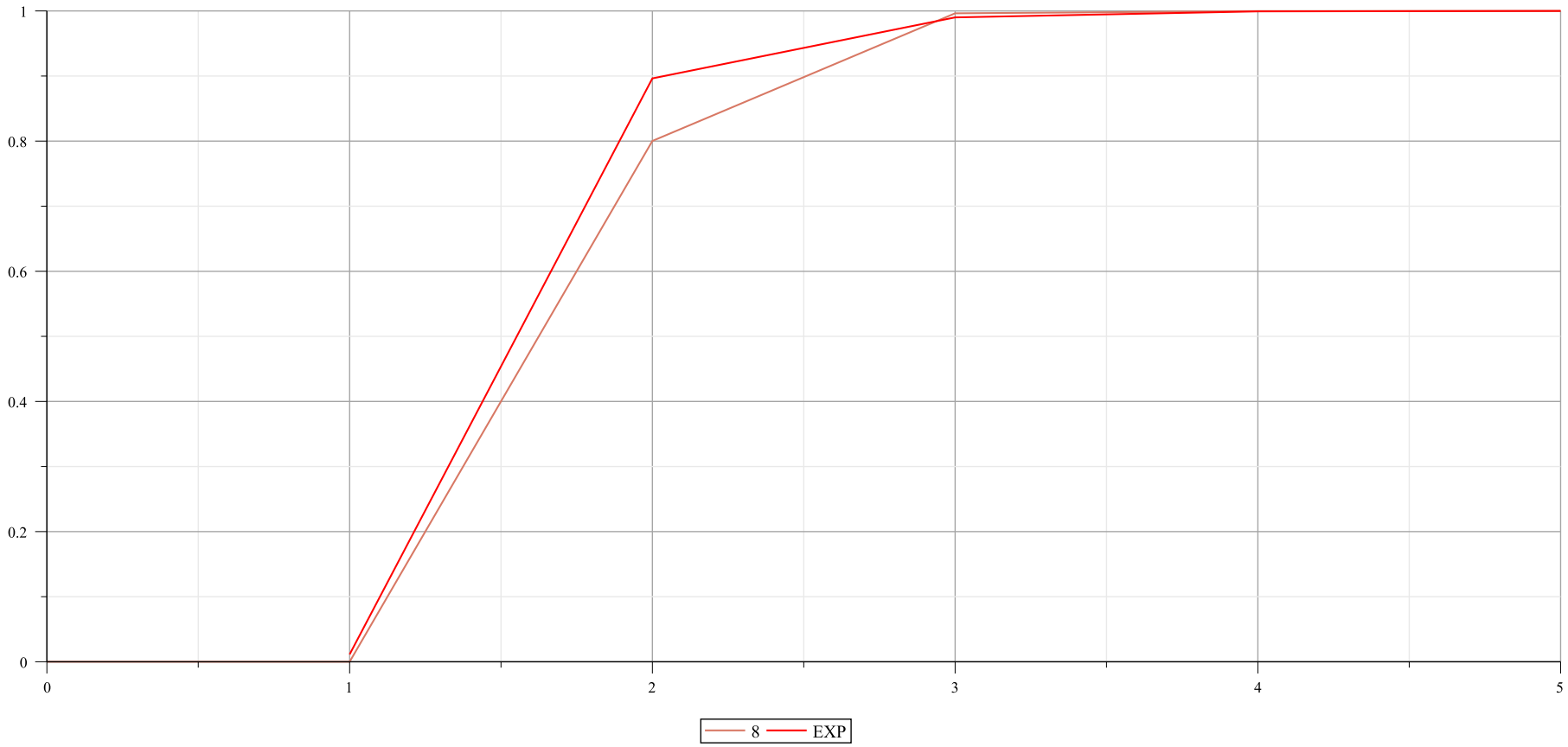
- Positive: Computing the spectra is not needed.
- Negative: Bounds get less tight.

# Example: Small-PRESENT



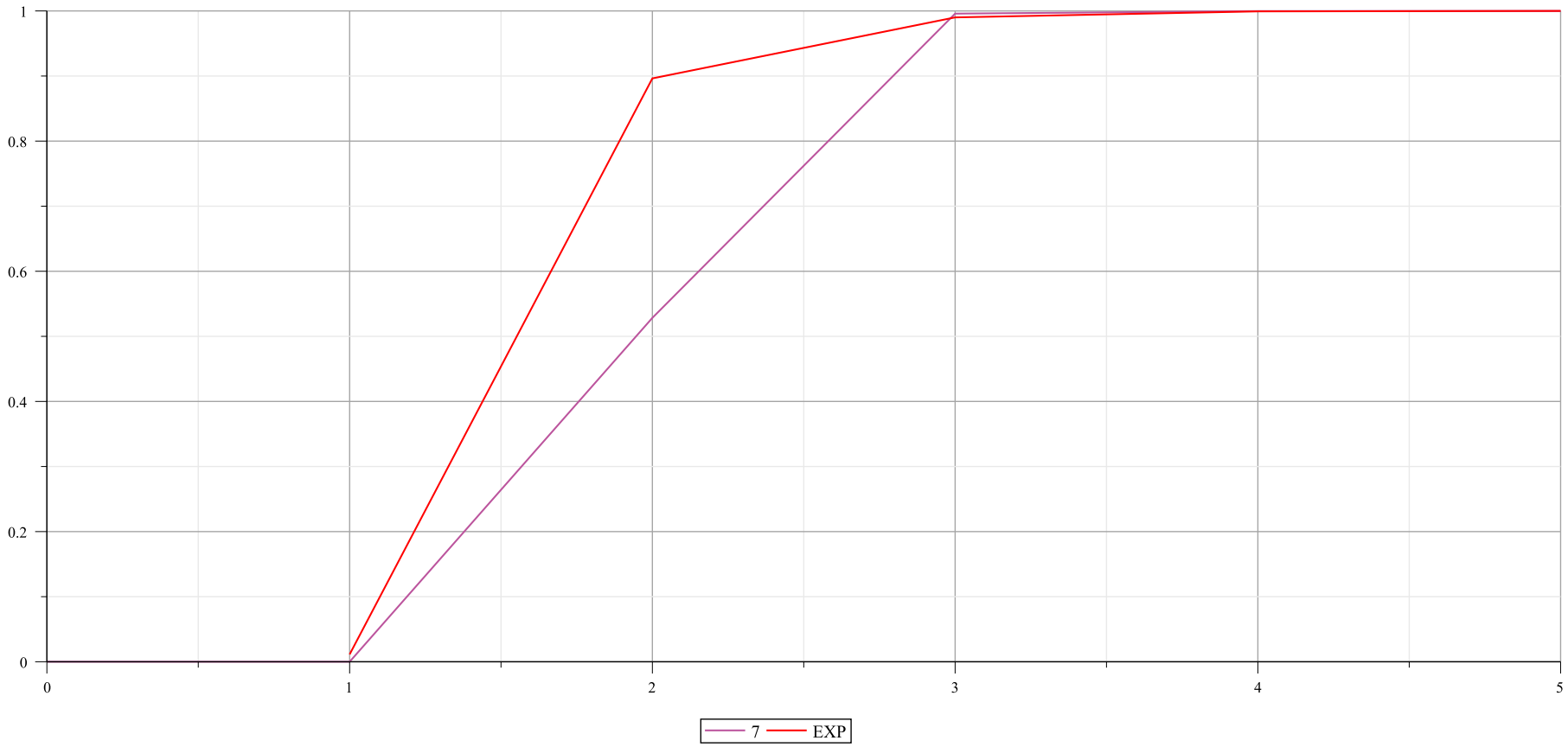

Experimental vs. first 9 $A_i$ considered.

# Example: Small-PRESENT



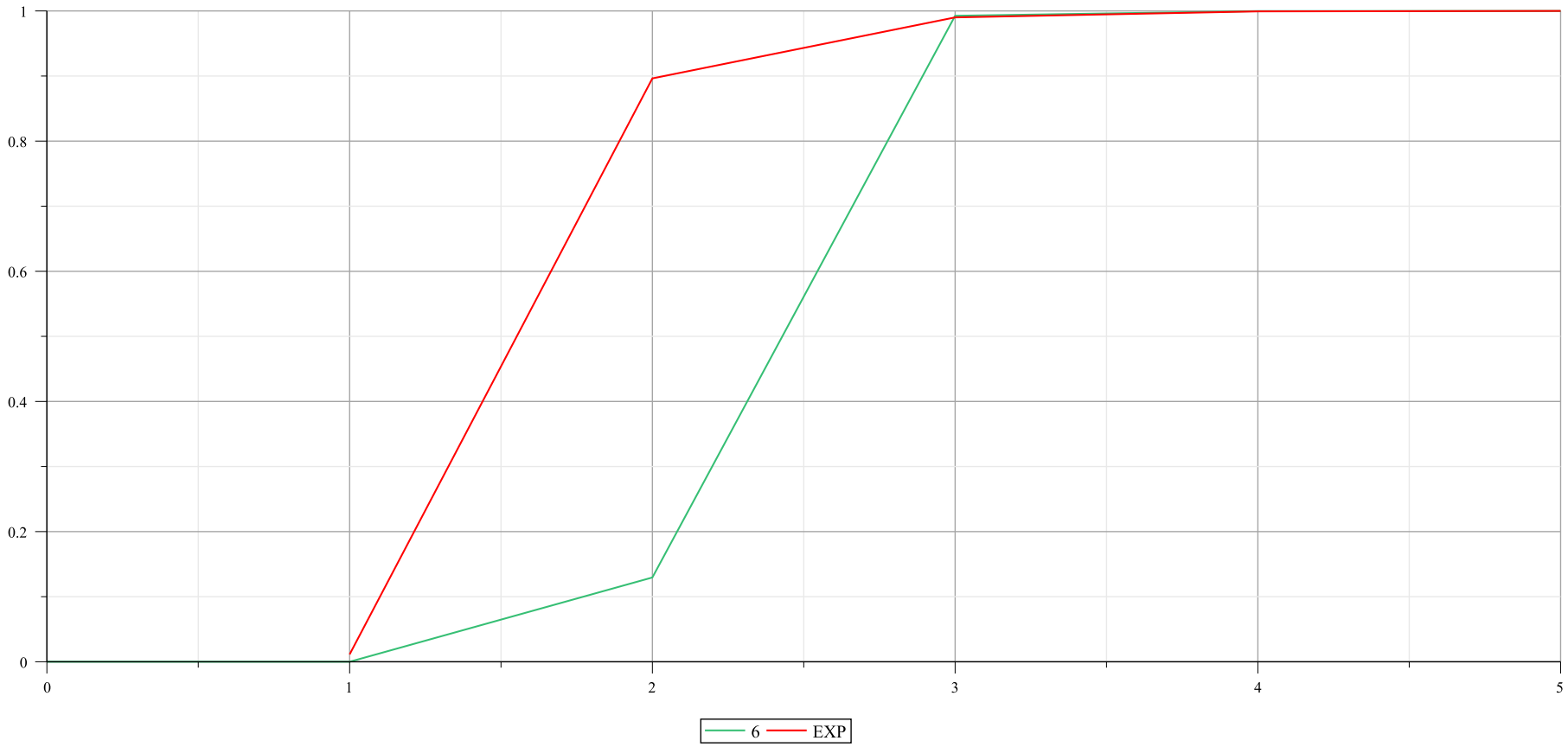

Experimental vs. first 8 $A_i$ considered.

# Example: Small-PRESENT



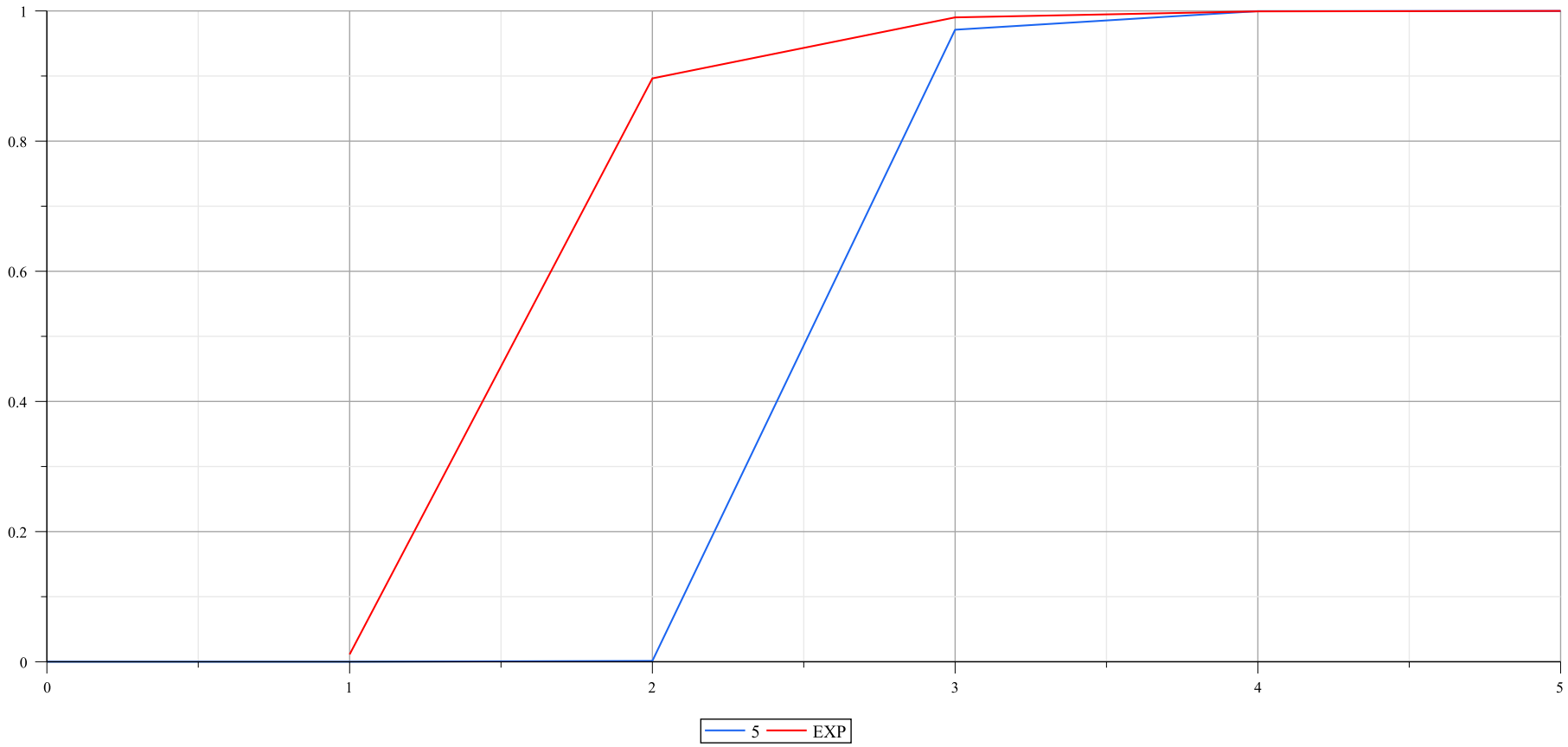

Experimental vs. first 7 $A_i$ considered.

# Example: Small-PRESENT



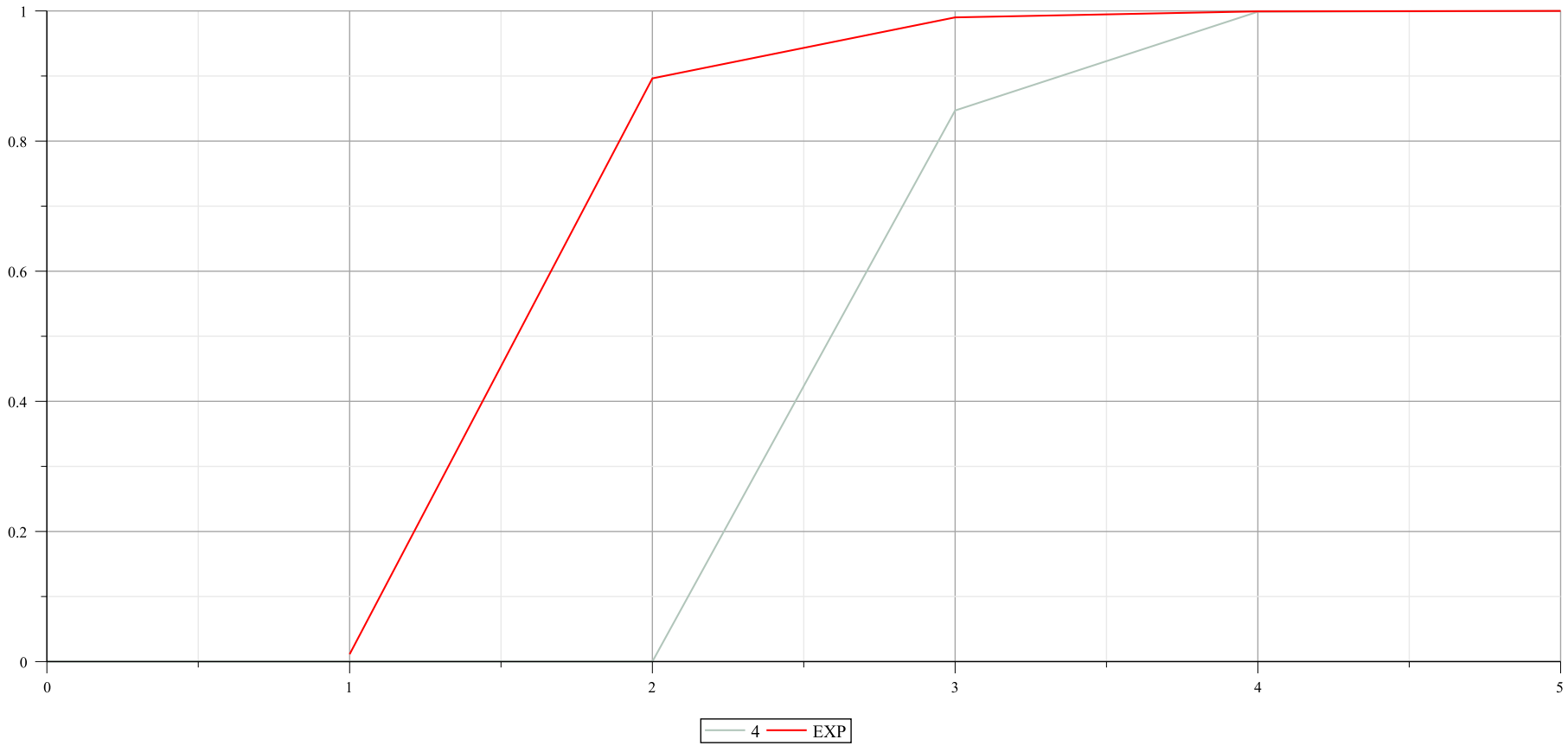

Experimental vs. first 6 $A_i$ considered.

# Example: Small-PRESENT



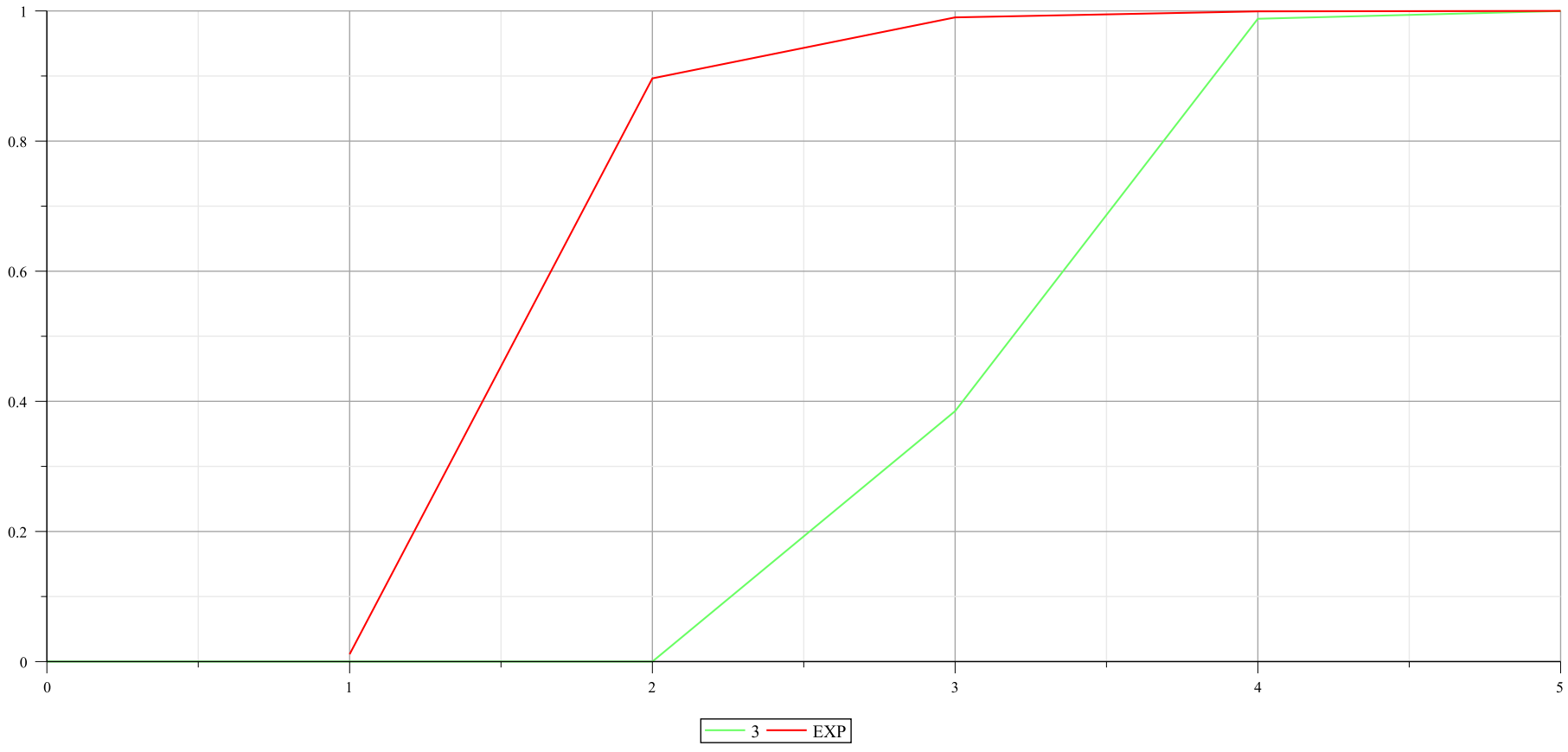

Experimental vs. first 5 $A_i$ considered.

# Example: Small-PRESENT



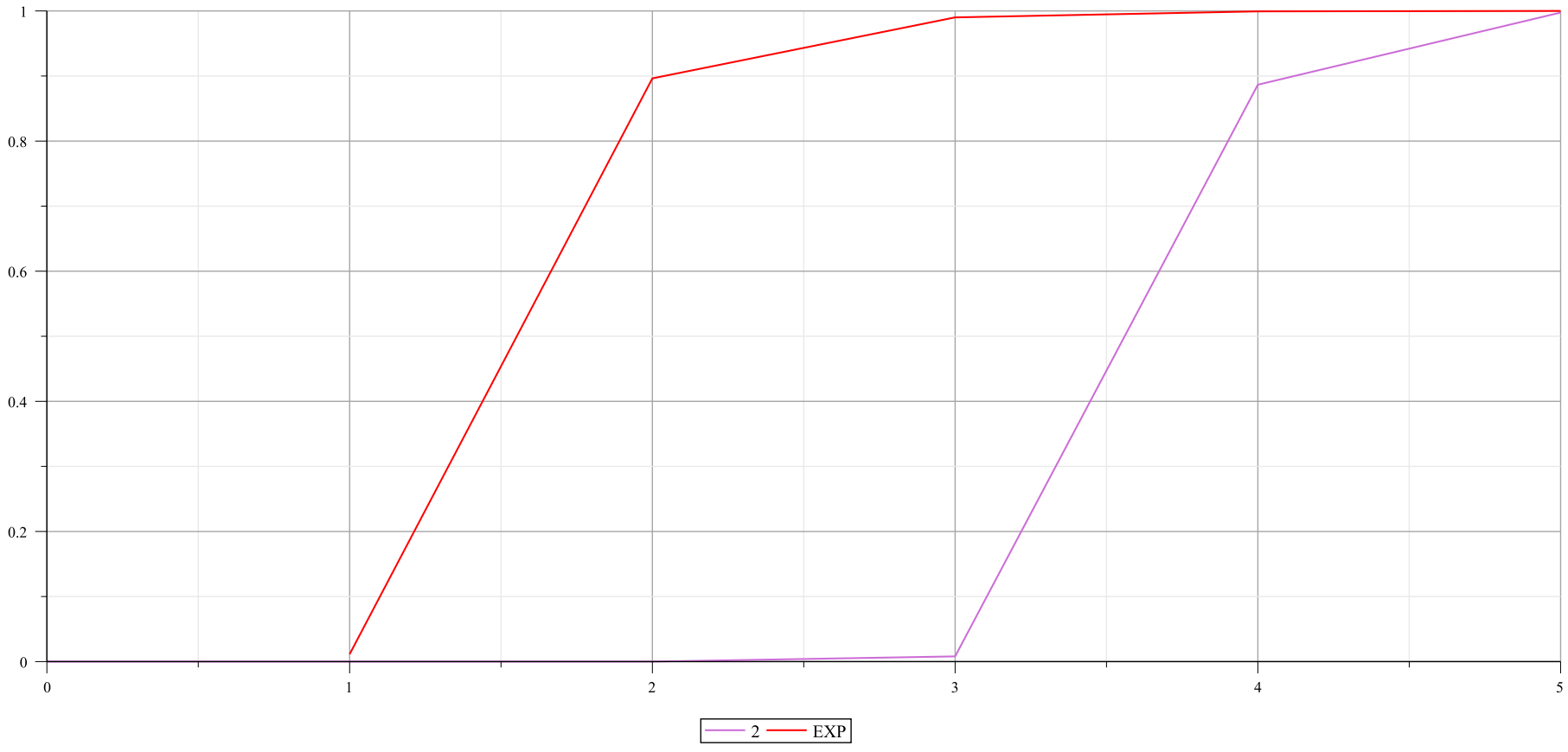

Experimental vs. first 4 $A_i$ considered.

# Example: Small-PRESENT



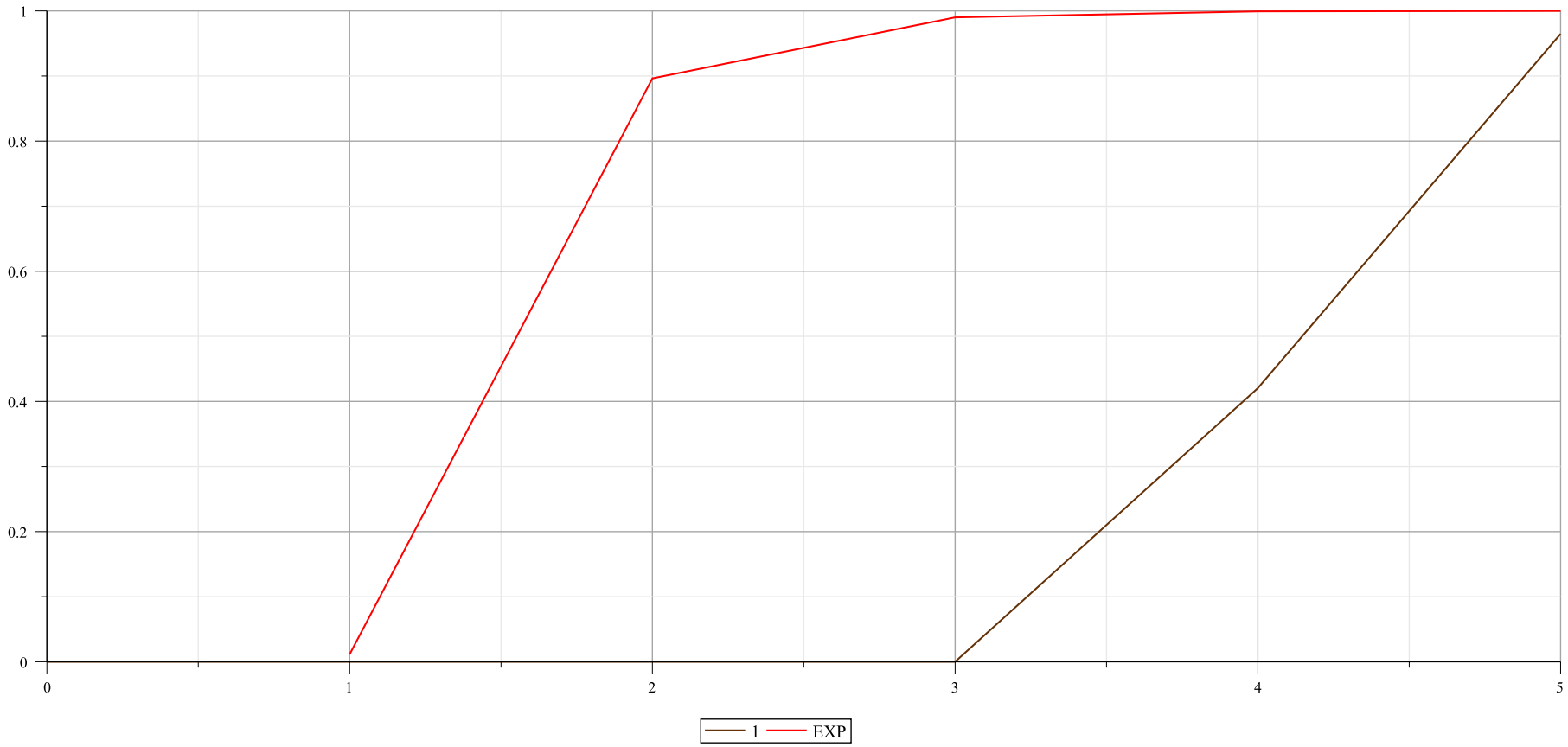

Experimental vs. first 3 $A_i$ considered.

# Example: Small-PRESENT



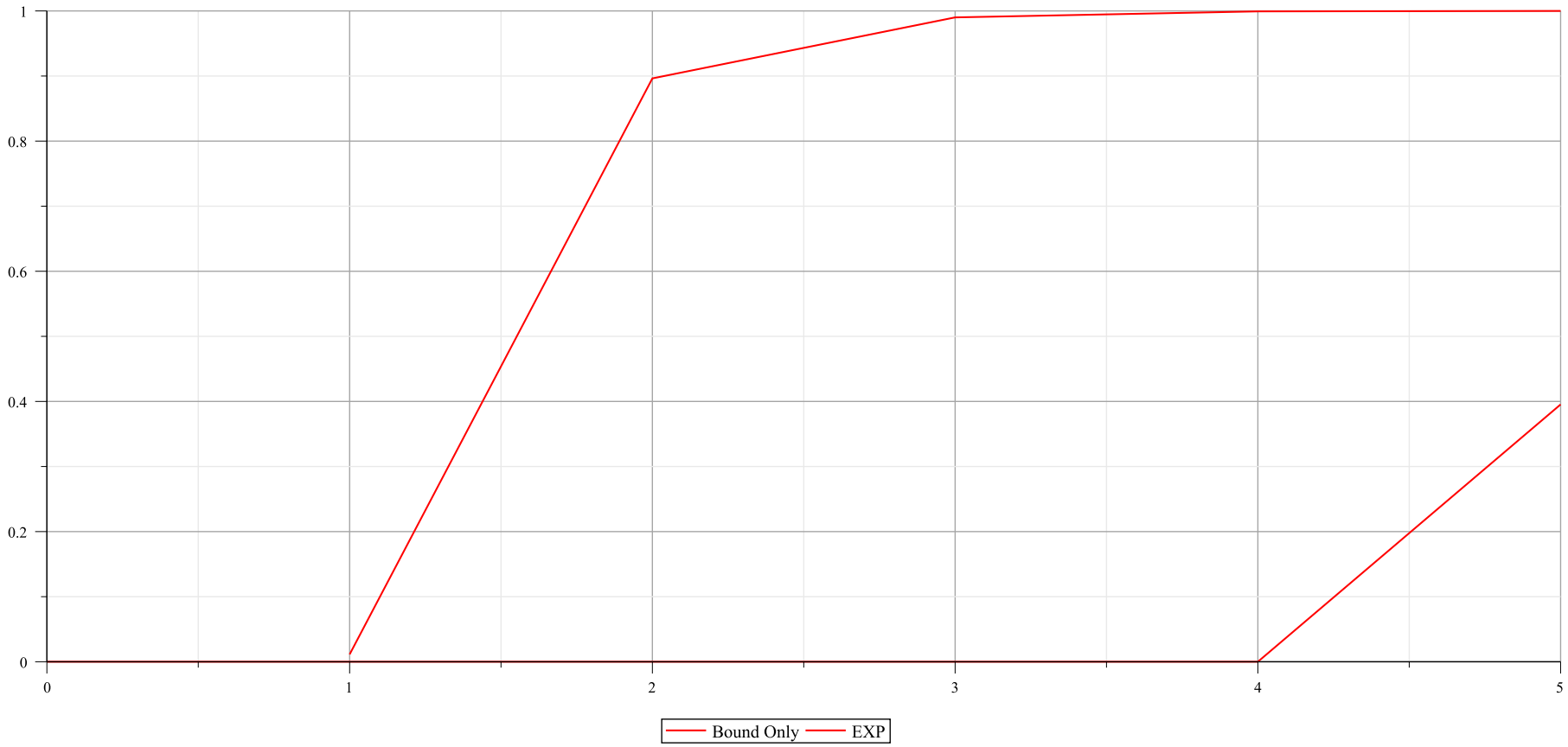

Experimental vs. first 2 $A_i$ considered.

# Example: Small-PRESENT




Experimental vs. first $A_i$ considered.

# Example: Small-PRESENT




Experimental vs. first bound only

# Outline

# Bound Only

Often: Only the bound is known.

**Question**

What can be said given the bound only?

**Theorem (Informal)**

*If the max. probability of a characteristic is $\leq 2^{-3n}$ then (with good probability) any characteristic is followed by at most one pair.*

# What Can Be Said? Examples

| algo | 1 | 2 | 3 |
|---|---|---|---|
| Grøstl-256 | 0 | 1 | 1 |
| PHOTON-256 | 1 | 1 | 1 |
| SPONGENT | 0 | 0.97 | 1 |

Lower bounds on the probability for at most $1, 2, 3$ pairs.

# The End

Thank you very much!