On the construction of Side-Channel Attack resilient S-boxes

Nikita Veshchikov

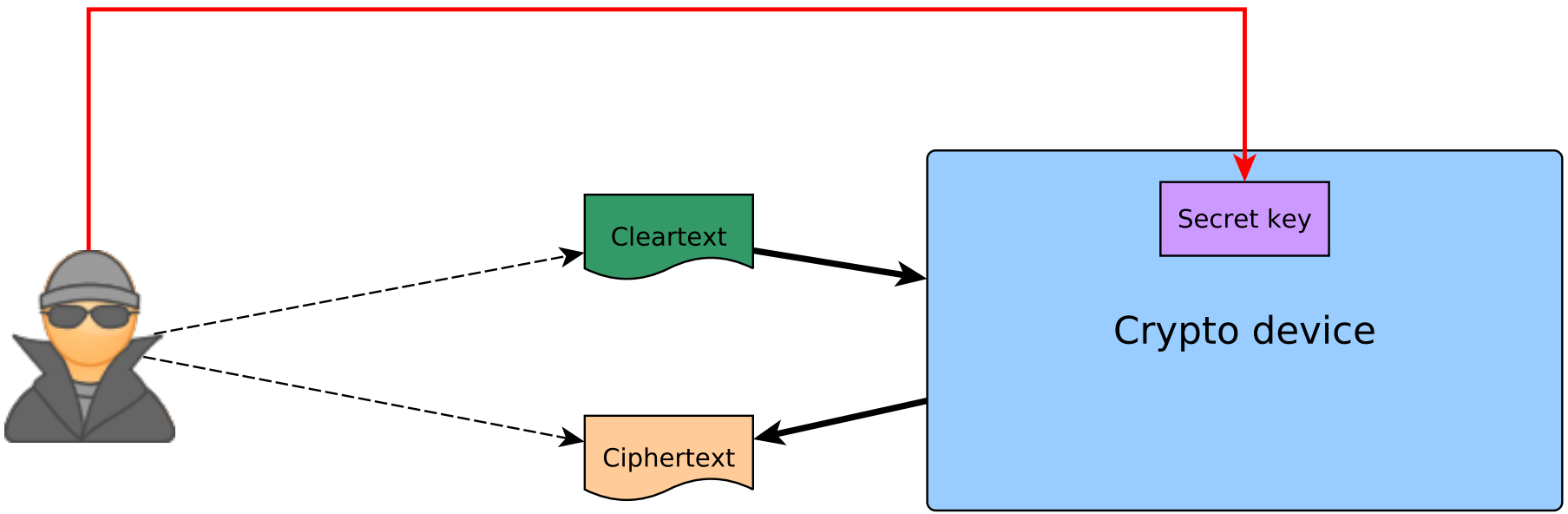
Collaboration with Liran Lerman, Stjepan Picek and Olivier Markowitch

Université Libre de Bruxelles, Belgium

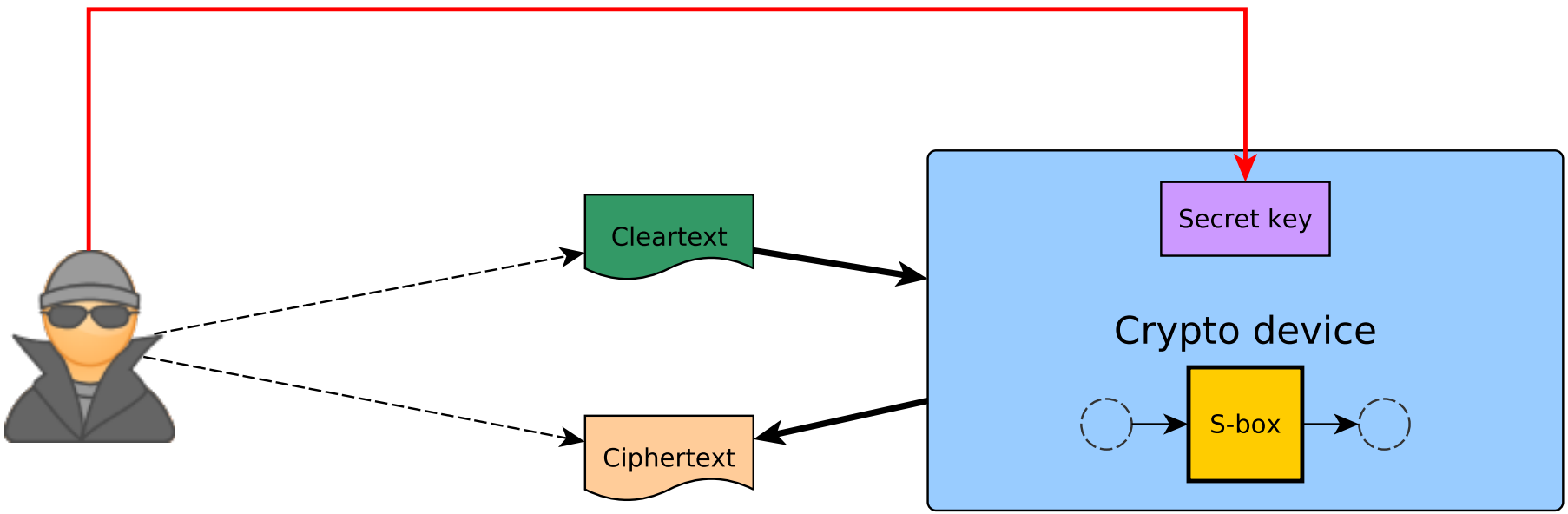
Paris, COSADE
13/04/2017

Intro

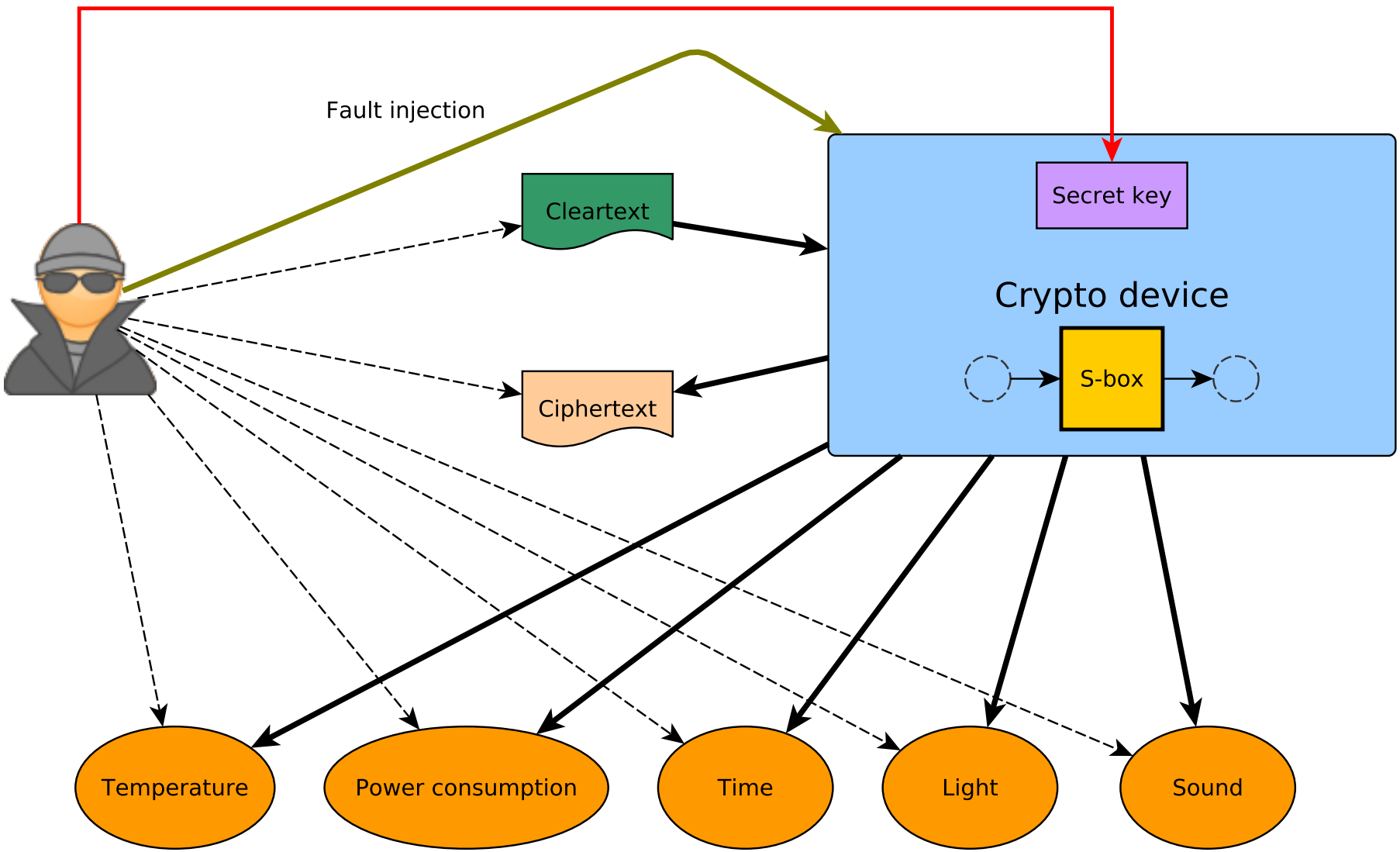
Classical cryptanalysis



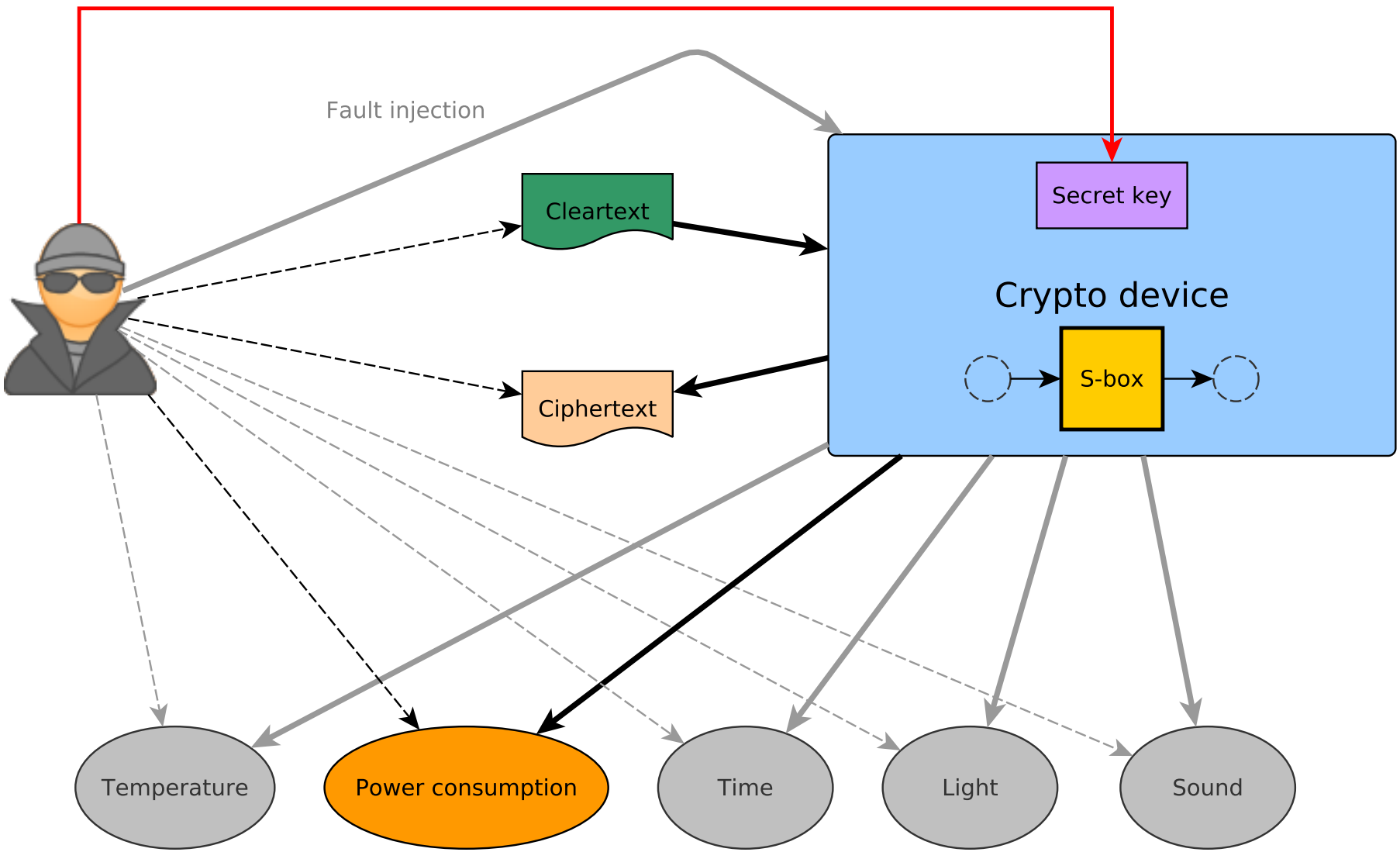
Designing a block cipher



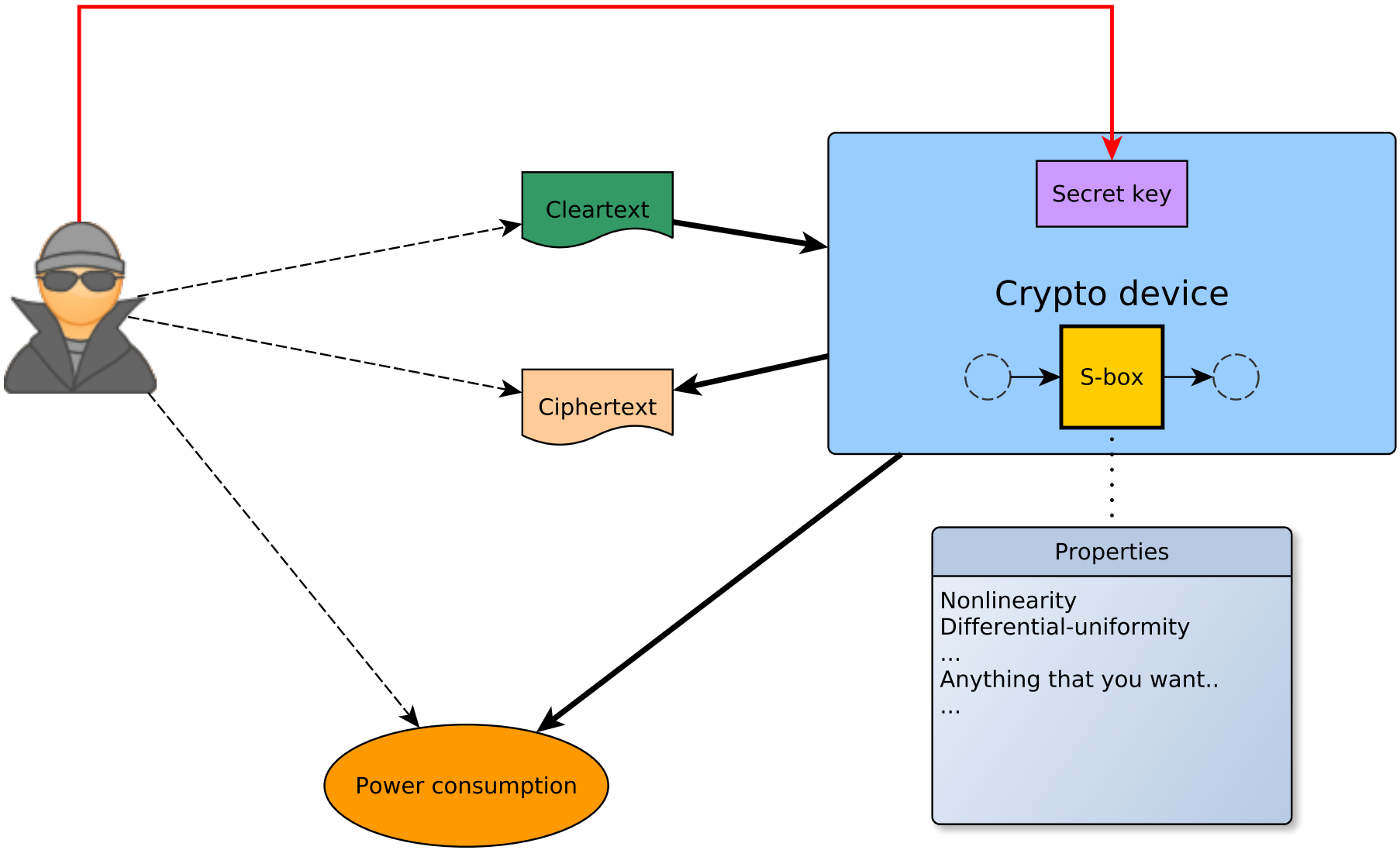
Side-channel attacks



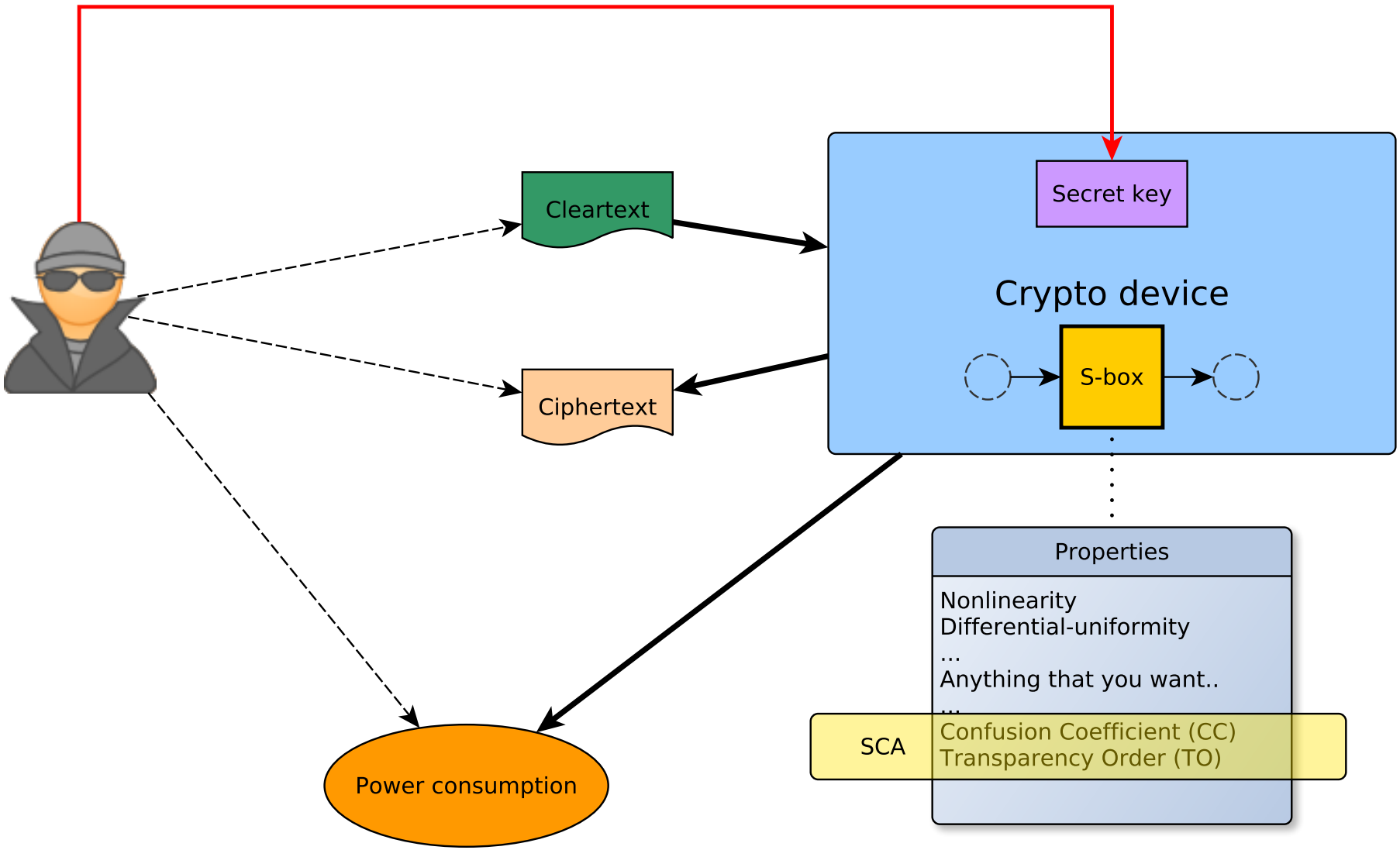
Power analysis



Properties of S-boxes



Properties of S-boxes: SCA



Let's build S-boxes!

Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes*

Stjepan Picek[1,3], Kostas Papagiannopoulos[1], Barış Ege[1],
Lejla Batina[1,2], and Domagoj Jakobovic[3]

[1]ICIS - Digital Security Group, Radboud University Nijmegen, The Netherlands
[2]ESAT/COSIC, KU Leuven, Belgium
[3]Faculty of Electrical Engineering and Computing
University of Zagreb, Croatia

Abstract. When studying the DPA resistance of S-boxes, the research community is divided in their opinions on what properties should be considered. So far, there exist only a few properties that aim at expressing the resilience of S-boxes to side-channel attacks. Recently, the confusion coefficient property was defined with the intention to characterize the resistance of an S-box. However, there exist no experimental results or methods for creating S-boxes with a "good" confusion coefficient property. In this paper, we employ a novel heuristic technique to generate S-boxes with "better" values of the confusion coefficient in terms of improving their side-channel resistance. We conduct extensive side-channel analysis and detect S-boxes that exhibit previously unseen behavior. For the 4×4 size we find S-boxes that belong to optimal classes, but they exhibit linear behavior when running a CPA attack, therefore preventing an attacker from achieving 100% success rate on recovering the key.

Let's build S-boxes!

Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes*

Stjepan Picek[1,3], Kostas Papagiannopoulos[1], Barış Ege[1],
Lejla Batina[1,2], and Domagoj Jakobovic[3]

[1]ICIS - Digital Security G
[2]ESA
[3]Faculty of
U

Abstract. When stu
community is divided
sidered. So far, there
the resilience of S-box
coefficient property w
resistance of an S-box
methods for creating
erty. In this paper, w
S-boxes with "better"
proving their side-cha
analysis and detect S-
the 4 × 4 size we find
exhibit linear behavio
an attacker from achi

Modified Transparency Order Property: Solution or Just Another Attempt

Stjepan Picek[1,2], Bodhisatwa Mazumdar[3],
Debdeep Mukhopadhyay[4], and Lejla Batina[2,5]

[1] Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia
[2] ICIS - Digital Security Group, Radboud University Nijmegen, The Netherlands
[3] New York University Abu Dhabi, Abu Dhabi
[4] Department of Computer Science and Engineering,
IIT Kharagpur, Kharagpur, India
[5] ESAT/COSIC, KU Leuven, Belgium

Abstract. S-boxes are usual targets of side-channel attacks and it is an open problem to develop design techniques for S-boxes with improved DPA resistance. One result along that line is the transparency order, a property that attempts to characterize the resilience of S-boxes against DPA attacks. Recently, it was shown there exist flaws with the original definition of transparency, which resulted in the new definition - modified transparency order. This paper develops techniques for constructions using the modified transparency as a guiding metric. For the 4 × 4 size, we significantly improve modified transparency order while remaining in the optimal classes. Experimental results are provided assuming a noisy HW leakage model to show the proposed S-boxes are more resistant than the original one of the PRESENT algorithm. We conclude with reports on 4 × 4 and 8 × 8 S-boxes where the results indicate that the modified transparency order could be a more useful metric than the transparency order. However, both measures are far from definitive solution on how to improve the DPA resistance.

Let's compare S-boxes!

Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes*

Stjepan Picek[1,3], Kostas Papagiannopoulos[1], Barış Ege[1],
Lejla Batina[1,2], and Domagoj Jakobovic[3]

[1]ICIS - Digital Security G
[2]ESA
[3]Faculty of
U

Abstract. When stu
community is divided
sidered. So far, there
the resilience of S-box
coefficient property w
resistance of an S-box
methods for creating
erty. In this paper, w
S-boxes with "better"
proving their side-cha
analysis and detect S-
the 4 × 4 size we find
exhibit linear behavio
an attacker from achi

Modified Transparency Order Property: Solution or Just Another Attempt

Stjepan Picek[1,2], Bodhisatwa Mazumdar[3],
Debdeep Mukhopadhyay[4], and Lejla Batina[2,5]

[1] Facu
[2] ICIS

Comparing Sboxes of Ciphers from the Perspective of Side-Channel Attacks

Liran Lerman and Olivier Markowitch and Nikita Veshchikov
Quality and Security of Information Systems,
Université libre de Bruxelles, Belgium
{liran.lerman, olivier.markowitch, nikita.veshchikov}@ulb.ac.be

***Abstract*—Side-channel attacks exploit physical characteristics of implementations of cryptographic algorithms in order to extract sensitive information such as the secret key. These physical attacks are among the most powerful attacks against real-world crypto-systems. This paper analyses the non-linear part (called Sboxes) of ciphers, which is often targeted by implementation attacks. We analyse Sboxes of several candidates that were submitted to the competition on authenticated encryption (CAESAR) as well as several other ciphers. We compare theoretical metrics with results from simulations and with real experiments. In this paper, we demonstrate that, in some contexts, the theoretical**

the resistance of cryptographic primitives against side-channel attacks. The serious consequences of such result is that (1) the evaluation laboratories of cryptographic implementations still require to apply side-channel attacks in order to discover the security level provided by cryptographic devices, and (2) the new cryptographic primitives taking into account these evaluation metrics during the design process may be compromised in front of side-channel attacks.

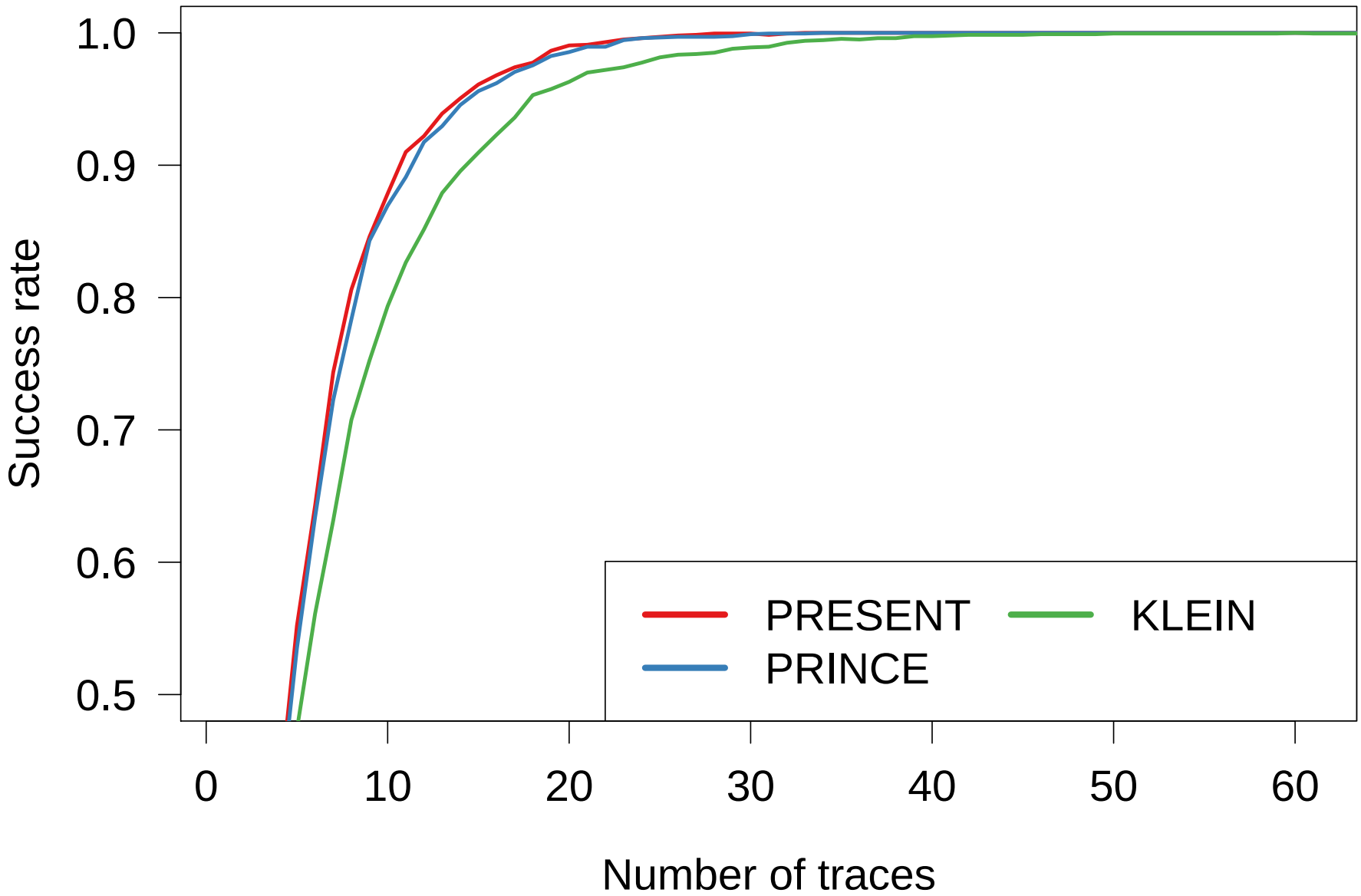
The rest of the paper is organised as follows. Section II contains preliminary notions on physical attacks and on theo-

New S-boxes!

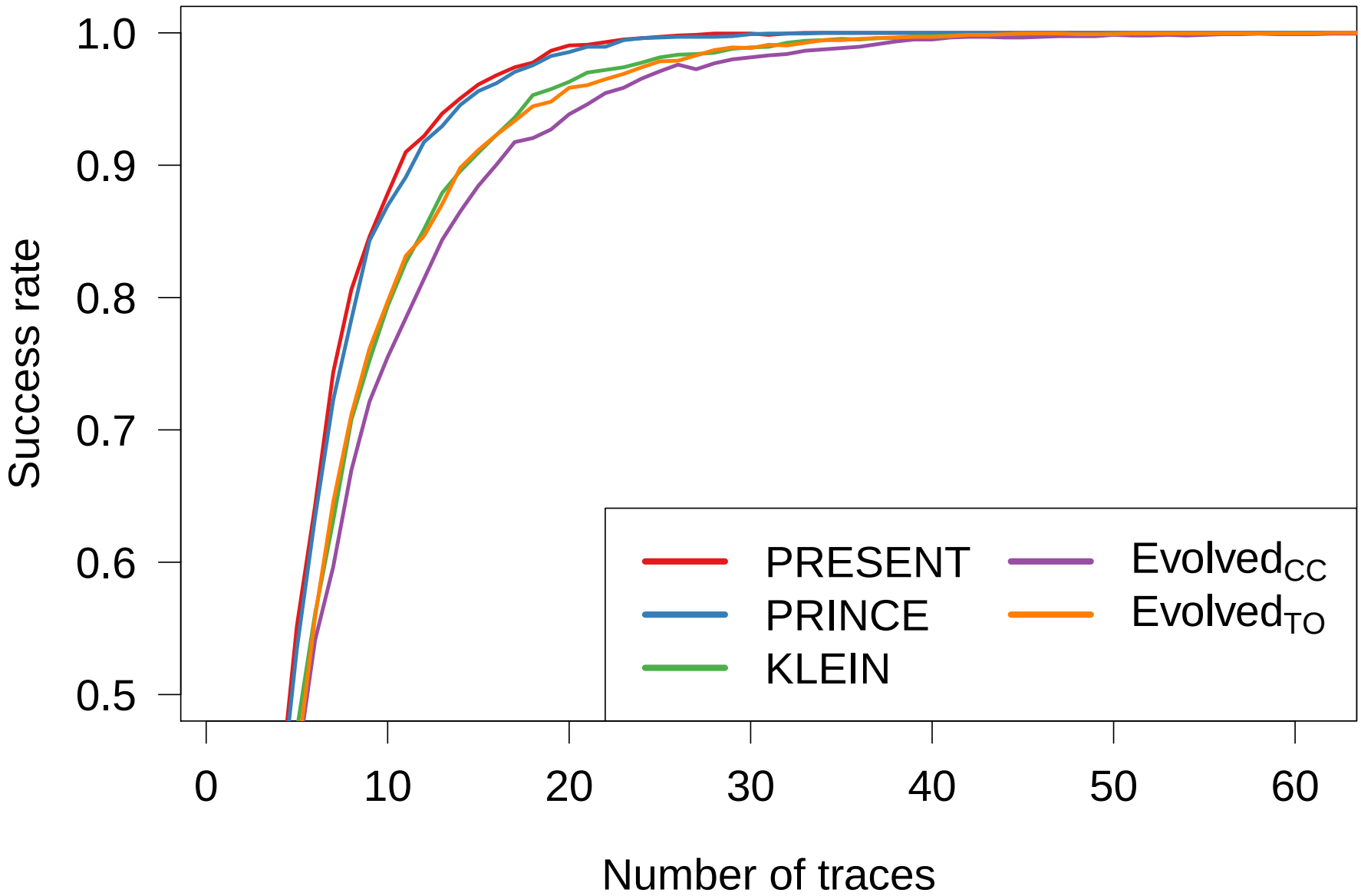
Design scope

- Genetic algorithms
- Success rate of CPA (HW) & TA (ATmega328)
- 4×4 and 5×5 S-boxes

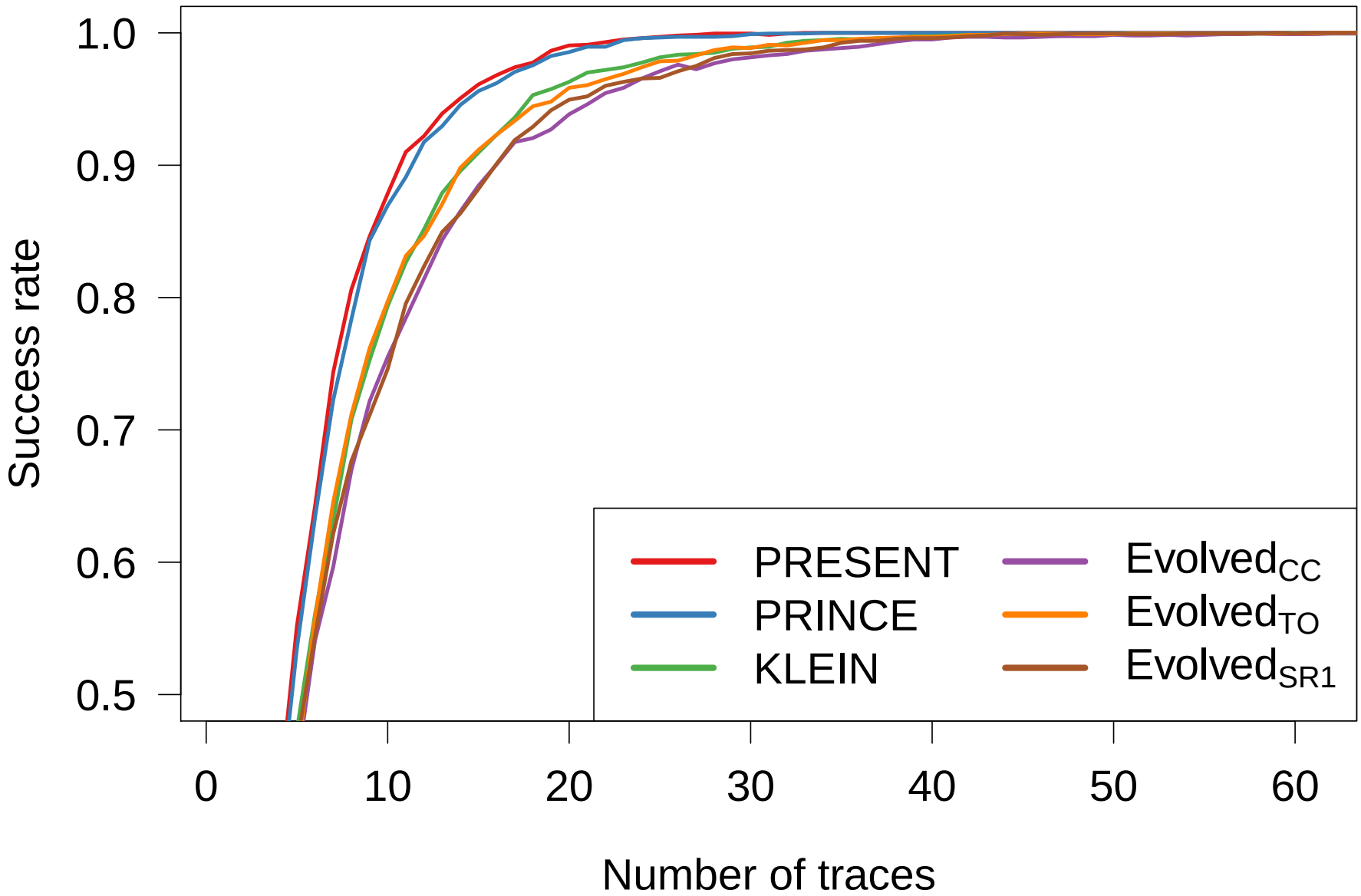
Success rates of CPA against S-boxes



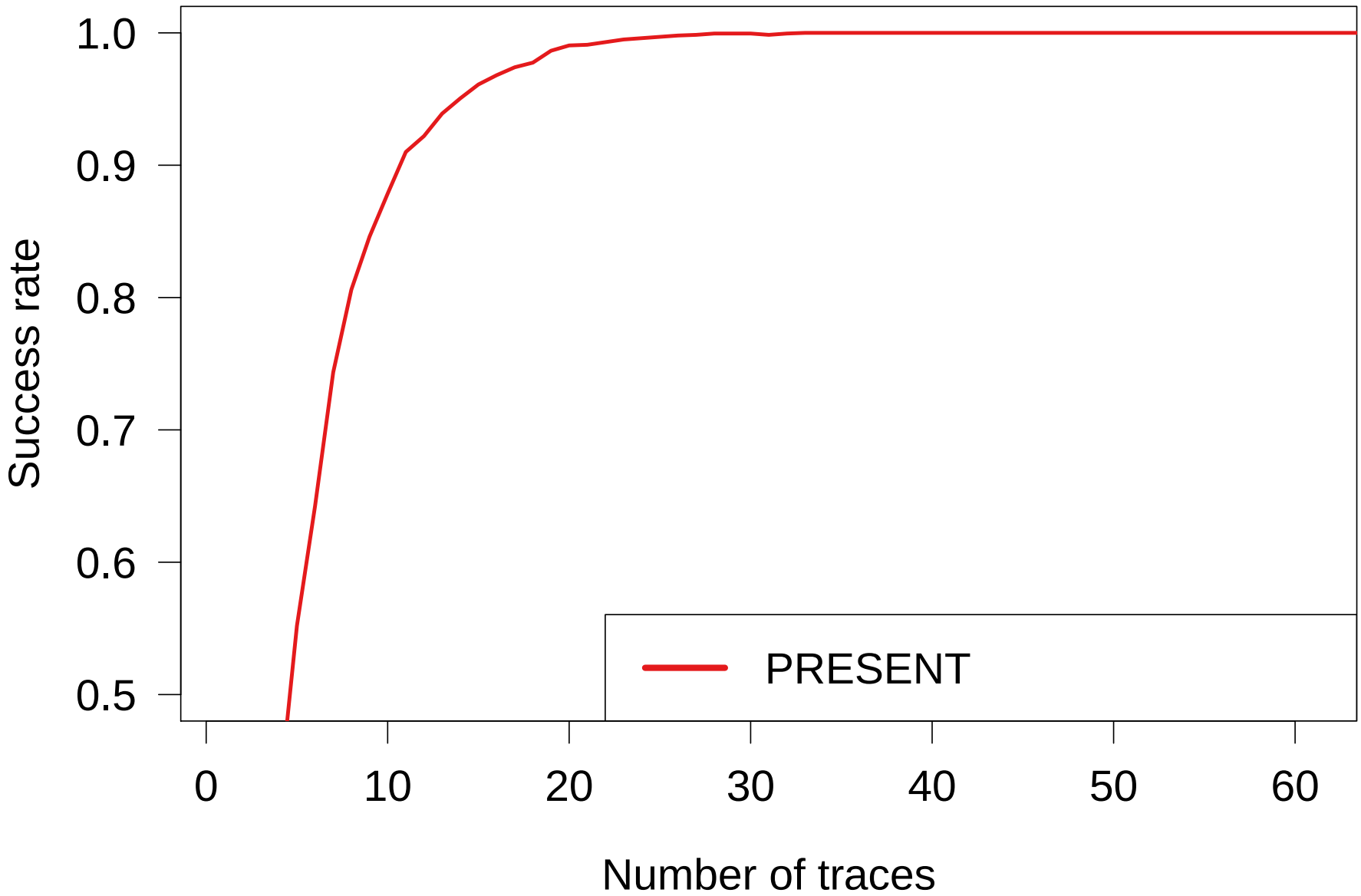
Success rates of CPA against S-boxes II



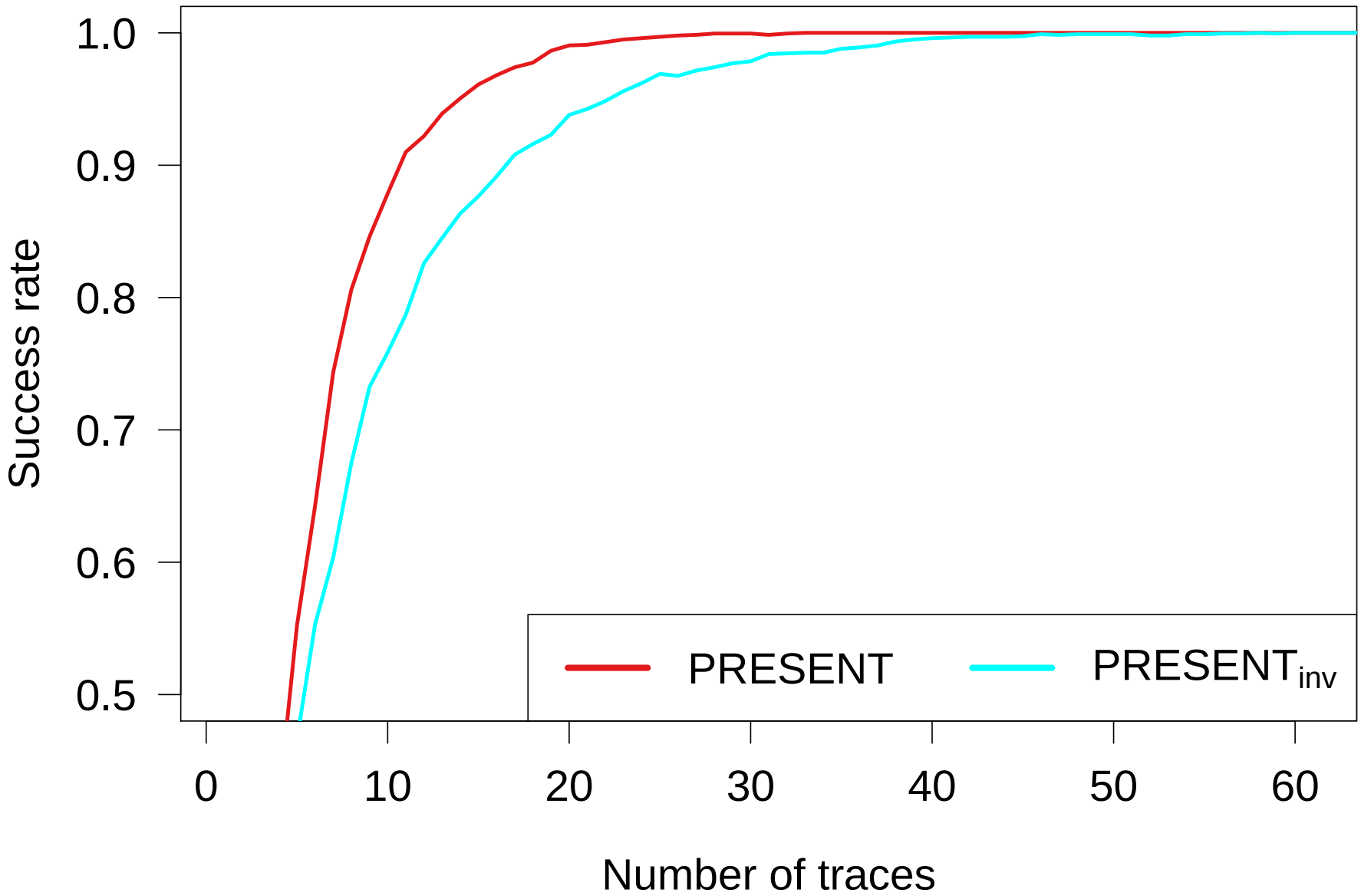
Success rate: here is a new one!



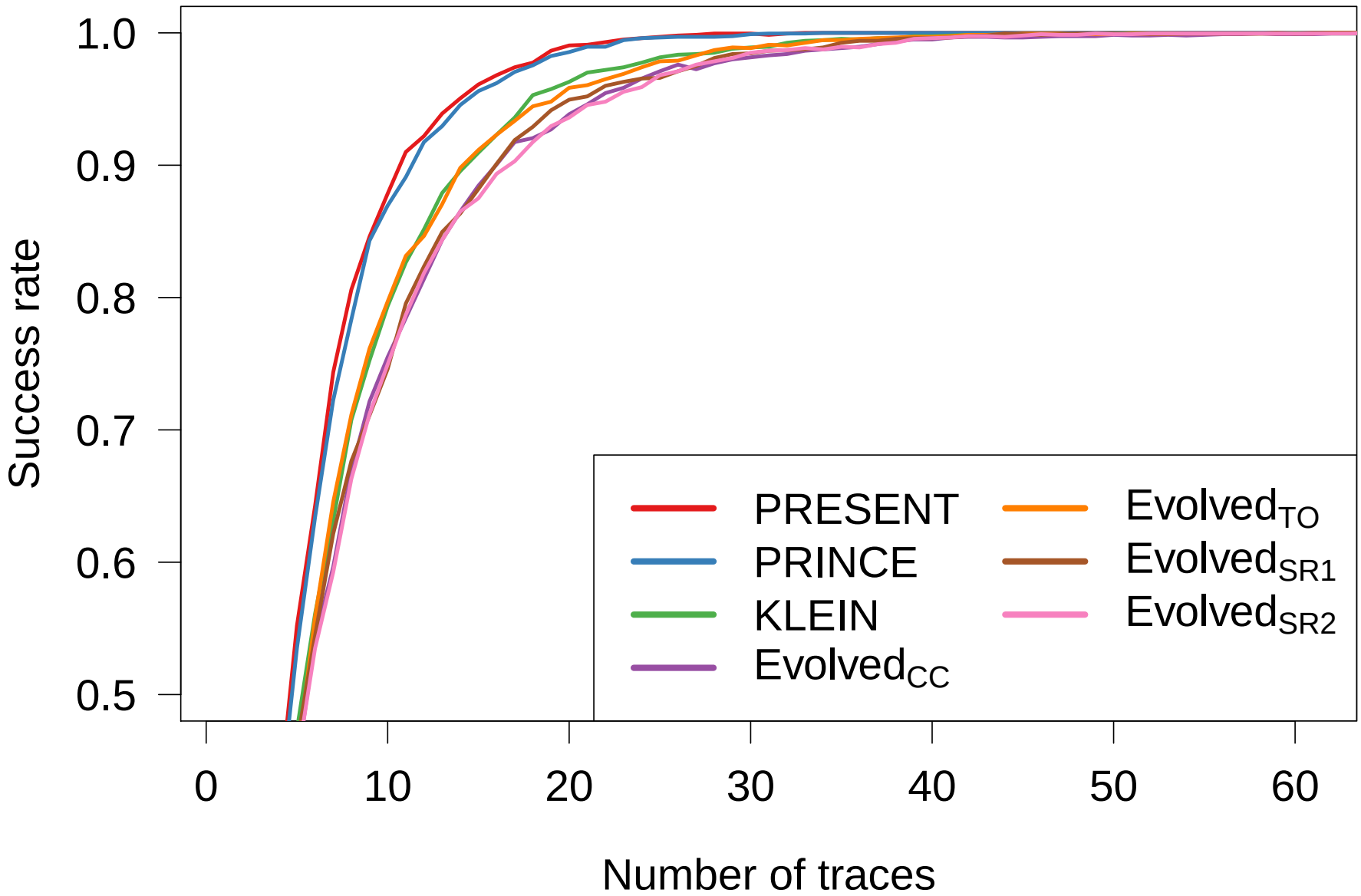
Success rate: Present S-box



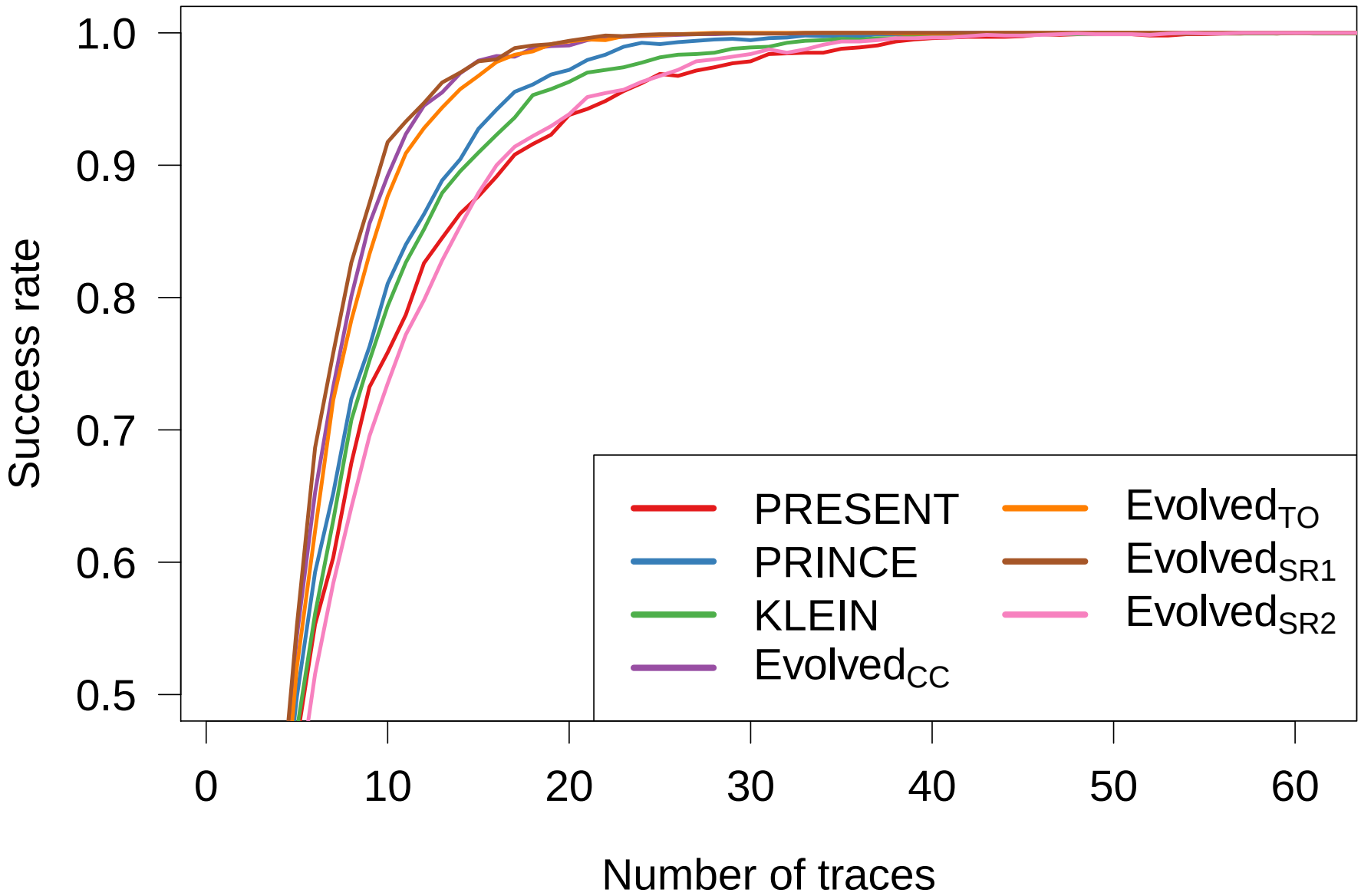
Forward vs. Inverse



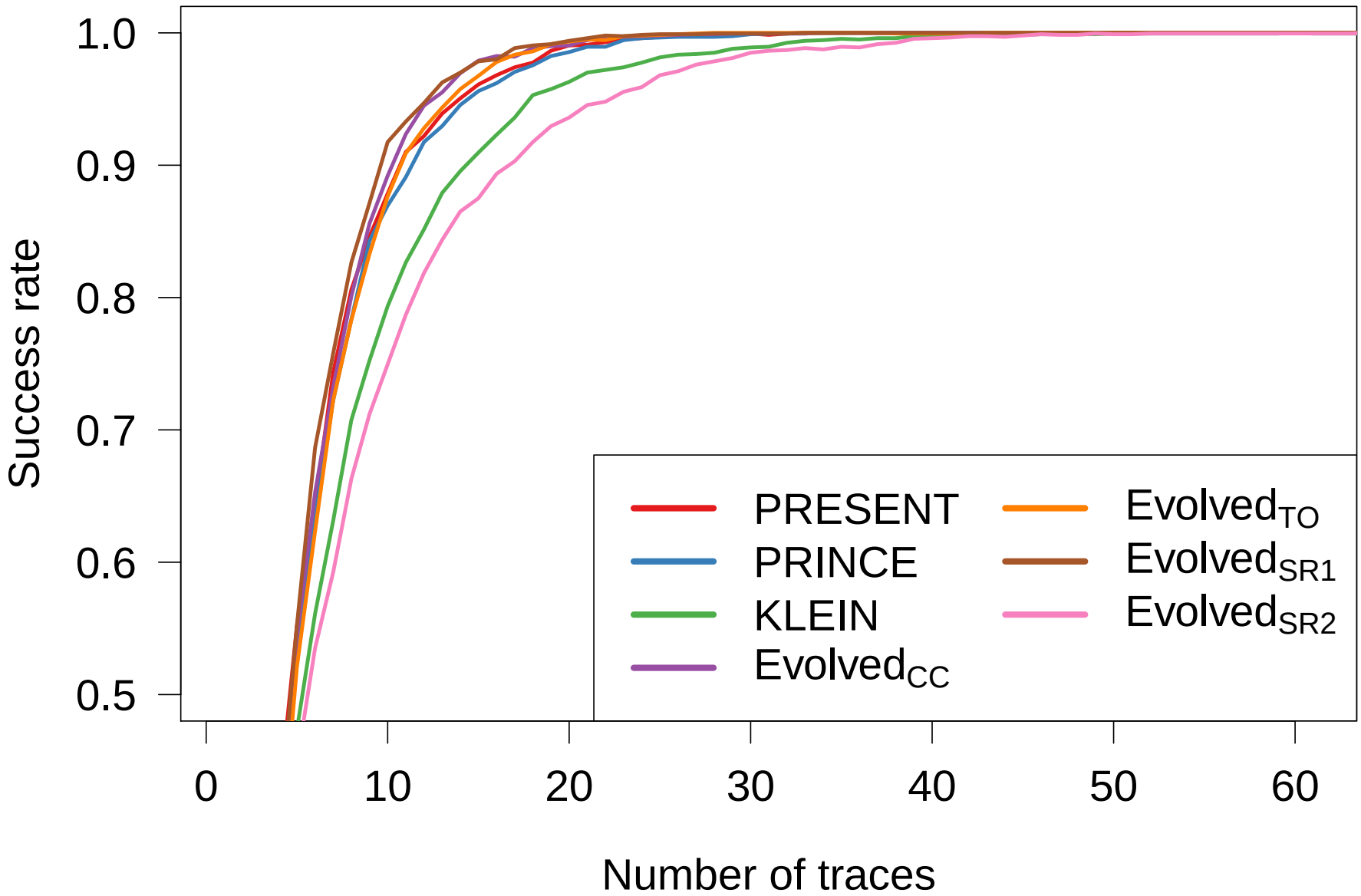
Success rates for S-boxes



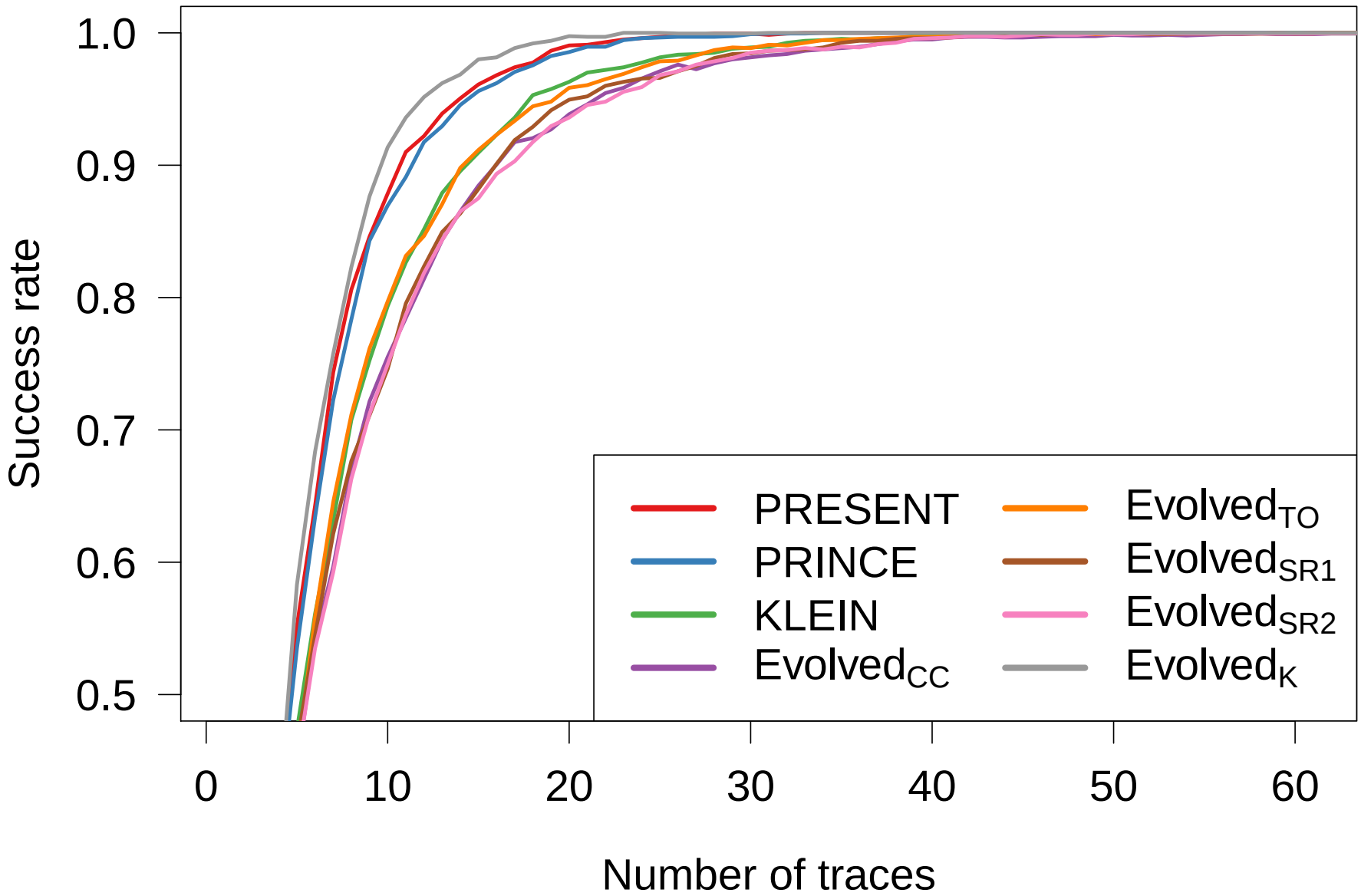
Success rates for S-boxes^{-1}



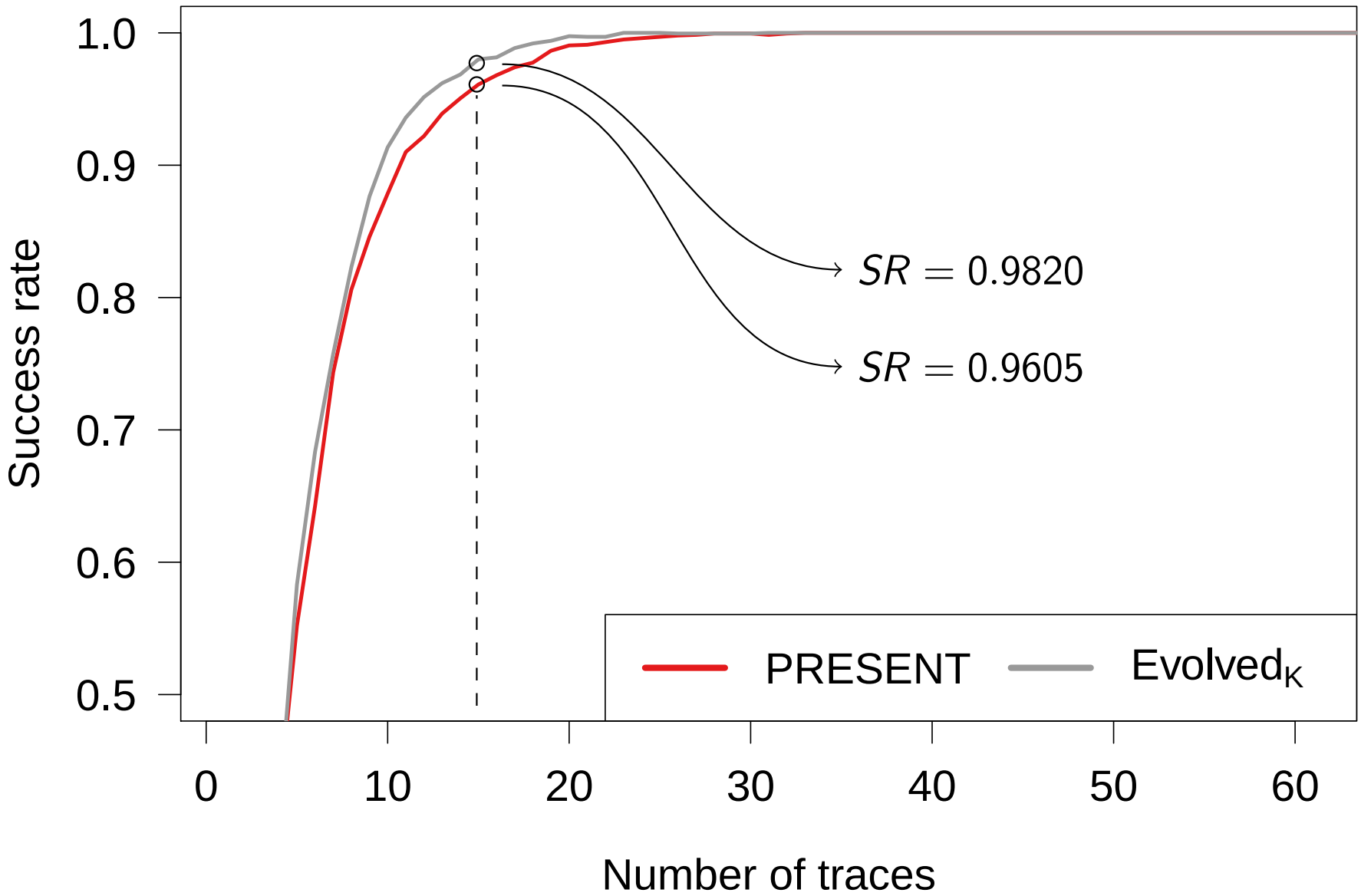
Max of success rates



Kleptographic S-box



How good is it?



Success rate of a full attack

One nibble of 4 bits

- Present : $SR = 0.9605$
- Evolved$K$: $SR = 0.9820$

Assmuing independent nibbles..

80-bit key

- Present : $SR = (0.9605)^{20} \approx 0.45$
- Evolved$K$: $SR = (0.9820)^{20} \approx 0.70$

128-bit key

- Present : $SR = (0.9605)^{32} \approx 0.28$
- Evolved$K$: $SR = (0.9820)^{32} \approx 0.56$

Success rate of a full attack

One nibble of 4 bits

- Present : $SR = 0.9605$
- Evolved$K$: $SR = 0.9820$

Assmuing independent nibbles..

80-bit key

- Present : $SR = (0.9605)^{20} \approx 0.45$
- Evolved$K$: $SR = (0.9820)^{20} \approx 0.70$

128-bit key

- Present : $SR = (0.9605)^{32} \approx 0.28$
- Evolved$K$: $SR = (0.9820)^{32} \approx 0.56$

Success rate of a full attack

One nibble of 4 bits

- Present : $SR = 0.9605$
- Evolved$K$: $SR = 0.9820$

Assmuing independent nibbles..

80-bit key

- Present : $SR = (0.9605)^{20} \approx 0.45$
- Evolved$K$: $SR = (0.9820)^{20} \approx 0.70$

128-bit key

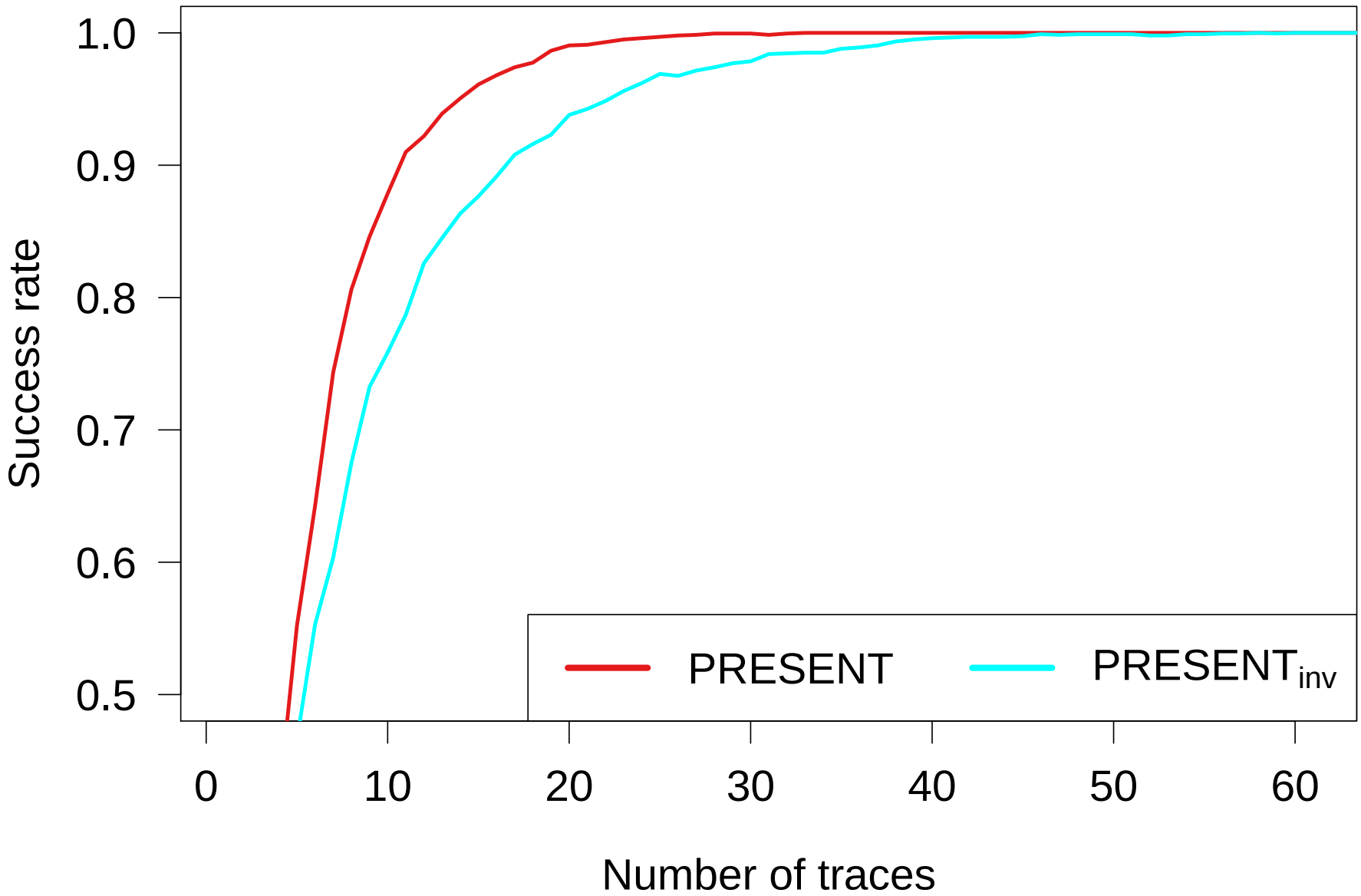
- Present : $SR = (0.9605)^{32} \approx 0.28$
- Evolved$K$: $SR = (0.9820)^{32} \approx 0.56$

Conclusions & Future works

Conclusion I

Now you have a new way of generating S-boxes!

Conclusion II



What's next?

- More properties!
- More leakage models!
- "Easy-to-mask" S-boxes?

Warning!
Kleptographic S-box!

```
0x0,0xF,0x1,0x9,0xB,0x5,0x8,0x2
0xE,0x3,0xC,0x6,0xD,0x4,0xA,0x7
```

If you see it in a cryptographic primitive immediately contact Nikita.Veshchikov@ulb.ac.be