Experimental algebraic differential cryptanalysis of SPN

Pavol Zajac[1] Alena Bednáriková

Institute of Computer Science and Mathematics
Slovak University of Technology

pavol.zajac@stuba.sk

Central European Conference on Cryptology 2020

[1] Supported by grant VEGA 1/0159/17.

Outline

Algebraic cryptanalysis overview

Algebraic cryptanalysis: compute the secret key k from equation

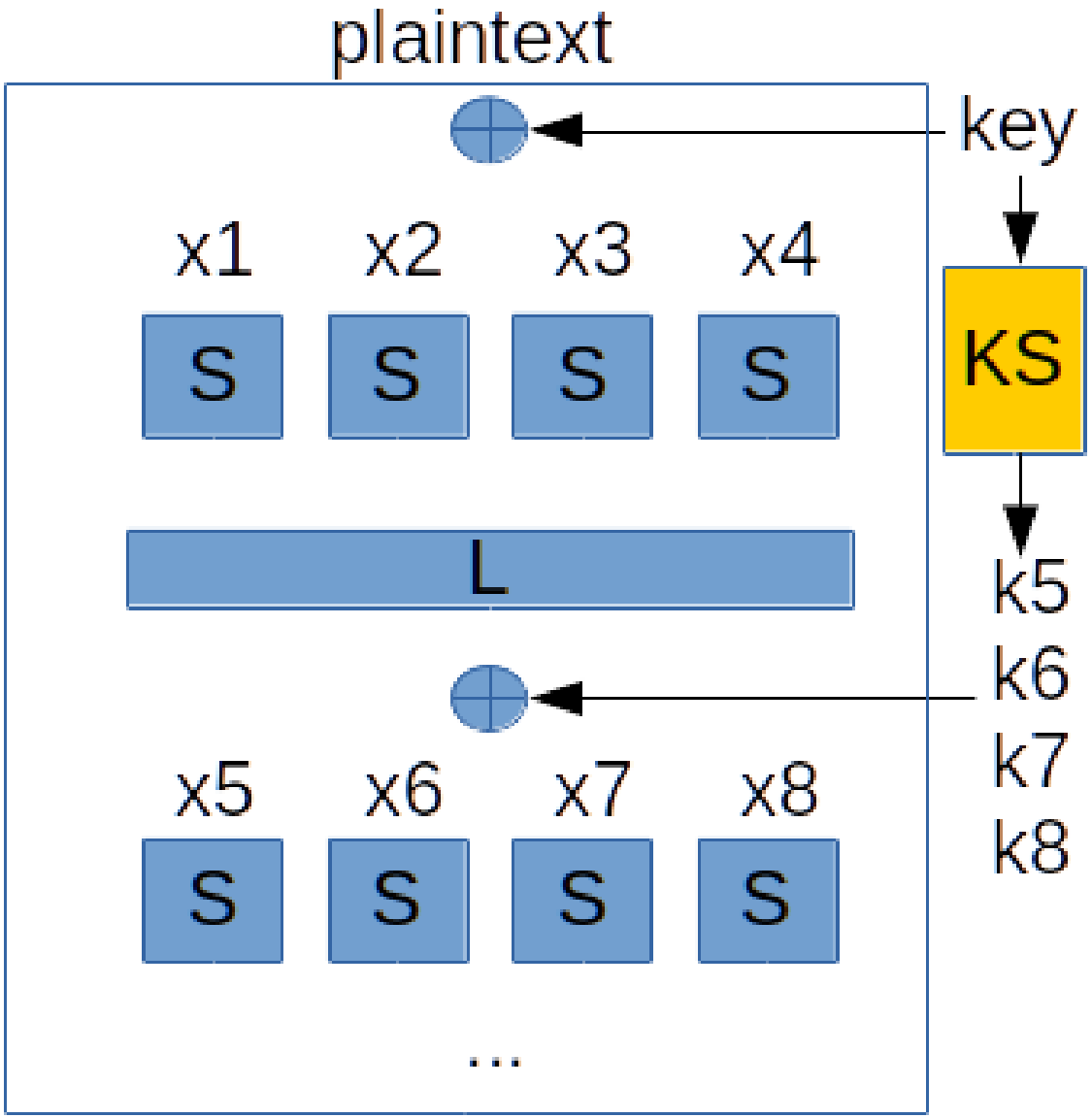
$$Enc(p, k) = c$$

1. Rewrite encryption as a system of equations.
2. Solve with a solver - NP hard in general.

Our experimental algebraic cryptanalysis

- We focus on a simple cipher model: Substitution Permutation Network (SPN)
- Equations are represented as Boolean predicates in CNF
- Solver: CryptoMiniSAT in SAGE

Substitution Permutation Network



SPN algebraic model

Unknowns:

- key bits,
- S-box inputs and outputs.

Predicates:

- S-boxes: $P_1(x, y)$ is true, iff $y = S(x)$
- Linear parts: $P_2(x, y, k)$ is true, iff $x \oplus k = y$
- Linear parts (2): $P_3(x, y)$ is true, iff $x = y$

S-box predicate

Predicate P_1 is based on the truth table defined by S-box:

x	y	$y = S(x)$
0000	0000	false
0000	0001	true
0000	0010	false
⋮	⋮	⋮

(0=false, 1=true)

$$(x_1 \vee x_2 \vee x_3 \vee x_4 \vee y_1 \vee y_2 \vee y_3 \vee y_4) \wedge$$
$$(x_1 \vee x_2 \vee x_3 \vee x_4 \vee y_1 \vee y_2 \vee \neg y_3 \vee y_4) \wedge \ldots$$

Multiple P-C pairs

Using multiple P-C pairs:

$$Enc(p_i, k) = c_i$$

Linear growth of system size with number of P-C pairs — slows down solvers.

Differential cryptanalysis

- Large number of P-C pairs: we use statistical properties of the whole set of P-C pairs.
- Differential cryptanalysis:
  1. model how differences are spread during encryption,
  2. find characteristic with high differential probability p,
  3. exploit the characteristic (using the set of P-C pairs).

Algebraic differential cryptanalysis

- Combination of differential and algebraic attacks.
- Basic method:
  1. prepare equations for a P-C pair:

$$Enc(p_1, k) = c_1 \wedge Enc(p_2, k) = c_2$$

  2. add linear equations corresponding to characteristic with probability p:

$$p_{1,1} \oplus p_{2,1} = \delta_1 \wedge \ldots$$

  3. Try to solve system for each P-C pair: gives solution with probability p.

Our new method

Main idea: Instead of using 2 systems of equations for both P-C pairs, and a set of linear equations, we use modified system for just one P-C pair.

$$Enc'(p_1, k) = c_1$$

Our new method

Main idea: Instead of using 2 systems of equations for both P-C pairs, and a set of linear equations, we use modified system for just one P-C pair.

$$Enc'(p_1, k) = c_1$$

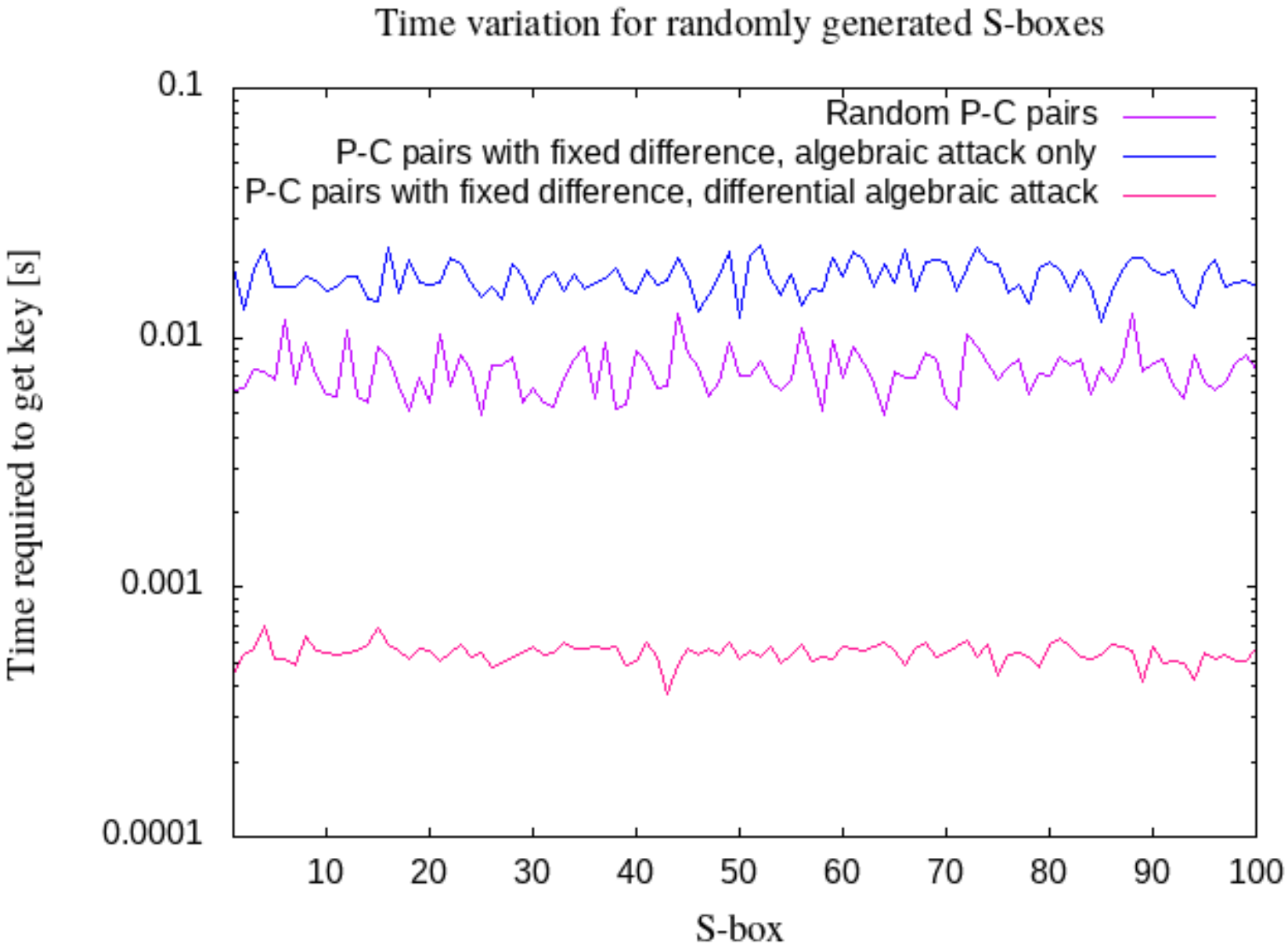
In Enc', we change S-box predicate:

$$P'_1(x, y) = \text{true iff } y = S(x) \wedge \Delta y = S(x \oplus \Delta x) \oplus S(x)$$

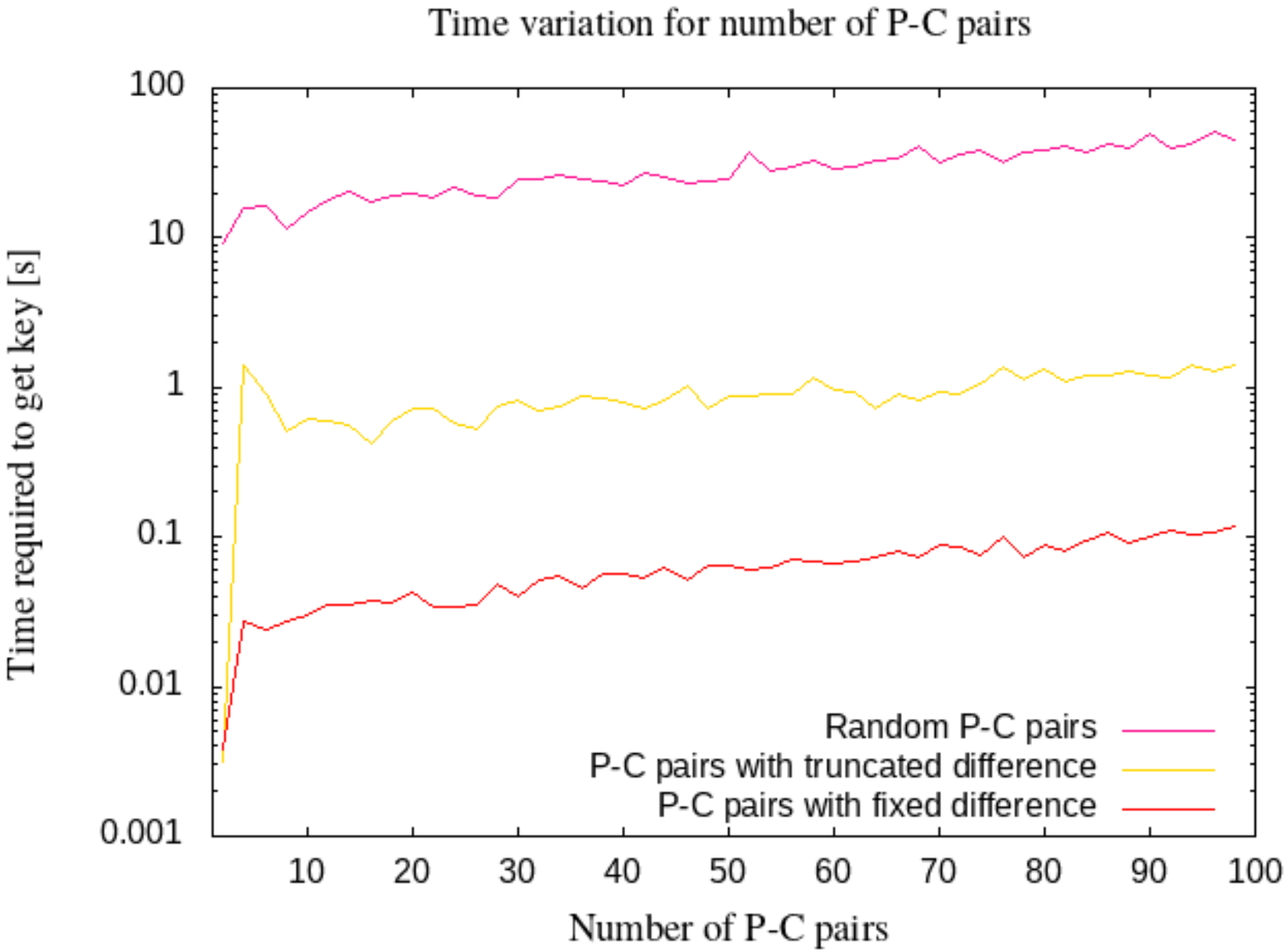
Modified S-box representation

X	Y	$\Delta X = 1011$	$\Delta Y = 0010$
		X'	Y'
0000	1110	1011	1100
0001	0100	1010	0110
0010	1101	1001	1111
0011	0001	1000	0011
0100	0010	1111	0000
0101	1111	1110	1101
0110	1011	1101	1001
0111	1000	1100	1010
1000	0011	0011	0001
1001	1010	0010	1000
1010	0110	0001	0100
1011	1100	0000	1110
1100	0101	0111	0111
1101	1001	0110	1011

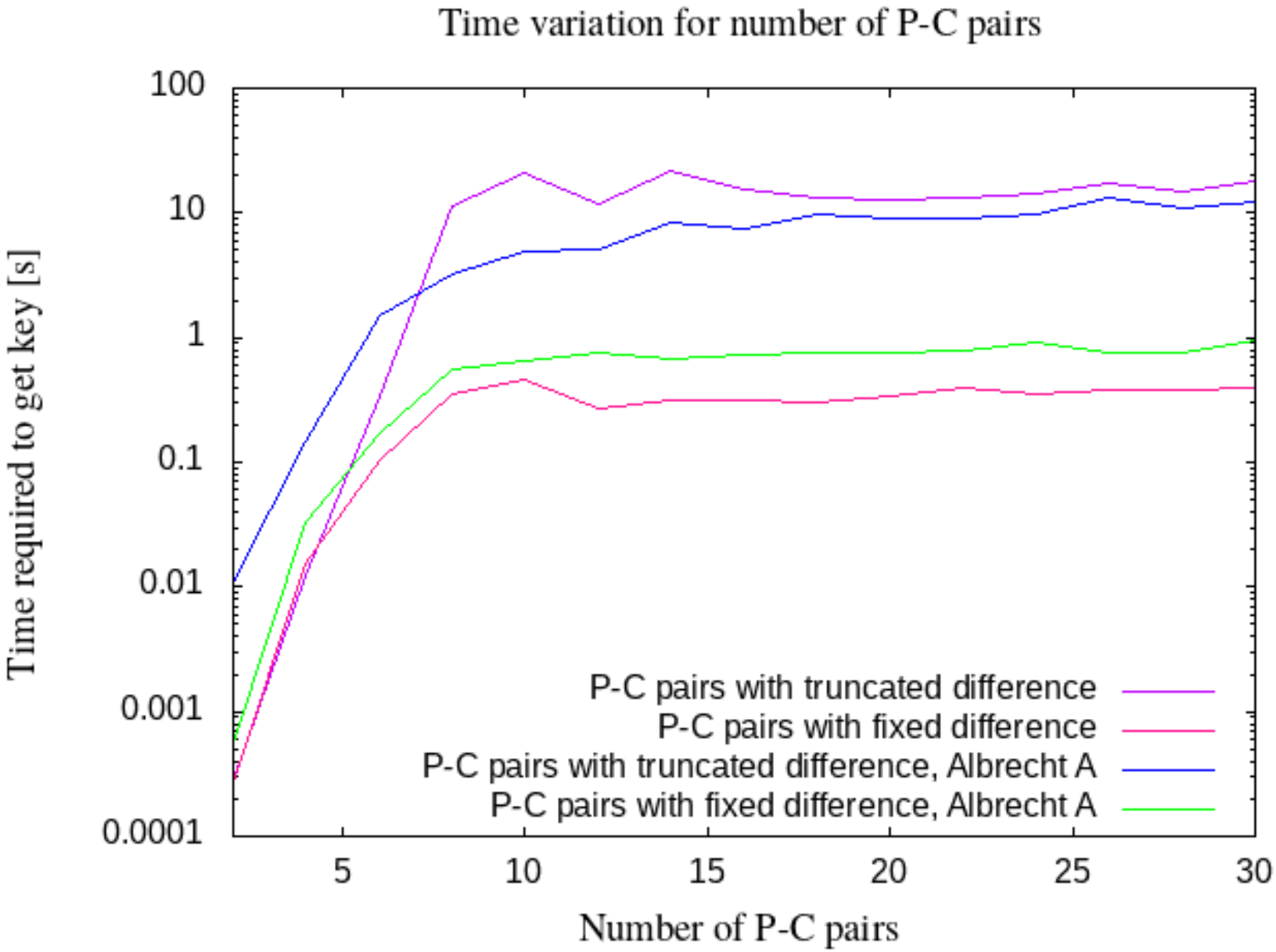
Experimental results



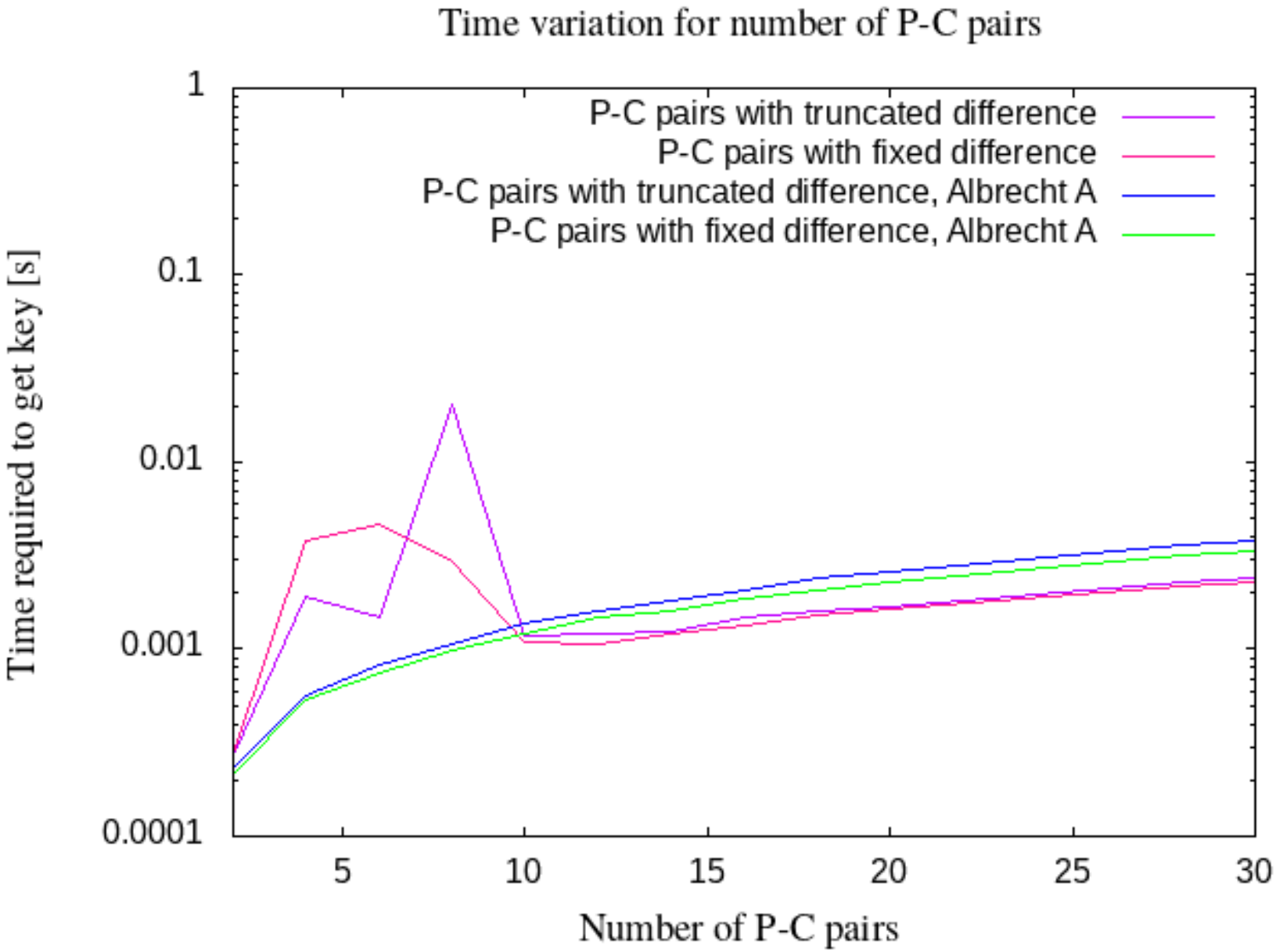
Experimental results



Experimental results



Experimental results



Total time to solve

When taking probability of the success under consideration:

P-C pairs	Algebraic [s]	Alg.-Truncated Diff. [s]	Alg.-Dif. [s]
2	9.3	0.1	2.5
4	15.6	96.4	1991.0
4*	15.6	1.3	5.1

* Hypothetic situation, if we could identify two sets of P-C pairs with the same probability as one set.

Summary

- We can model P-C pair with expected difference with an equation system with a single P-C pair and modified S-box equations.
- The new representation can speed up algebraic differential cryptanalysis.
- Open question: Is it possible to distinguish between a set with a valid difference and a set with no valid difference?