Rump Session 2016

How to (Correctly) Invoke Wagner

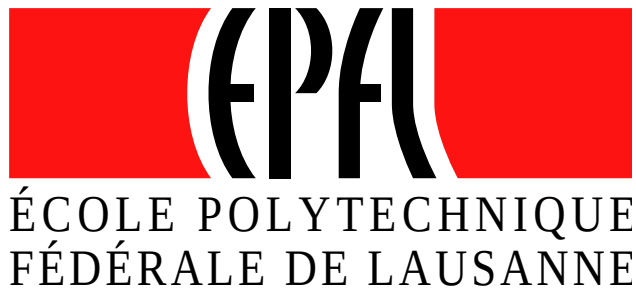
Sonia Bogos; Serge Vaudenay

EPFL

How to (Correctly) Invoke ~~Mozart~~ Wagner

New Results on LPN Solvers

Sonia Bogos and Serge Vaudenay

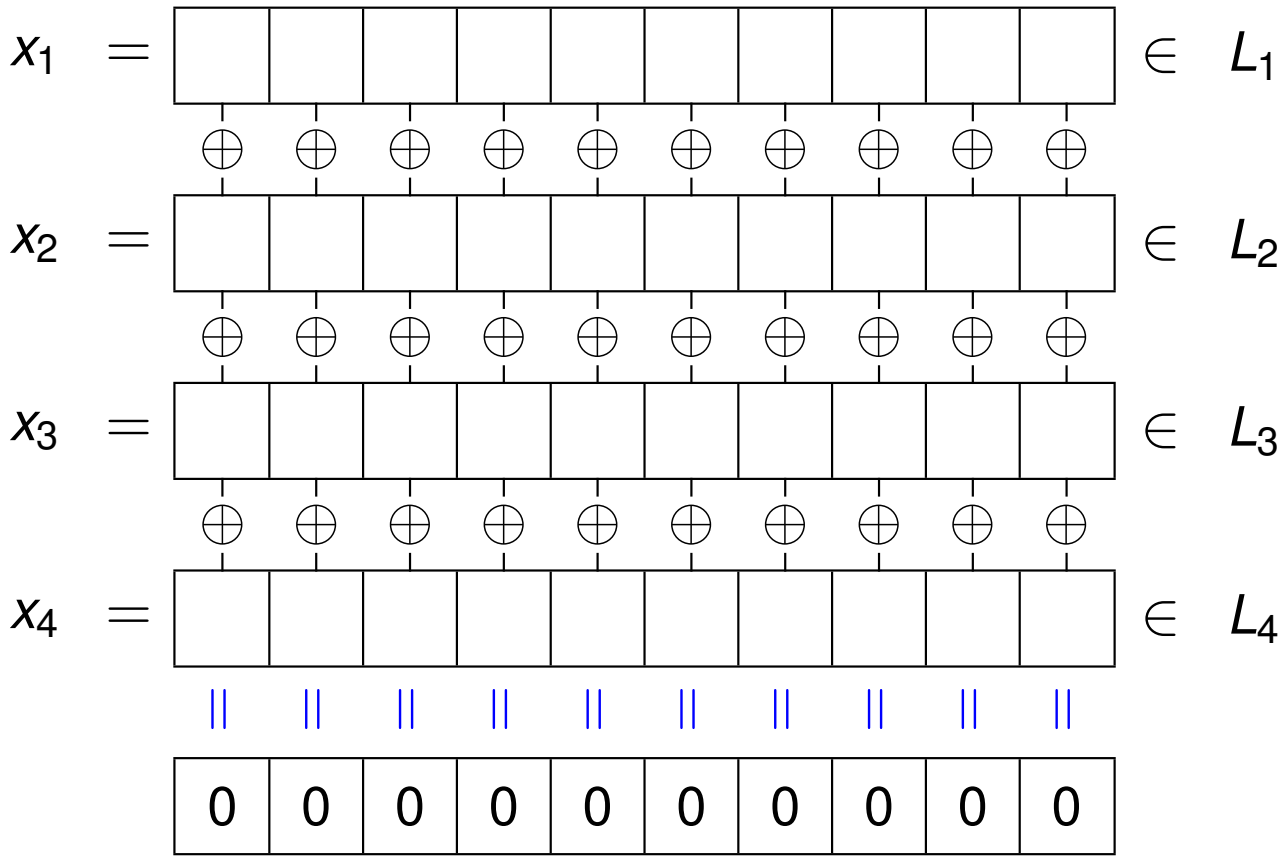


http://lasec.epfl.ch/

LASEC

The Zero Four-Sum Problem

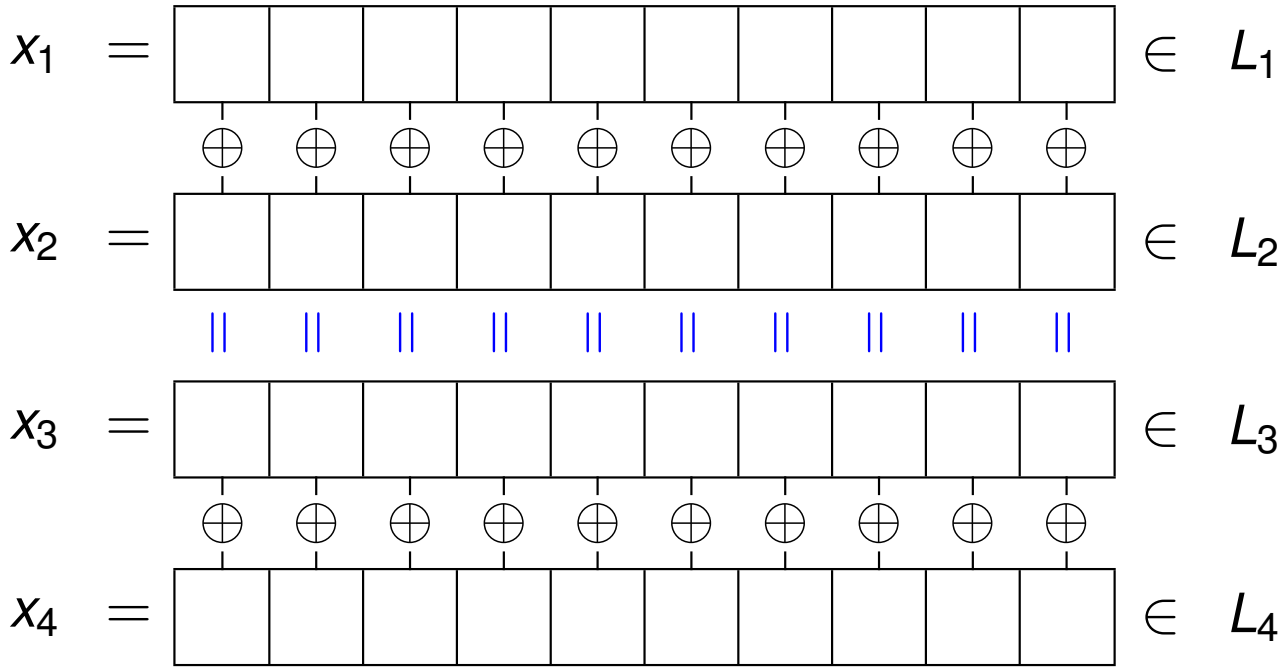
L_1, L_2, L_3, L_4: set of n ℓ-bit strings; look for s solutions



need $n = s^{\frac{1}{4}} 2^{\frac{\ell}{4}}$

The Collision Algorithm (Mozart)

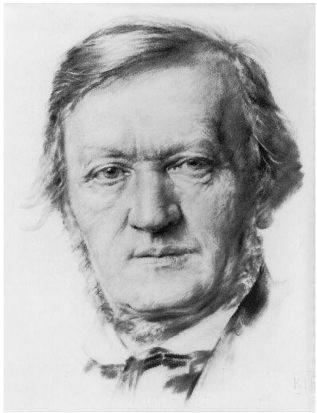
L_1, L_2, L_3, L_4: set of n ℓ-bit strings; look for s solutions



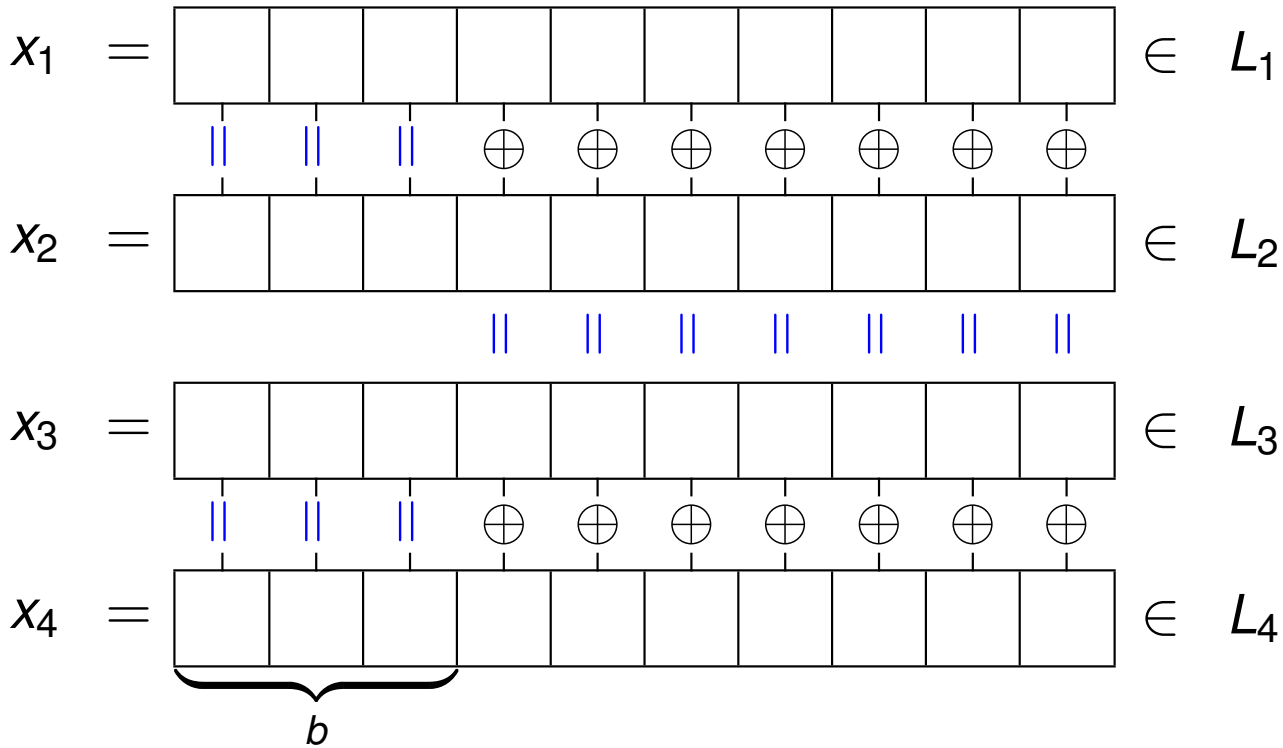
Algorithm 1: make list of all $x_1 \oplus x_2$ and $x_3 \oplus x_4$ and look for collisions; comp $= O(n^2 + s)$

$$n = s^{\frac{1}{4}} 2^{\frac{\ell}{4}}, \text{comp} = O(s^{\frac{1}{2}} 2^{\frac{\ell}{2}})$$

The Wagner Algorithm



L_1, L_2, L_3, L_4: set of n ℓ-bit strings; look for s solutions



Algorithm 2: same with list of XORs starting with b zero bits
$n = s^{\frac{1}{4}} 2^{\frac{b+\ell}{4}}$, comp $= O(n + n^2 2^{-b} + s)$

$$b_{\text{opt}} = \frac{\ell + \log_2 s}{3},\ n = s^{\frac{1}{3}} 2^{\frac{\ell}{3}},\ \text{comp} = O(s^{\frac{1}{3}} 2^{\frac{\ell}{3}})$$

[ZJW16] Invoking ~~Mozart~~ Wagner

Faster Algorithms for Solving LPN, Zhang, Jiao, Wang, EUROCRYPT 2016

In the algorithm to solve LPN$(512, 1/8)$:

LF(4) algorithm with $s = 2^{54}$, $\ell = 156$

	[ZJW16]	Mozart	Wagner
n	$s^{\frac{1}{4}}2^{\frac{\ell}{4}} = 2^{53}$	$s^{\frac{1}{4}}2^{\frac{\ell}{4}} = 2^{53}$	$s^{\frac{1}{3}}2^{\frac{\ell}{3}} = 2^{70}$
comp	$s^{\frac{1}{3}}2^{\frac{\ell}{3}} = 2^{70}$	$s^{\frac{1}{2}}2^{\frac{\ell}{2}} = 2^{105}$	$s^{\frac{1}{3}}2^{\frac{\ell}{3}} = 2^{70}$

(Table 7, p.192; $n \leftarrow n[1]$, $s \leftarrow n[2]$, $\ell \leftarrow b$)

Strange Complexities in [ZJW16]

$$x_1 \oplus \cdots \oplus x_a$$

Bit complexity to XOR $a = 10$ u-bit strings (bytes: $u = 8$)

- naive approach: $O(au)$ bit operations, too expensive (must be done 2^{71} times for LPN$(512, 1/8)$)
- [ZJW16] approach: $O(1)$ using a table lookup
  just read $T(x_1 \| \cdots \| x_a)$
  BUT: cost of concatenation is neglected!

$\rightarrow$ complexity results must be multiplied by 2^6

Corrected Complexity Table

LPN instance	$(512, 1/8)$	$(532, 1/8)$	$(592, 1/8)$
[GJL14] paper	$2^{79.9}$	$2^{81.82}$	$2^{88.07}$
(corrected)	$2^{89.04}$	$2^{90.43}$	$2^{97.87}$
[GJL14] talk	$2^{79.7}$		
(corrected)	$2^{89.04}$		
[ZJW16]	$2^{74.732}$	$2^{76.902}$	$2^{83.843}$
(corrected)	$2^{80.45}$	$2^{82.53}$	$2^{89.46}$
our results			
(breaking news!)	$2^{78.85}$	$2^{81.90}$	$2^{88.16}$

algorithms as greedy as a raccoon

Conclusion

"My IQ is one of the highest — and you all know it! Please don't feel so stupid or insecure; it's not your fault."

Donald Trump

- Bogos, Vaudenay:
  Observations on the LPN Solving Algorithm from Eurocrypt'16,
  eprint 2016/451