AriC

2014-2019

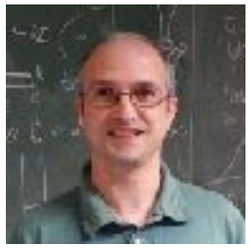
HCERES Visiting Committee - February 2020

I. Figures

Team

13 permanent members


C.-P. Jeannerod


V. Lefèvre


2018

A. Passelègue


N. Revol


B. Salvy


N. Brisebarre


2016

B. Libert


J.-M. Muller


G. Villard


F. Laguillaumie

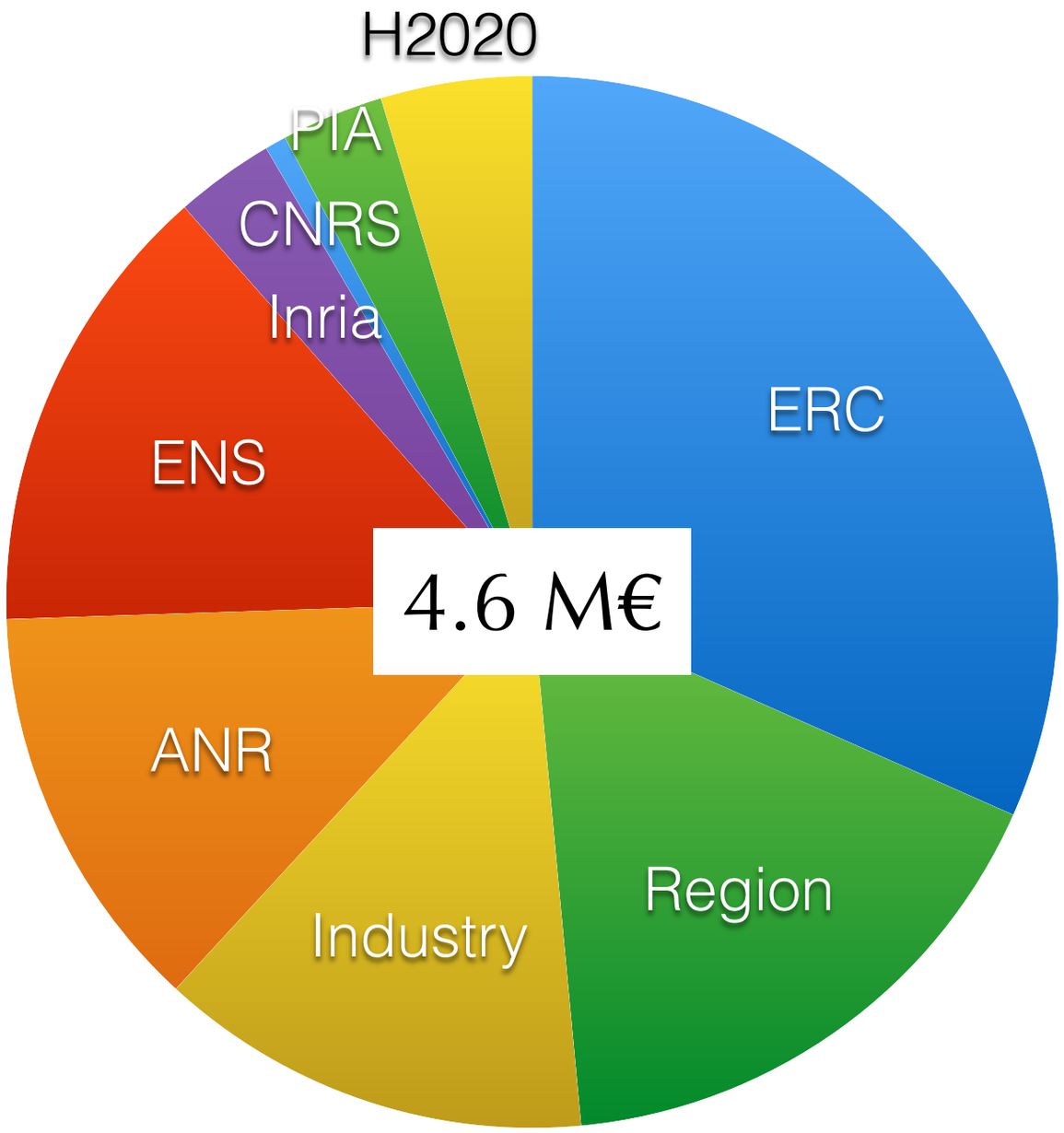

N. Louvet


G. Hanrot


D. Stehlé

+ 4 post-docs, 8 PhD students, 1/2 engineer

Funding



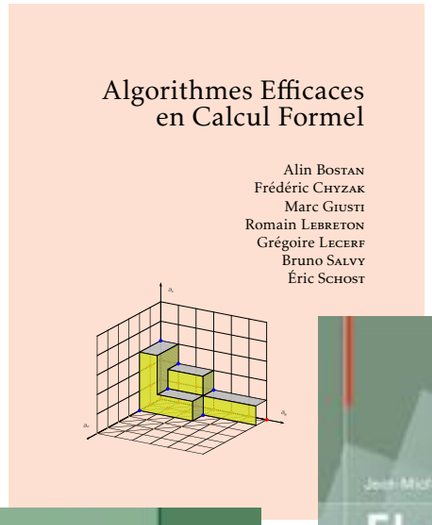
Plus:

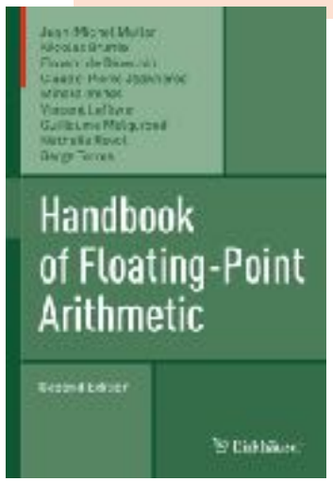
NSERC, Polytechnique:
2 x 1/2 PhD

(does not include the salaries of permanent members)

Output

3 books
12 PhD theses
63 articles
119 conferences





Best Papers

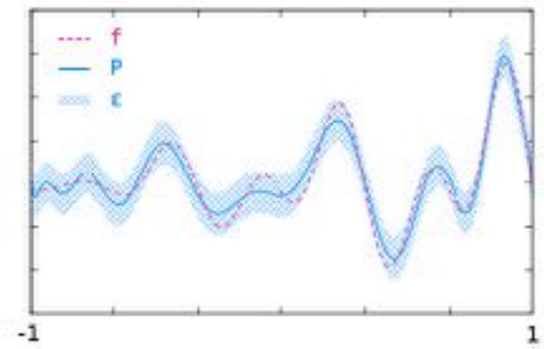
Asiacrypt 2015 Eurocrypt 2015
ISSAC 2015 ISSAC 2018
ISSAC 2019 NEW
+ best student paper ISSAC 2015

NIST

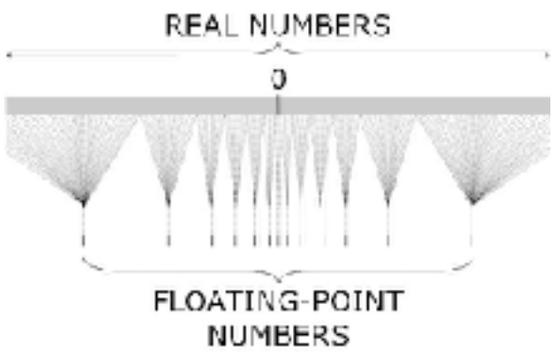
2/26 proposals selected for Round 2 of
Post-Quantum Cryptography Standardization

II. Science

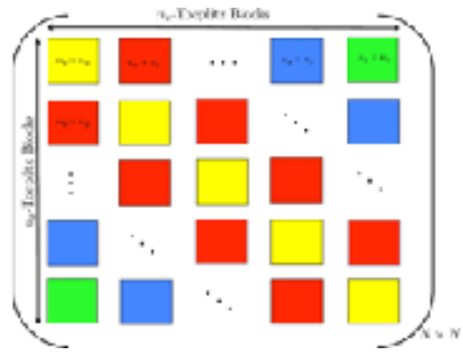
Overview: Reliability & Efficiency



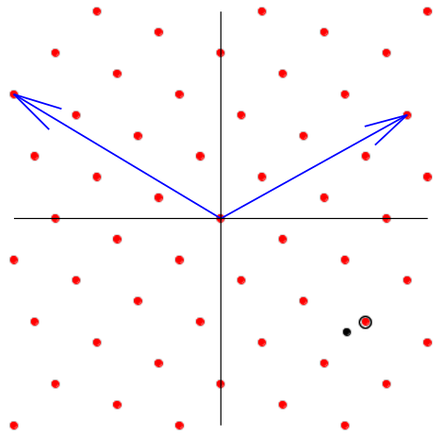
Controlled **approximation** schemes



Floating-point arithmetic



Algebraic algorithms



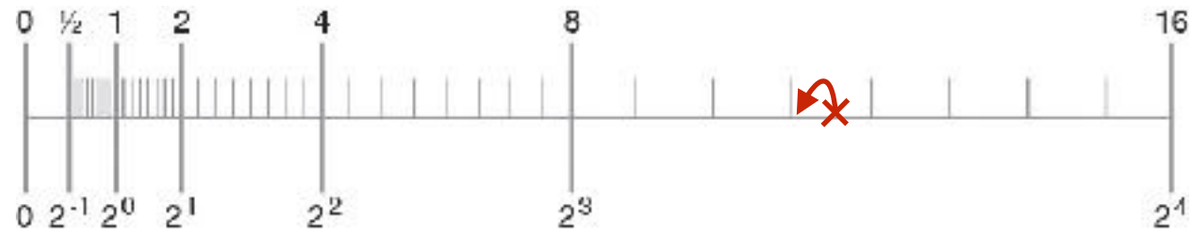
Lattices & Cryptography

fplll

Hardware–Software–Algorithms–Complexity

Robustness of 2Sum and Fast2Sum

Floating-point numbers:



5 rounding modes in IEEE754
(useful e.g., for interval arithmetic)

```
def Fast2Sum(a,b):
  s = a + b
  z = s - a
  t = b - z
  return s,t
```

1960's

Classical. In radix 2, if |a|≥|b|, rounding to nearest, t is (a+b)–s.

The exact error is accessible.

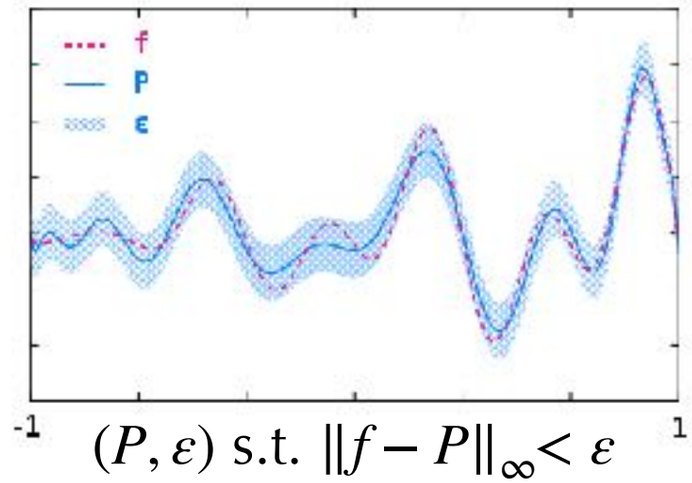
New. When executed with rounding mode o, t=o((a+b)–s).

\+ no spurious overflow
\+ similar result for 2Sum
(no hypothesis on |a|,|b|)

```
def 2Sum(a,b):
  s = a + b
  a2= s - b
  b2= s - a2
  da= a - a2
  db= b - b2
  t = da + db
  return s,t
```

[ACM TOMS 17]

Validated Numerical Solution of Linear Ordinary Differential Equations



(P, ε) s.t. $\|f - P\|_\infty < \varepsilon$

Input: equation, initial conditions, $\varepsilon > 0$

Output: rigorous polynomial approximation

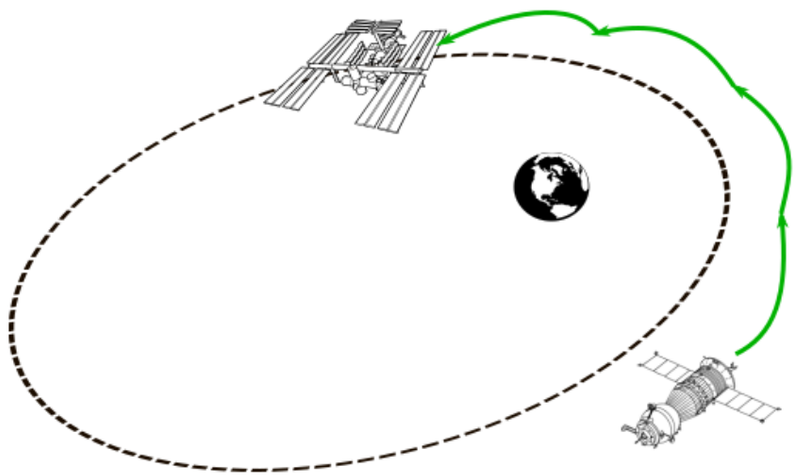
Ingredients:

1. Compute f in the Chebyshev basis
2. Rewrite the LODE $(I + K)(f^{(r)}) = g$
3. Compute a good approximation
4. Use Banach's fixed-point theorem, bounding automatically approximation and rounding errors.

order of the equation

compact integral operator

Almost band structure —> Complexity linear wrt truncation order.



Spacecraft Rendezvous

final location within $4 \cdot 10^{-8}$m
final speed 0 within $2 \cdot 10^{-11}$ms^{-1}

[ACM TOMS 18;ISSAC 18]

Functional Encryption

Setup	Ciphertext	Computation
1. (mpk, msk) 2. $(msk, F) \mapsto sk_F$	$C := \mathrm{Enc}_{mpk}(M)$	$F(M) = \mathrm{Dec}_{sk_F}(C)$

Only *F(M)* is revealed

New. First fully secure functional encryption for inner products

$$F_x : y \mapsto x \cdot y$$

Solutions based on **standard assumptions**:

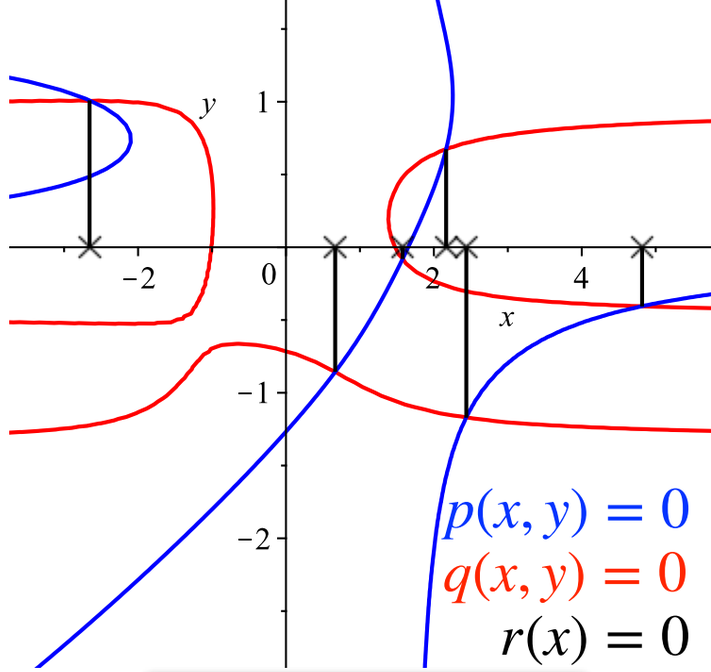
. Decision Diffie-Hellman (discrete-log based);
. Decision Composite Residuosity (factoring based);
. Learning-with-Errors problem (lattice based, conjectured **quantum resistant**).

Applications to:

. statistics;
. polynomial evaluation;
. more advanced FE;
. trace-and-revoke systems.

[Crypto 16;CCS 17;Asiacrypt 18,19;PKC 20]

Faster Bivariate Resultant



Eliminate y between p and q

Input: $p(x,y), q(x,y)$ with $\deg_x = d, \deg_y = n$

Output: $r(x) := \mathrm{Res}_y(p,q) = \det(\underbrace{\mathrm{Syl}(p,q)}_{S})$

Previous record (70's)
$\tilde{O}(n^2 d)$

New algorithm: $\tilde{O}(n^{2-1/\omega} d)$
under genericity conditions

1. $H :=$ upper-right $m \times m$ of $S^{-1} \bmod x^{4d\lceil n/m\rceil+1}$ — Structured matrix algorithms
2. $QH - R = O(x^{4d\lceil n/m\rceil+1}),\ \deg Q \le 2d\lceil n/m\rceil$ — Matrix Padé approximant
3. Generically, $r \propto \det Q$; $m \sim n^{1/\omega}$ optimizes the complexity.

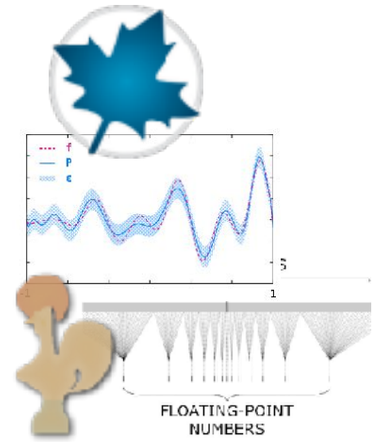
A fruit of 25 years of progress on structured & polynomial matrices

[ISSAC 18]

Plans for the Future

Certified Approximation

Development of theoretical/practical tools for certified approximation at all levels

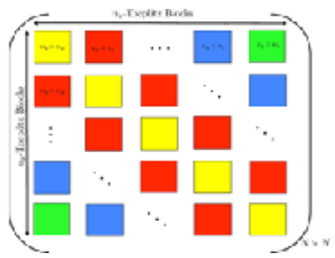


Computer Arithmetic

Tame and exploit the new processor instructions

Preparation of the next IEEE 754 standard

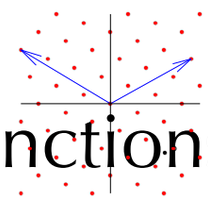
Sharp error analyses for higher level algorithms



Lattices & Cryptography

Improve use & efficiency of lattice-based crypto

Practical functional encryption for more general functions



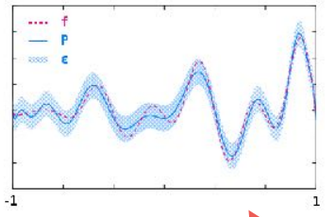
Algebraic Algorithms

Fundamental algo. on structured & polynomial matrices

Symbolic summation and integration algorithms

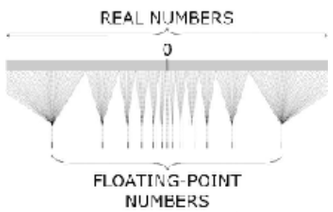
A.: Interactions between Themes

Controlled approximation schemes

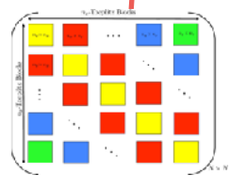


Error analyses for high-level algos
Floating-point coefficients in approx.

Floating-point arithmetic

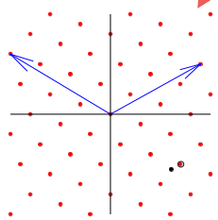


Expansions in various bases
Linear differential equations



Algebraic algorithms

fplll



Geometry of numbers

Lattices & Cryptography

Ideal lattices
Polynomial systems
Computation of relations

Hardware–Software–Algorithms–Complexity

Connexions

National: GDR-IM (1200+ members): co-direction, committees, animation of groups.

Paris, Grenoble, Toulouse, Amsterdam, Barcelona, Hamburg, Linz, London, Uppsala

International: steering committees of Arith, AofA, PQCrypto.

UCLA, NCSU, Florida Atlantic U., Waterloo, Vancouver

Editorial boards: IEEE Trans. on Computers; J. Symbolic Computation; J. Algebra; J. Cryptology; Reliable Computing.

Beijing, Madras, Seoul, Singapore

Melbourne

The End