In Defense of Attacks:

Some Major Successes in Cryptanalysis

Anne Canteaut

Inria Paris, équipe-projet COSMIQ

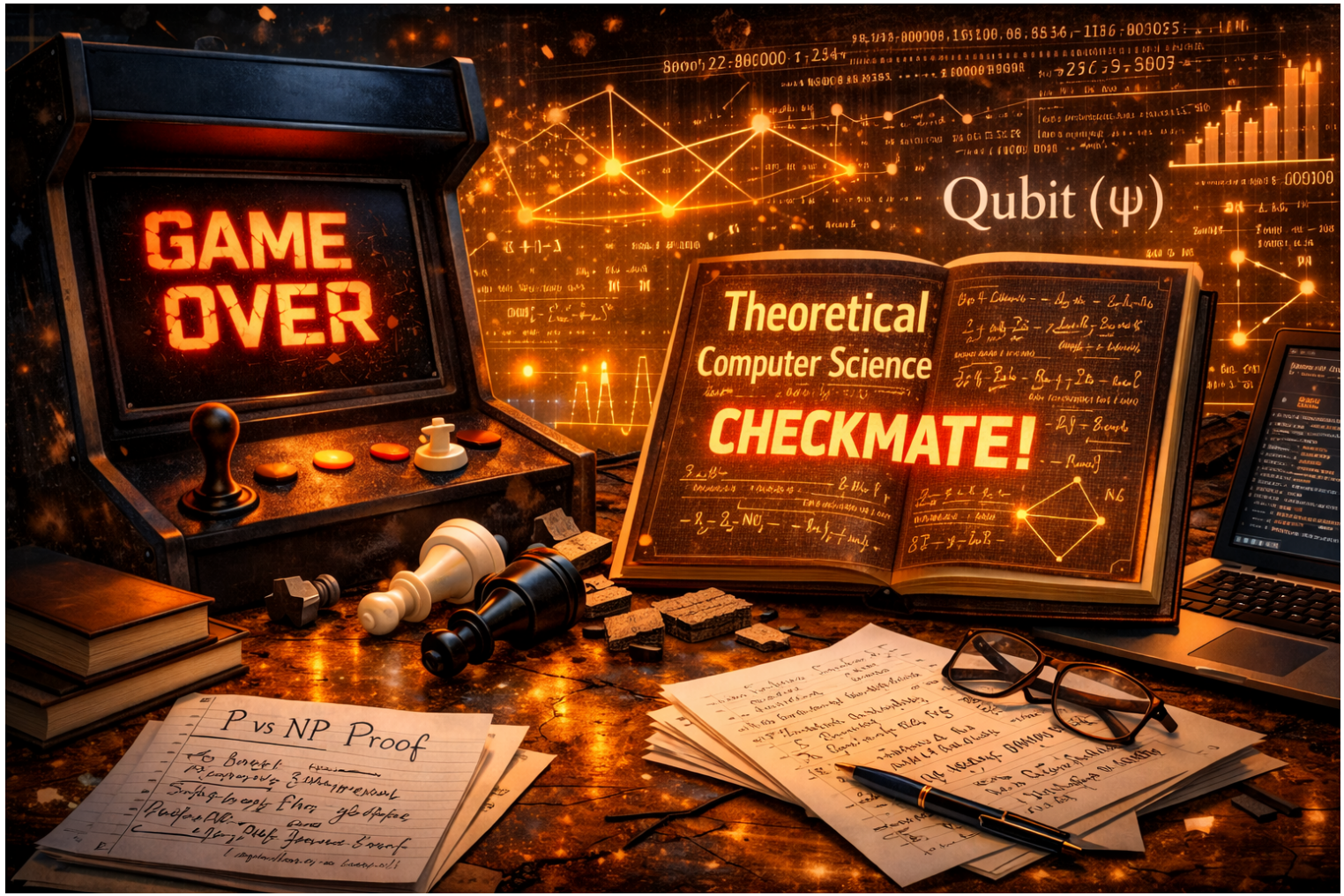
www.paris.inria.fr/secret/Anne.Canteaut/

GdR IFM's 20th anniversary - March 17, 2026

The Two Sides of Cryptology

The shield and the spear

From the mid 80's [Goldreich, Goldwasser, Micali...]



The Modern View (from the 1990's)

Attacks:

algorithms, upper bounds on the security level

Security proofs:

theorems, guarantees on the security level

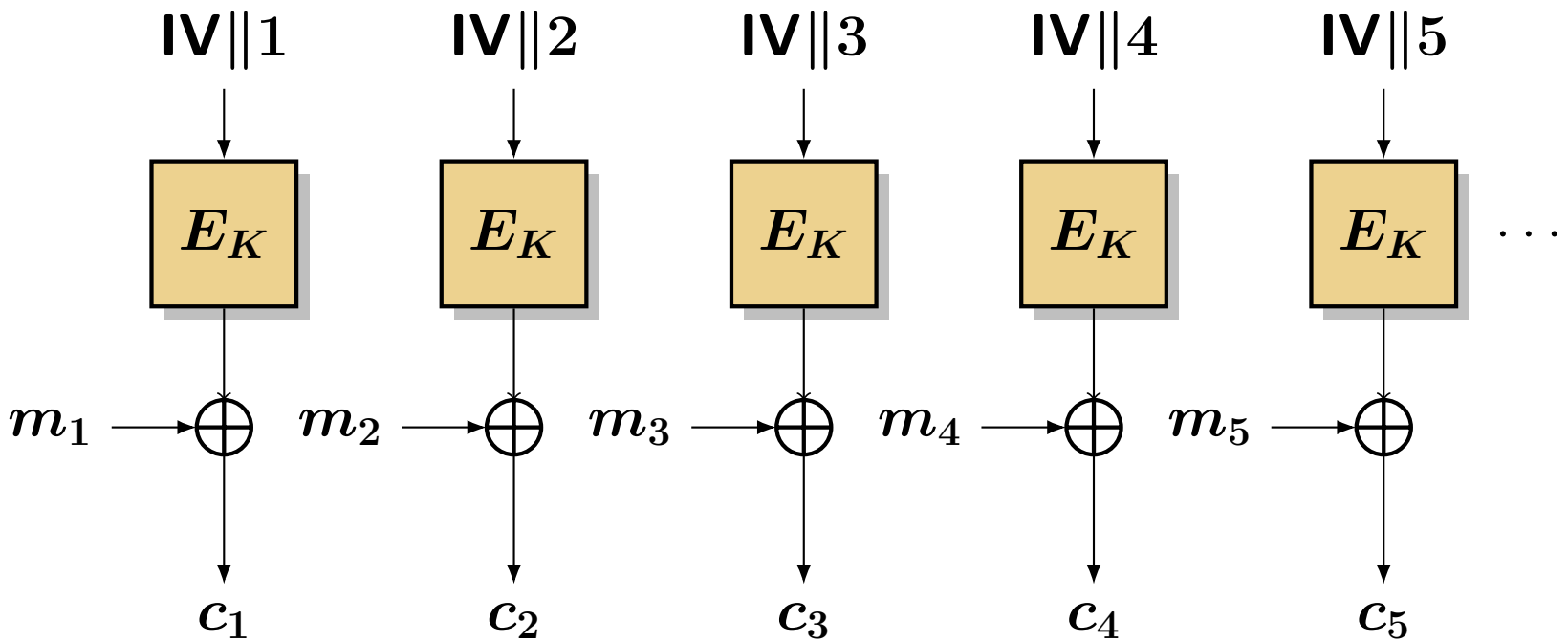
Encryption schemes

Two steps for encrypting plaintexts of an arbitrary length:

1. design a block cipher, i.e., a family of bijections operating on $\{0,1\}^n$.

2. design a mode of operation describing how this block cipher can be used for encrypting messages of any length.

CTR mode for encryption



where E_K is a block cipher, i..e, a bijection of $\{0,1\}^n$ indexed by the key and **IV** is a public nonce.

Security proof [Bellare, Desai, Kilian, Jokipii, Rogaway 94-97]

Security model:

Indistinguishability from random bits

Theorem. Let $\mathcal{A}$ be an adversary attacking $\mathbf{CTR}[E]$ with queries corresponding to σ plaintext blocks. Then there exists an adversary $\mathcal{B}$ for distinguishing E from a random permutation with advantage

$$\mathbf{Adv}_{E}(\mathcal{B}) \geq \mathbf{Adv}_{\mathbf{CTR}[E]}(\mathcal{A}) - \frac{\sigma^2}{2^{n+1}}$$

The running time and number of queries of $\mathcal{B}$ are essentially the same as those of $\mathcal{A}$.

Remaining questions

- Is the reduction tight?
- Is the security model relevant?
- Is the underlying block cipher E secure?

A more appropriate terminology

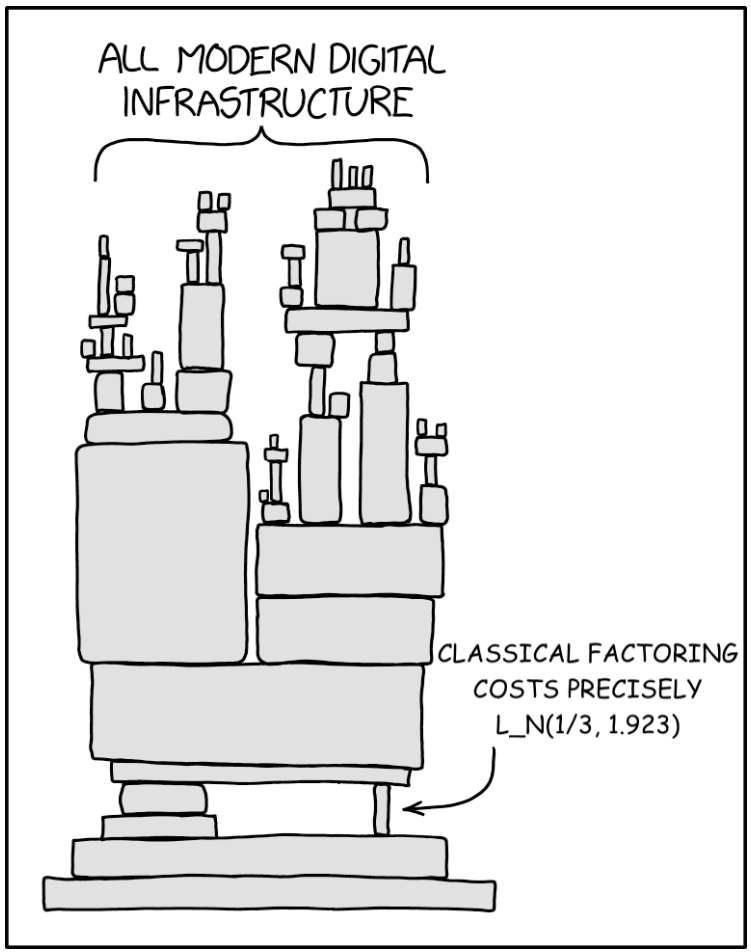
Security arguments, security reductions

Guarantees on the security level for a given security model and under some assumptions.

Security analysis:

Upper bounds on the security level, also applies to the assumptions.

Without cryptanalysis [Heninger 24]



Apologies to xkcd/2347

Competitions for standardization

- SHA-3 hash function (2007-2012)
- Lightweight authenticated encryption (2019-2023)
- Post-quantum key-exchange and signature (2017-)

The rest of this talk

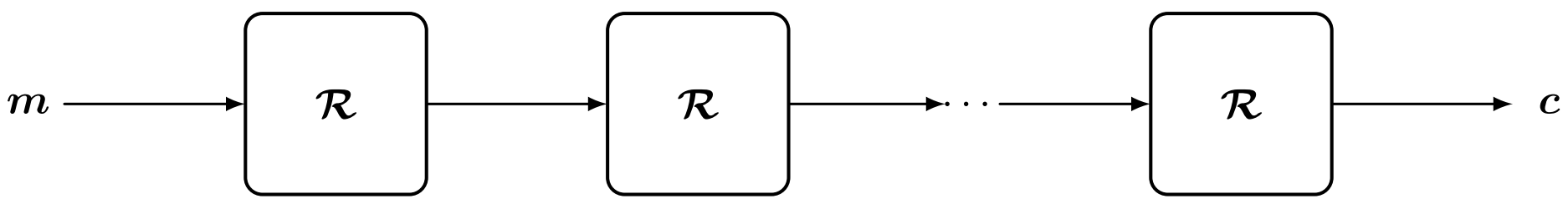
1. Block ciphers

2. Hard problems for post-quantum cryptography

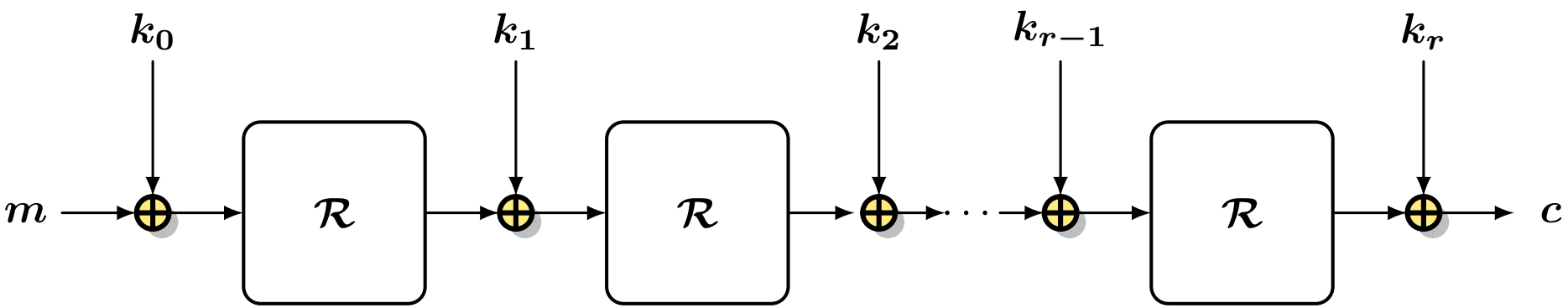
3. Hard problems for number-theoretic cryptography

Block ciphers

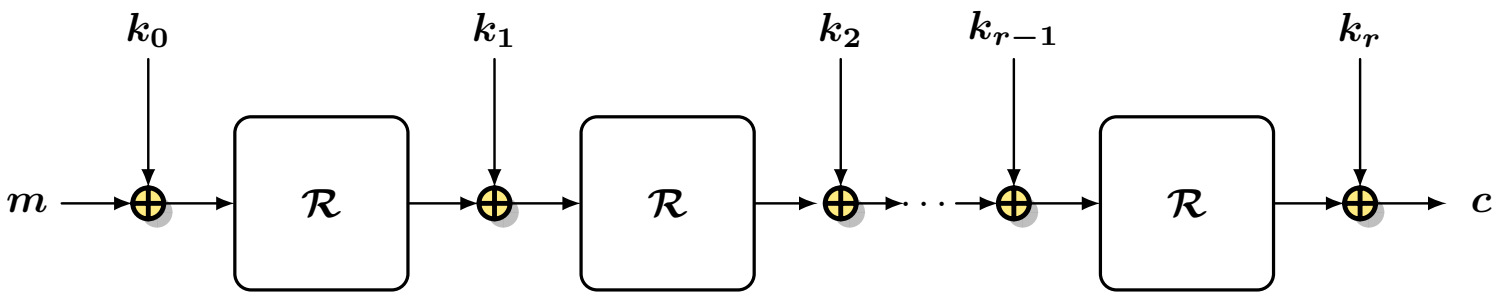
Iterated construction



Iterated construction



New applications (lightweight, easy-to-mask, FHE friendly...)



New performance metrics for many applications:

minimize the number of multiplications or the multiplicative depth of $\mathcal{R}$

$\longrightarrow$ Impact on the security of the entire cipher?

New applications (lightweight, easy-to-mask, FHE friendly...)

Each ciphertext bit can be written as a polynomial of n Boolean variables

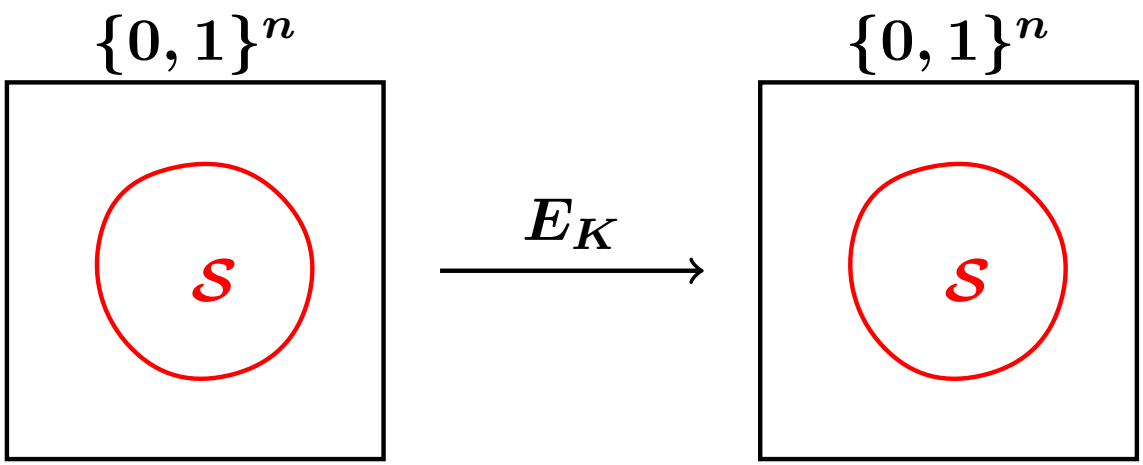
$$\sum_{I \subseteq \{1,\ldots,n\}} a_I(K) \left(\prod_{i \in I} x_i \right), \text{ with } a_I(K) \in \{0,1\}$$

New algorithms for computing the coefficients of the polynomials over the rounds.

- Division property [Todo 15] $\longrightarrow$ cryptanalysis of MISTY1 (ISO/IEC 18033)
- New algebraic formulations [Boura, C. 16] [Udovenko 21] [Beyne, Verbauwhede 23]
- Many algorithmic improvements [Boura, C. 16] [Todo, Morri 16] [Hao et al. 20] [Hu et al. 20] [Hebborn 22]...
- Generalization to non-binary fields [Beyne, Verbauwhede 24-25]

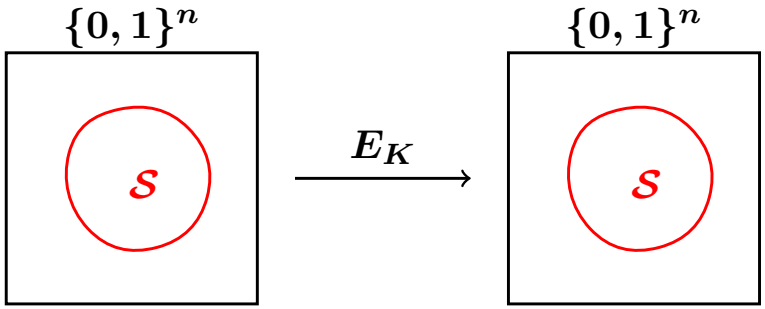
Invariants for weak-key classes

Non-trivial subset of $\{0,1\}^n$ invariant under E_K for some K:



$$E_K(\mathcal{S}) = \mathcal{S}$$

Invariants for weak-key classes



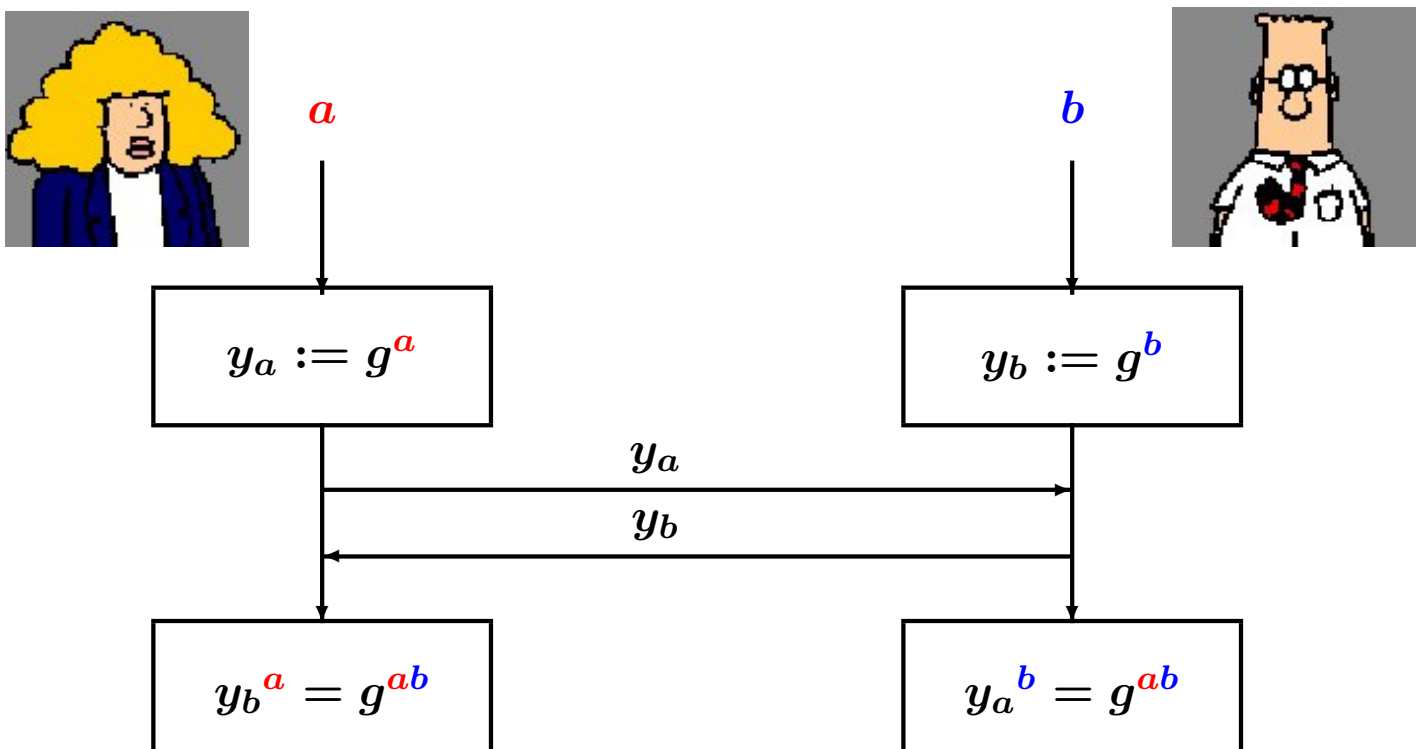
- Invariant subspaces [Leander et al. 11][Leander, Minaud, Rønjom 15][Guo et al. 16], cryptanalysis of iScream...
- Nonlinear invariant [Todo, Leander, Sasaki 16], cryptanalysis of Scream, Midori64...
- Algebraic formalization as eigenvectors of the correlation matrix [Beyne 18]
- Security criteria [Beierle, C., Leander, Rotella 17]...

New direction: how the behavior of E_K for a fixed K deviates from the average behavior.

Post-quantum asymmetric cryptography

Diffie-Hellman key exchange

Let G be a finite cyclic group and g a generator of G.



Underlying hard problem

Discrete logarithm problem.

Let G be a finite cyclic group and g a generator of G.

Given $h \in G$, find x such that $g^x = h$.

Underlying hard problem

Discrete logarithm problem.

Let G be a finite cyclic group and g a generator of G.

Given $h \in G$, find x such that $g^x = h$.

Computational Diffie-Hellman problem.

Let G be a finite cyclic group and g a generator of G.

Given g^a and g^b, compute g^{ab}.

Open question.

Is CDHP at least as hard as DLP?

Underlying hard problem

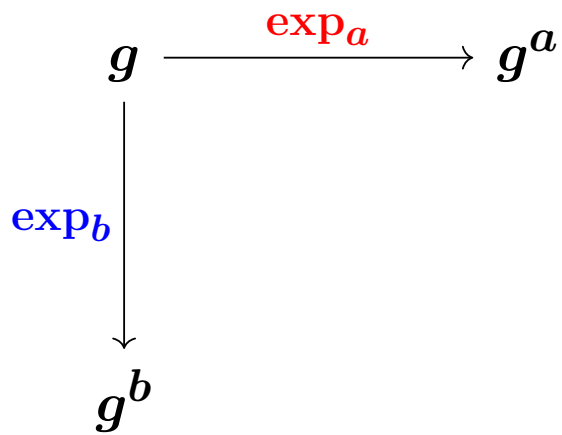
Discrete logarithm problem.

Let G be a finite cyclic group and g a generator of G.

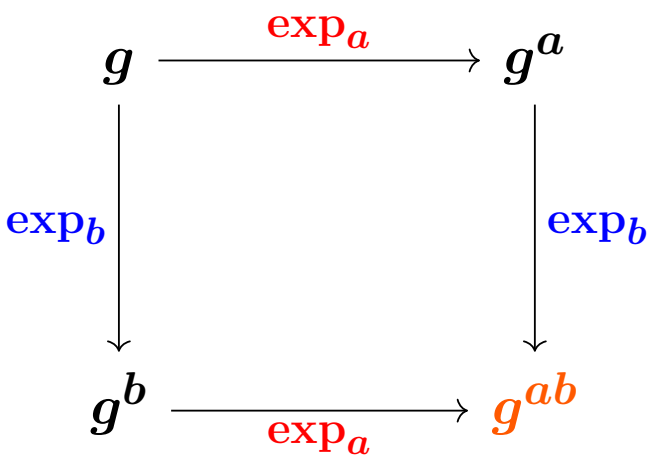
Given $h \in G$, find x such that $g^x = h$.

Solved in polynomial time by a quantum algorithm [Shor 94]

Another view of Diffie-Hellman key exchange



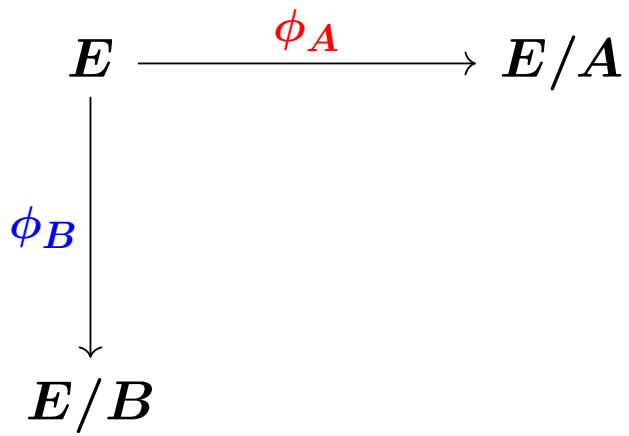
Another view of Diffie-Hellman key exchange



SIDH - Supersingular isogeny Diffie-Hellman [Jao, De Feo 11]

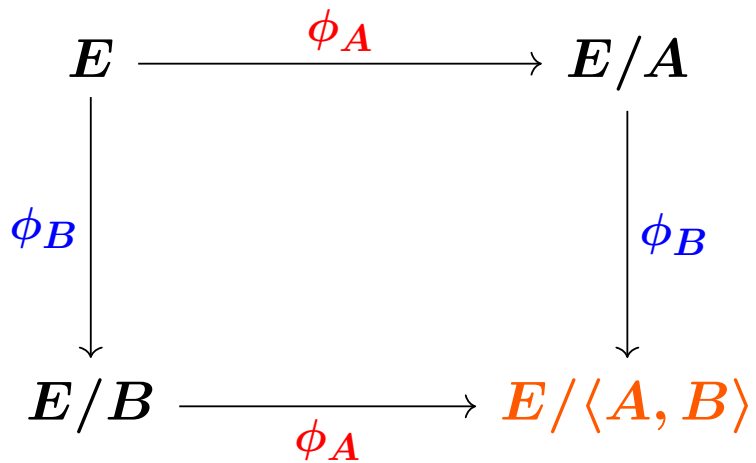
Consider a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ with $p = 2^\alpha 3^\beta f \pm 1$.

A is a secret cyclic subgroup of $E[2^\alpha]$ and B is a secret cyclic subgroup of $E[3^\beta]$



SIDH - Supersingular isogeny Diffie-Hellman [Jao, De Feo 11]

Consider a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ with $p = 2^\alpha 3^\beta f \pm 1$.



Additional knowledge of $\phi_A(P_B), \phi_A(Q_B)$ for $P_B, Q_B \in E[3^\beta]$
and of $\phi_B(P_A), \phi_B(Q_A)$ for $P_A, Q_A \in E[2^\alpha]$

Underlying hard problem

Supersingular isogeny problem.

Let E and E' be two supersingular elliptic curves over $\mathbb{F}_{p^2}$.

Find an isogeny $\phi : E \to E'$.

$\to$ Best known classical algorithm $\mathcal{O}(p^{1/4})$, quantum $\mathcal{O}(p^{1/6})$.

Underlying hard problem

Supersingular isogeny problem.

Let E and E' be two supersingular elliptic curves over $\mathbb{F}_{p^2}$.
Find an isogeny $\phi : E \to E'$.

$\to$ Best known classical algorithm $\mathcal{O}(p^{1/4})$, quantum $\mathcal{O}(p^{1/6})$.

SIDH problem.

Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$.
Given two public curves $E_A = E/A$ and $E_B = E/B$ and the images of two torsion points under secret isogenies, compute

$$E_{AB} = E/\langle A, B \rangle$$

Cryptanalysis of SIDH [Castryck, Decru 23][Robert 23]

SIDH problem. Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$.
Given two public curves $E_A = E/A$ and $E_B = E/B$ and the images of two torsion basis points under secret isogenies, compute

$$E_{AB} = E/\langle A, B\rangle$$

Attack.

- Lift the problem to product surface $E \times E_A$ which is an Abelian surface. Inside this surface, the secret isogeny ϕ_A corresponds to a special algebraic curve.
- The values of $\phi_A(P_B)$ and $\phi_A(Q_B)$ give points on that curve.
- Once you know enough points on an algebraic curve, you can recover the whole curve, i.e. ϕ_A in polynomial time.

$\longrightarrow$ Attack of all instances of the NIST candidate in a few seconds on a PC.

What's about lattice-based cryptography?

Cryptology ePrint Archive

Quantum Algorithms for Lattice Problems

Yilei Chen, Tsinghua University, Shanghai Artificial Intelligence Laboratory, Shanghai Qi Zhi Institute

Abstract

We show a polynomial time quantum algorithm for solving the learning with errors problem (LWE) with certain polynomial modulus-noise ratios. Combining with the reductions from lattice problems to LWE shown by Regev [J.ACM 2009], we obtain polynomial time quantum algorithms for solving the decisional shortest vector problem (GapSVP) and the shortest independent vector problem (SIVP) for all n-dimensional lattices within approximation factors of $\tilde{\Omega}(n^{4.5})$. Previously, no polynomial or even subexponential time quantum algorithms were known for solving GapSVP or SIVP for all lattices within any polynomial approximation factors.

Back to pre-quantum asymmetric cryptography

Discrete logarithm over finite fields

Setting of many constructions, like pairing-based cryptography, zero-knowledge proofs...

$$L_q(\alpha) = \exp\left((c + o(1))\,(\log q)^{\alpha}\,(\log\log q)^{1-\alpha}\right)$$

- For $\alpha = 1$: exponential in $\log q$
- For $\alpha = 0$: polynomial in $\log q$.

Twenty years ago... [Joux, Lercier, Smart, Vercauteren 06]

The discrete log problem in any field of size q can be solved with asymptotic complexity $L_q(1/3)$.

A quasi-polynomial algorithm [Barbulescu, Gaudry, Joux, Thomé 14]

A discrete logarithm in a finite field of size $q = p^n$ can be computed in time

$$\max(p, n)^{\mathcal{O}(\log n)}$$

$\longrightarrow$ It works especially for small characteristic.

CADO-NFS (Levchin Prize 2025)

https://cado-nfs.gitlabpages.inria.fr/

CADO-NFS

Crible Algébrique: Distribution, Optimisation - Number Field Sieve

Home
Prerequisites
Download
Development
Bugs / Support
User Reports

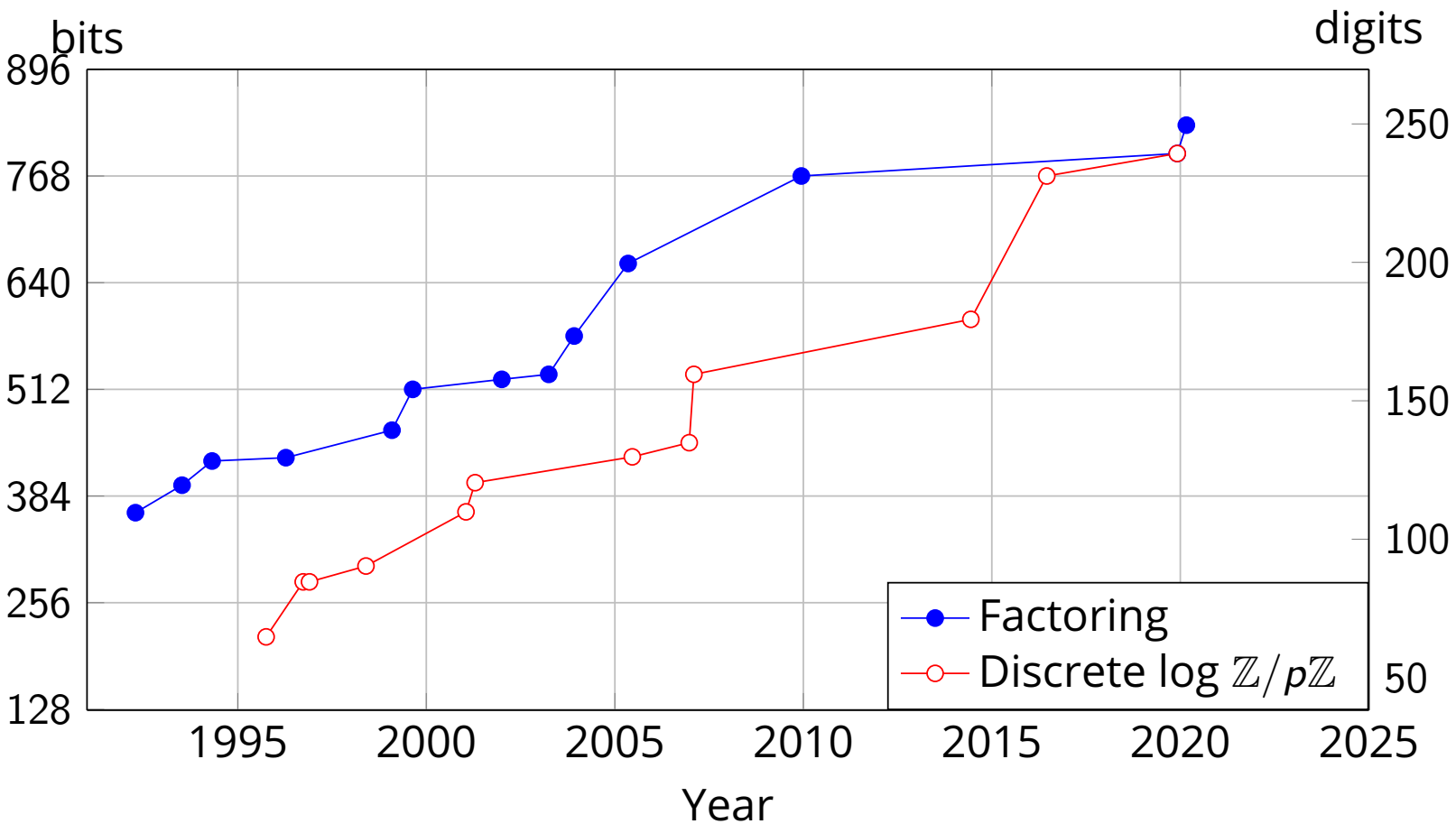
Introduction

CADO-NFS is a complete implementation in C/C++ of the Number Field Sieve (NFS) algorithm for factoring integers and computing discrete logarithms in f
It consists in various programs corresponding to all the phases of the algorithm, and a general script that runs them, possibly in parallel over a network of com
CADO-NFS is distributed under the Gnu Lesser General Public License (LGPL) version 2.1 (or any later version).

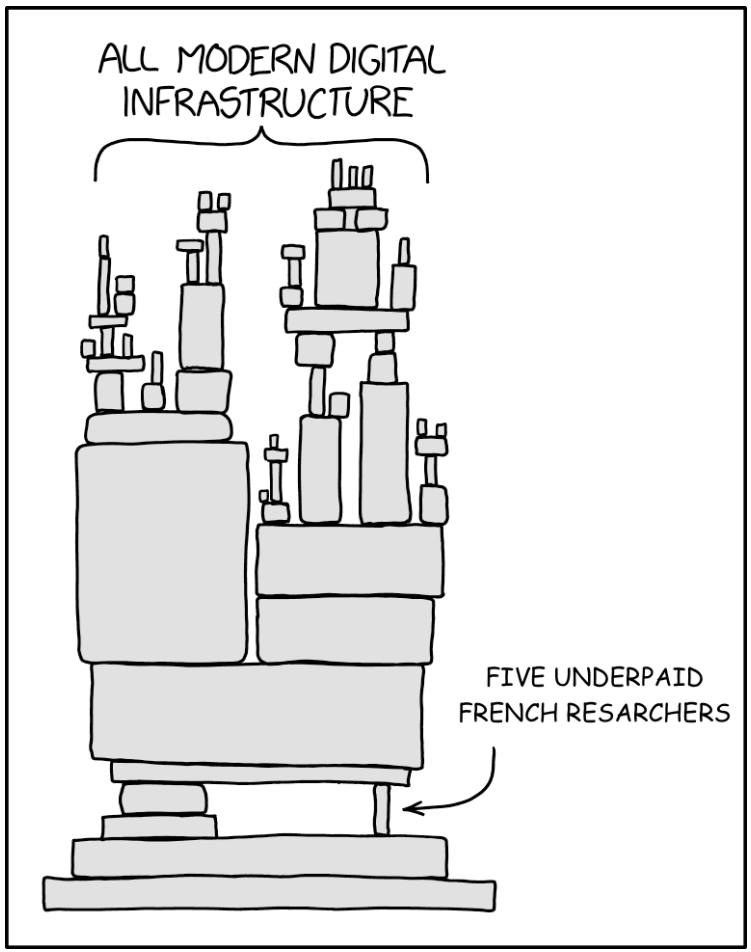
CADO-NFS is the result of a collaborative effort involving many persons, over various periods of time. The current list of active contributors can be extracted
git repository or from the openhub.net page. A tentative list of CADO-NFS authors is (alphabetical order):

- Shi Bai
- Razvan Barbulescu
- Cyril Bouvier
- Richard Brent
- Christophe Clavier
- Jérémie Detrey
- Andreas Enge
- Alain Filbois
- Nuno Franco
- Pierrick Gaudry
- Laurent Grémy
- Aurore Guillevic
- Nadia Heninger
- Laurent Imbert
- Alexander Kruppa
- Jérome Milan
- François Morain
- Lionel Muller
- Thomas Prest
- Thomas Richard
- Emmanuel Thomé
- Marion Videau
- Paul Zimmermann

Factoring and discrete log records – taken from [Heninger 24]



A realistic view of asymmetric cryptography? – taken from [Heninger 24]



Apologies to xkcd/2347

Conclusions

Cryptanalysis represents only 15-20 % of the papers in cryptography.

Geographical origin of the cryptanalysis papers (Eurocrypt/Crypto/Asiacrypt 25):
45 % from Europe, 25 % from Asia and 25 % from North America.

Possible reasons.

- less prestigious than provable security
- requires a lot of time (and maybe too much expertise for a PhD project)
- fewer citations.

Conclusions

Cryptanalysis represents only 15-20 % of the papers in cryptography.

Geographical origin of the cryptanalysis papers (Eurocrypt/Crypto/Asiacrypt 25):
45 % from Europe, 25 % from Asia and 25 % from North America.

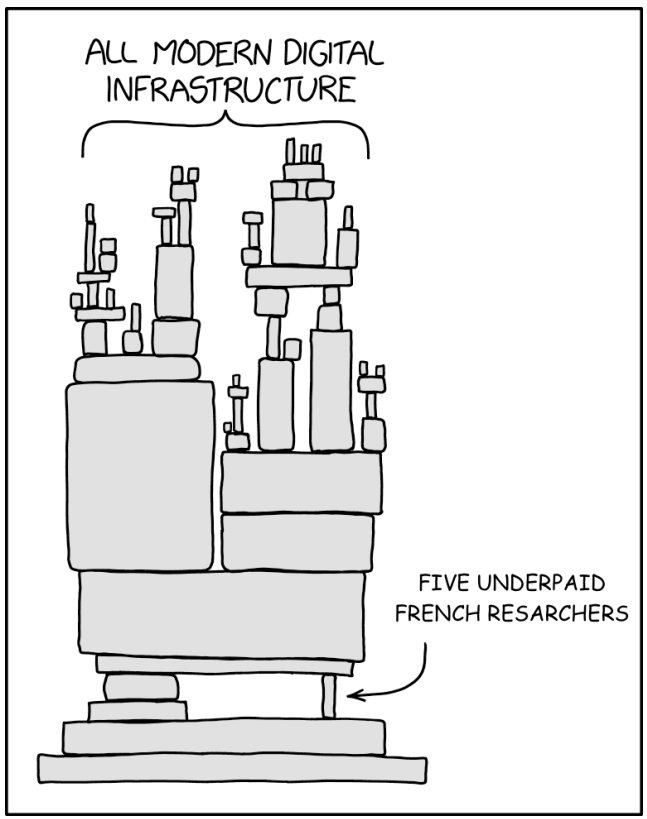
Possible reasons.

- less prestigious than provable security
- requires a lot of time (and maybe too much expertise for a PhD project)
- fewer citations.

However

- Cryptanalysis is also a science!
- Assumptions used in security proofs need to be further studied, in the quantum and classical settings.
- A breakthrough cannot be ruled out, even for problems that have been studied for long.

Thank you!



Credit: N. Heninger