Lettre des "Lundi de la cybersécurité" n° 91

Prouver la connaissance d'un secret sans le divulguer

Les protocoles de preuves à divulgation nulle de connaissances

Prouver qu'on connait le contenu d'un message sans le divulguer ?

Par les protocoles de preuves à divulgation nulle de connaissances (zero-knowledge)

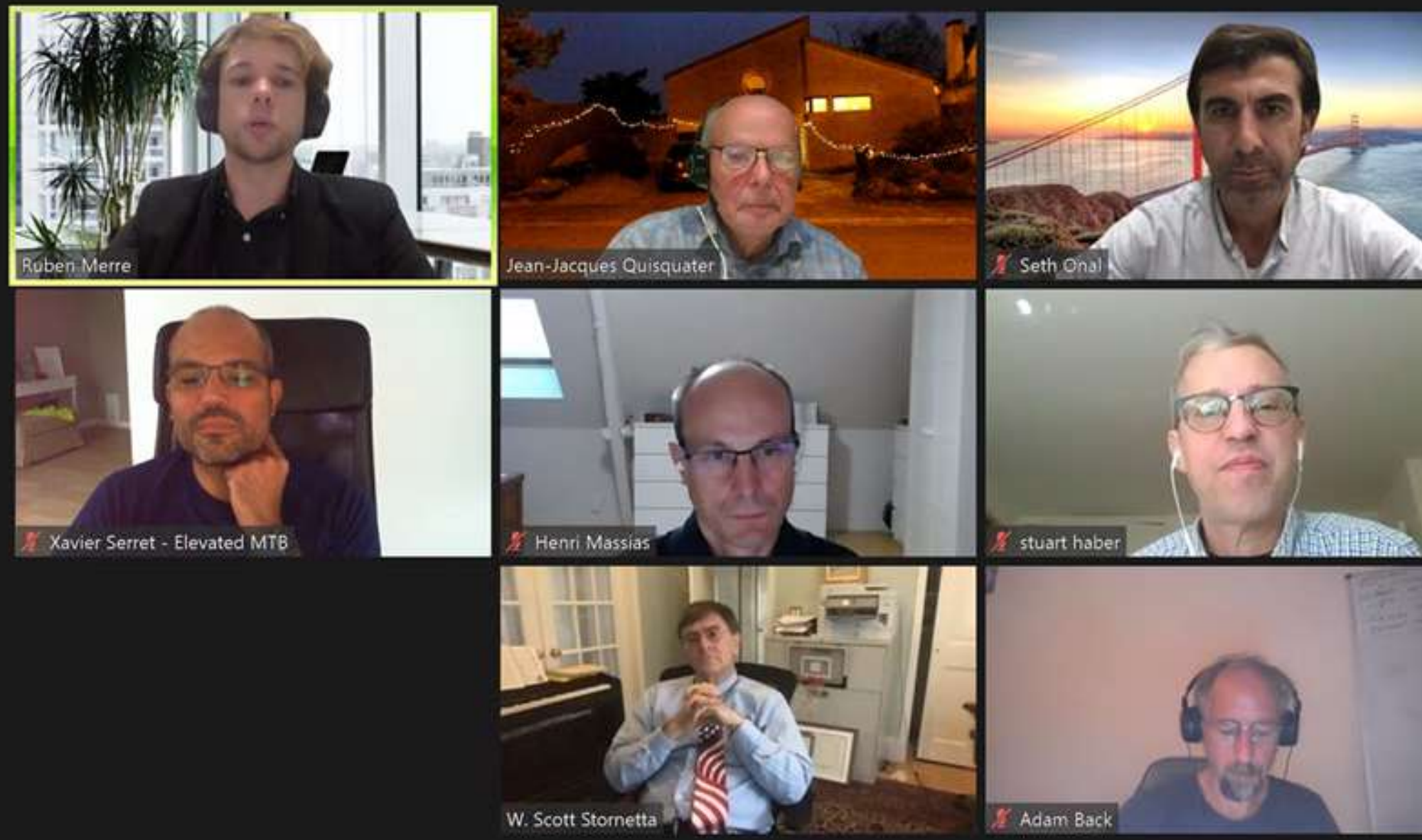
Jean-Jacques Quisquater

UCLouvain

UCLouvain

1/10/2020

Versus NYT



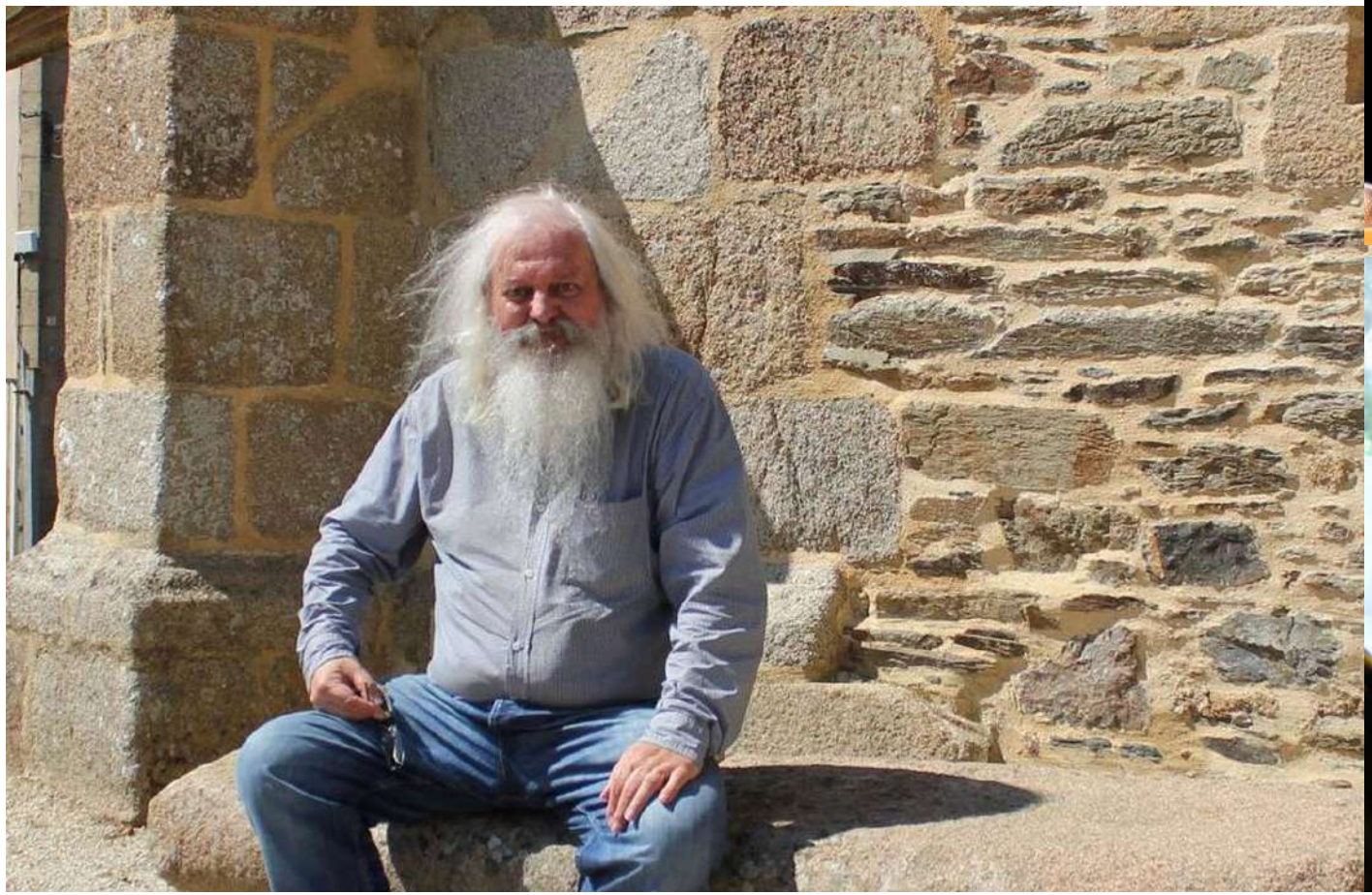
En introduction :

- Inventé il y a plus de 40 ans, les protocoles cryptographiques de type zero-knowledge regagnent en actualité et grandes utilisations,
- J'ai eu le privilège et la chance de connaître, de rencontrer, de discuter, etc, avec les créateurs, en temps réel, et nous sommes toujours amis, et plus, nous le verrons, car Louis Guillou et moi-même y avons contribué très tôt,
- Cette présentation sera une introduction historique vécue, et illustrée, des concepts, avec des anecdotes peu connues, une explication complète abordable, prête à l'emploi pour vos meilleures futures applications,
- Merci pour cette invitation et votre écoute,
- Cet exposé est dédié à la mémoire de Louis Guillou, mon ami, et complice depuis 1980,
- Ceci n'est pas un cours et un expert trouvera certainement que je manque ici de rigueur.

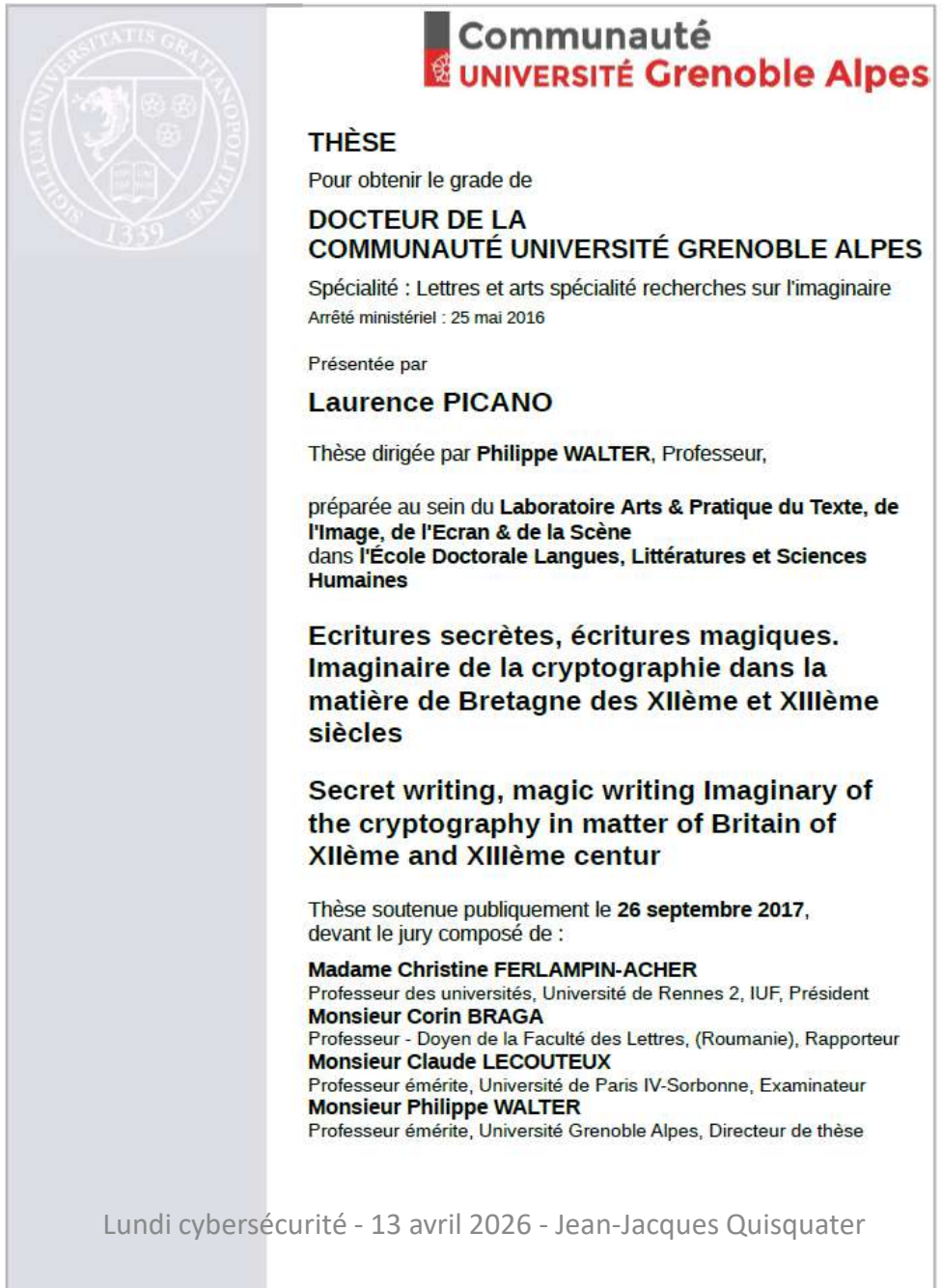
Plan

- La magie et ZK : Rubik
- Les débuts publics de la cryptographie à clé publique : Diffie-Hellman, Merkle, RSA
- Définition informelle de ZK et premiers exemples approchés (basé sur le hash et mots de passe, signature)
- Les inventeurs : Goldwasser-Micali-Rackoff : débuts difficiles
  - Quelques définitions utiles
- Protocole Fiat-Shamir (+ brevet) : l'idée géniale mais pas assez efficace
- L'histoire de GQ (+ brevet), intervention de Fiat
- La caverne familiale d'Ali-Baba : les rôles de Philips et Gilles Brassard, intervention de Tom Berson
- Utilisations (TV à péage) et contrefaçons (FS, GQ, …) : EMV ?, ISO
- Le procès avec RSA, inc et Novell : rencontre avec les grands (avocats)
- GQ2, une longue histoire qui finit par une vente du brevet : et aussi EMV versus GQ2
- La traversée du désert
- Le renouveau actuel du ZK : usages (blockchain, cryptomonnaies, etc), conférences et standards
- Le futur du ZK versus le quantique : et la recherche continue.

Louis Guillou



Bretagne, magie, cryptographie



Communauté
UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir le grade de

DOCTEUR DE LA COMMUNAUTÉ UNIVERSITÉ GRENOBLE ALPES

Spécialité : Lettres et arts spécialité recherches sur l'imaginaire

Arrêté ministériel : 25 mai 2016

Présentée par

Laurence PICANO

Thèse dirigée par **Philippe WALTER**, Professeur,

préparée au sein du **Laboratoire Arts & Pratique du Texte, de l'Image, de l'Ecran & de la Scène**
dans **l'École Doctorale Langues, Littératures et Sciences Humaines**

Ecritures secrètes, écritures magiques. Imaginaire de la cryptographie dans la matière de Bretagne des XIIème et XIIIème siècles

Secret writing, magic writing Imaginary of the cryptography in matter of Britain of XIIème and XIIIème centur

Thèse soutenue publiquement le **26 septembre 2017**,
devant le jury composé de :

Madame Christine FERLAMPIN-ACHER
Professeur des universités, Université de Rennes 2, IUF, Président
Monsieur Corin BRAGA
Professeur - Doyen de la Faculté des Lettres, (Roumanie), Rapporteur
Monsieur Claude LECOUTEUX
Professeur émérite, Université de Paris IV-Sorbonne, Examinateur
Monsieur Philippe WALTER
Professeur émérite, Université Grenoble Alpes, Directeur de thèse

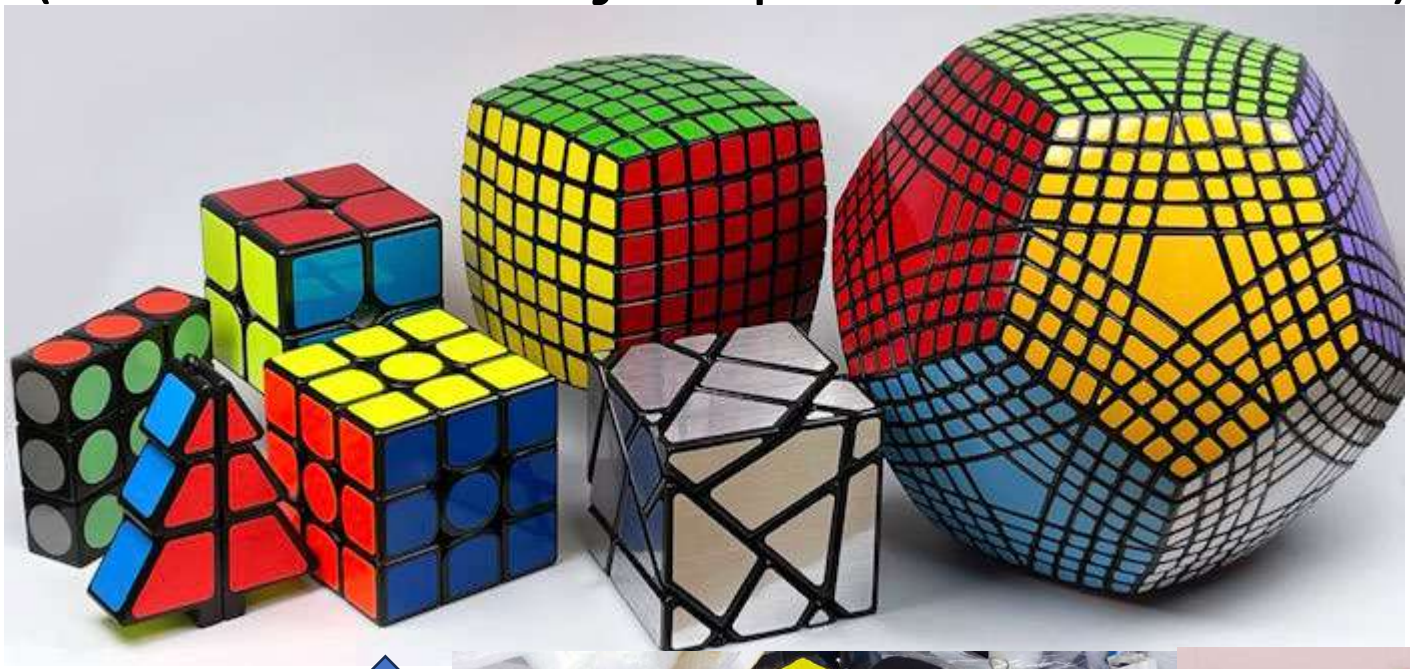
Prouver que l'on a un secret sans le révéler ?

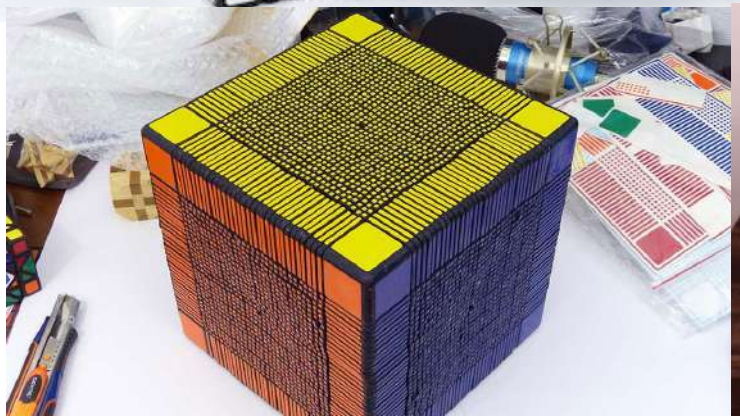
- J'ai regardé dans le passé et j'ai trouvé des traces de telles méthodes dans l'ancienne Egypte et le Moyen-Age européen :
  peu convaincant car cela utilise souvent le fait de pouvoir revenir au passé …,

- Par contre, les magiciens sont bien de la partie : j'ai un secret et je vous montre le résultat sans révéler le « truc » ou mon « pouvoir »,

- Donc, on commence ainsi, …

Le cube de Ernö Rubik – 450 millions d'exemplaires (et sa famille jusqu'au 49x49x49)





Documentation sur le cube de Rubik

- https://ruwix.com/
- https://ruwix.com/blog/49x49x49-big-rubiks-cube/
- Simulation : https://www.youtube.com/watch?v=xOJtLb_rPVg
  - 32768 x 32768 x 32768

Notices of the AMS

Juin–Juillet 2013

(fonctions de hachage)

Rubik's for Cryptographers

Christophe Petit and Jean-Jacques Quisquater

Presumably hard mathematical problems stand at the core of modern cryptography. A typical security proof for a cryptographic protocol relates its resistance against a particular attack to the hardness of some mathematical problem. Very few problems have survived thorough cryptanalysis, the most established ones being the integer factorization problem and the discrete logarithm problems on finite fields and elliptic curves. Other problems have been suggested, related, for example, to hyperelliptic curves, lattices [42], error-correcting codes [31], or multivariate polynomial equations [35] (the so-called postquantum cryptographic algorithms). They are currently less trusted than the three previous ones, but they might join or replace them in the future.

In this paper we discuss three alternative computational problems: namely the *balance, representation, and factorization problems in finite non-Abelian groups*. Interestingly, these problems can be seen as generalizations of the Rubik's Cube. The famous 3D puzzle is notoriously "hard" [12], but of course not in a cryptographic sense. Computer programs solve it instantaneously, and even human champions need less than ten seconds. Nevertheless, the "extensions" considered in this paper were proposed as the core computational problems underlying the security of *Cayley hash functions*, an elegant construction of a very important cryptographic primitive.

For the cryptographic applications to be secure, the balance, representation, and factorization problems must be computationally hard. These problems are of course easy for the Rubik's Cube. They are also easy in a few other particular cases, but they may still be hard in general. In fact, they are strongly connected to famous problems in group theory and can be seen as algorithmic versions of a twenty-year-old conjecture of Babai on the diameters of Cayley graphs. Although the conjecture is now proved for all parameters of interest in cryptography, many of the proofs are nonconstructive, hence useless, to "break" the functions.

In the last twenty years, the cryptography community (for Cayley hash functions) and the mathematics community (for Babai's conjecture) have been working independently on very similar problems. The goal of this paper is to bridge the results obtained by the two communities, with the cryptographic application in mind. In particular, we review known results coming from both sides, we provide some general attacks and design principles for the Cayley hash function construction, and finally we propose some parameters that can be considered as "safe" from our current knowledge of these problems.

Notation. In this paper, p will always be a prime and n a positive integer. We write $\mathbb{F}_q$ for the finite field with q elements. We identify the finite field $\mathbb{F}_{p^n}$ with $\mathbb{F}_p[X]/(q(X))$, where q is an irreducible polynomial over $\mathbb{F}_p$. If K is a finite field and m is a positive integer, we write $SL(m, K)$ for the special linear group of degree m over K, in other words, the group of m-by-m matrices over K with determinant 1. We write $PSL(m, K)$ for the projective special linear group of degree m over K, which is the quotient of $SL(m, K)$ by the set $\{\lambda I, \lambda \in K\}$. Finally, we write S_n for the group of permutations on n elements.

Outline. The remainder of this paper is organized as follows. In the first section we recall the Cayley

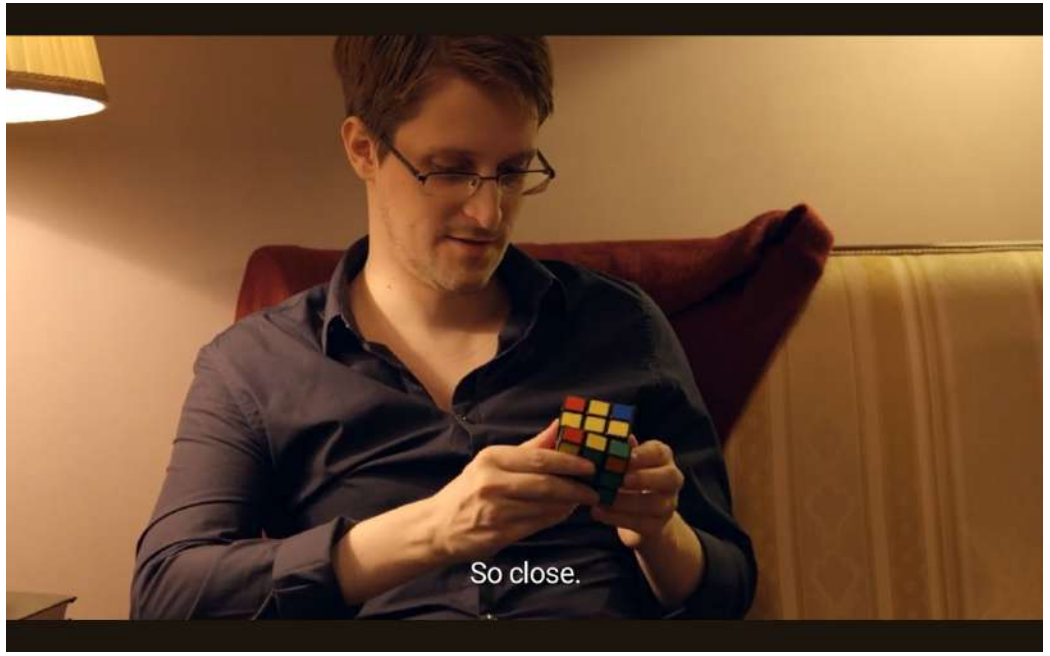
Christophe Petit is a research fellow of the Belgian Fund for Scientific Research (F.R.S.-FNRS) at Université catholique de Louvain (UCL). His email address is christophe.petit@uclouvain.be.

Jean-Jacques Quisquater is with the UCL Crypto Group. His email address is jjq@uclouvain.be.

DOI: http://dx.doi.org/10.1090/noti1001

Ce cube, signal convenu de Edward Snowden

- A-t-il sorti une carte micro SD ainsi de l'antre blindée de la NSA à Hawaï (2013) ? C'est que suggère le film « Snowden » (2016) et c'est Edward qui a écrit cette histoire … Rien n'est moins sûr cependant. Cela reste secret. Le modèle qu'Edward montre publiquement n'a été commercialisé qu'en 2014 …



- Par contre, il est bon pour les

résoudre …

La magie

Secrets and how to prove them: A magician's guide to zero-knowledge proofs

Michael Blau
09.08.23

https://a16zcrypto.com/posts/article/a-magicians-guide-to-zero-knowledge-proofs/

TAGS

tech trends

zero knowledge & succinct proof systems

share post

Any sufficiently advanced technology is indistinguishable from magic (or so science fiction writer Arthur C. Clarke famously said). One such area of science-fiction-like progress is that of zero-knowledge proofs (or ZKPs), a cryptographic tool that addresses two critical challenges in web3: scalability and privacy. In particular, ZKPs could be the key to unlocking lower transaction fees, designing new privacy-preserving applications, and, as a result, welcome the next billion crypto users. Even beyond crypto, ZKPs may one day help transmit sensitive data securely, combat illicit finance, or fight disinformation.

But what *are* ZKPs? There are many clever explanations out there for engineers, researchers, and the crypto community, but they aren't always intended for audiences with less experience in crypto or computer science. Even with the wealth of analogies available – from Waldo to Ali Baba's Cave – it's not easy to find an accurate, easy-to-grasp explanation of ZKPs that fully captures their superpowers.

So in this post, I combine my background in both crypto and magic to explore a new analogy: Think of ZKPs like a great magic trick. Check out the demo below, and read on for an overview of the defining properties (scalability and privacy) of ZKPs – and how all of this plays out using magic.

Magie : j’ai un secret que je ne révèle pas

π Numérique π Économie

Zero-knowledge : la solution aux problèmes de confidentialité sur la blockchain ?

Le 9 mars 2023 4 min. de lecture

Daniel Augot
directeur de recherche à l'Inria et responsable de la chaire Blockchain

En bref

- Le « zero-knowledge » est un concept du monde de la cryptomonnaie qui permet de prouver l'existence de certaines informations sans les divulguer.
- Cette technologie est à distinguer du chiffrement, où toutes les données sont accessibles dès lors qu'on possède la clé de déchiffrement.
- Les deux protocoles de preuve zero-knowledge les plus connus dans le monde de la blockchain sont les zk-STARKs et les zk-SNARKs.
- Ces protocoles présentent l'avantage de fournir des preuves plus courtes et plus rapides à vérifier.
- Le monde de la recherche n'a pas dit son dernier mot pour autant et cherche toujours à optimiser les performances de calcul et de vérification des données.

Dans le monde des blockchains et des cryptomonnaies, le concept de zero-knowledge est souvent évoqué comme une solution efficiente aux problèmes de confidentialité et de respect de la vie privée. En effet, le principe de cette technologie est de prouver l'existence de certaines informations sans avoir à les divulguer. Une avancée majeure qui n'obstrue pas la recherche sur les systèmes déjà existants.

La preuve « zero-knowledge » est-elle l'avenir des blockchains ?

Il faut dire que les cas pratiques autour de cette technologie sont nombreux. Elle peut notamment servir à vérifier l'identité d'une personne sans en révéler le nom. Si quelqu'un souhaite prouver qu'il a plus de 18 ans, il peut utiliser son permis de conduire. Cependant, ce geste révèlera non seulement des informations sur son âge, mais aussi son nom, sa date de naissance et un certain nombre de données personnelles. Une preuve « zero-knowledge » peut permettre de prouver que cette personne a plus de 18 ans, sans révéler aucune des informations figurant sur le permis de conduire.

Le zero-knowledge peut également prouver que quelqu'un a bien effectué une transaction sans en dévoiler le montant. Le processus ? La fonction dite de hachage cryptographique. Cette fonction de hachage, qui n'a pas d'équivalent dans le monde réel, est un algorithme qui transforme n'importe quel donnée numérique (une image, un fichier texte, etc.) en une valeur de taille fixe, comme une suite de 256 bits. Par exemple, le standard SHA-256

Dans la même thématique :

Vers un internet quantique grâce à la téléportation

Ukraine : une guerre hybride sur le terrain de la désinformation

IA Act : quels impacts pour les secteurs sensibles en Europe ?

Histoire rapide de la cryptographie civile

- Cryptographie
  - Clé publique
  - Clé secrète
  - Post-quantique

- **Protocole zero-knowledge**

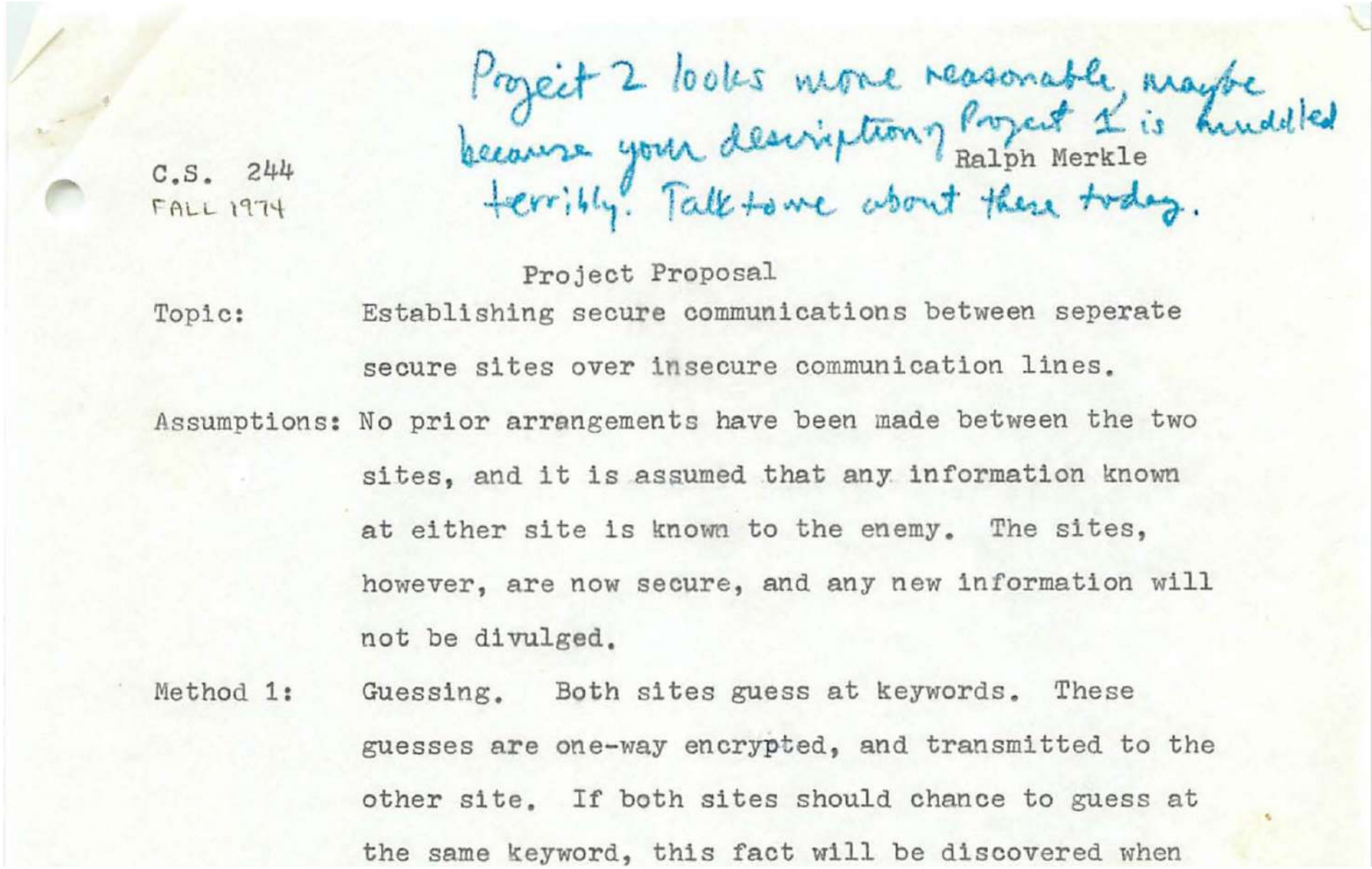
- Systèmes homomorphiques

- MPC (https://www.mpcalliance.org/) : multi party computation

Histoire : plus de détails

- Système à clé publique : Diffie-Hellman, Merkle
  - Turing
  - Factorisation (Don Knuth, Jevons)
  - Exponentielle (John Gill III : relation avec Norbert Cot)
- signature
- RSA
- Système basé sur l'identité
  - Carte à puce (éviter le détournement, vu de France)
  - Shamir (presque correct)
- Goldwasser, Micali, Rackoff
- Fiat-Shamir
- Astuce Fiat-Shamir pour non-interactif
- Guillou-Quisquater (Desmedt, Simmons)
- Etc

Idée de Ralph Merkle (automne 1974)



Project 2 looks more reasonable, maybe because your description Project 1 is muddled terribly. Talk to me about these today.
Ralph Merkle

C.S. 244
FALL 1974

Project Proposal

Topic: Establishing secure communications between seperate secure sites over insecure communication lines.

Assumptions: No prior arrangements have been made between the two sites, and it is assumed that any information known at either site is known to the enemy. The sites, however, are now secure, and any new information will not be divulged.

Method 1: Guessing. Both sites guess at keywords. These guesses are one-way encrypted, and transmitted to the other site. If both sites should chance to guess at the same keyword, this fact will be discovered when

For more information about the events in the Fall of 1974, you can read the Computer History Museum's interview:

Computer History Museum

Ralph Merkle: 2011 Fellows Interview
Public-Key Cryptography

CS 244

In the Fall of 1974, as an undergraduate, I enrolled in CS244, the Computer Security course offered at UC Berkeley and taught by Lance Hoffman. We were required to submit two project proposals, one of which we would complete for the course. I submitted a proposal for what would eventually become known as Public Key Cryptography -- which Hoffman rejected. I dropped the course, but kept working on the idea.

Unfortunately, I lost track of the proposal and didn't find it again until September 8th, 2005, while cleaning out some boxes of old folders. There, neatly labeled "244 Project Proposal" was a folder containing the original 7 page project proposal. I've scanned it in for those interested in this bit of historical arcana.

The original CS244 project proposal from Fall of 1974 (7 page PDF).

Besides describing "Method 1," now better known as the puzzles method, the project proposal goes on to discuss "Method 2" which involved converting a "two-way encryption technique" into an "apparently one-way encryption technique" which would then be transmitted to the "other site" which would use it to encrypt messages. The only way to decrypt the messages would be with the original "two-way technique from which it [the one-way technique] was derived." The project proposal notes that "This method would also have advantages in other applications..."

After Hoffman rejected this proposal, I rewrote it to be shorter and simpler. Following is the two-page simplified version, resubmitted to Hoffman and showing his comments.

The second project proposal (2 page PDF).

Submitting to CACM

Hoffman continued to show little interest so I dropped the course, but kept working on the idea. I showed an early draft to Bob Fabry, then on the faculty at Berkeley, who immediately recognized it as both novel and valuable and said "Publish it, win fame and fortune!" I then submitted it to Susan Graham, then an Editor at the Communications of the ACM in August of 1975. As I was to learn, Fabry's response was rare.

Graham sent my submitted paper out for review and received the following response from an "experienced cryptography expert" whose identity is unknown to this day:

> "I am sorry to have to inform you that the paper is not in the main stream of present cryptography thinking and I would not recommend that it be published in the Communications of the ACM."
>
> "Experience shows that it is extremely dangerous to transmit key information in the clear."

With this blanket rejection of public key cryptography by an "expert", she rejected my article. She "was particularly bothered by the fact that there are no references to the literature. Has anyone else ever investigated this approach. If they consider it and reject it, why?"

I had failed to provide any references to the prior work on public key cryptography, and the reasons previous workers in the field had rejected it as impossible. I should have looked up "public key cryptography" on Google before submitting my paper. My defense is feeble: there was no Google, the term "public key cryptography" did not yet exist, and there were no previous workers in the field. There were no words for what I had done, and looking up a concept to show that no one had previously thought of it is difficult. This is not a unique problem: it illustrates a problem faced by anyone trying to explain a new idea to an "expert" who expects a properly referenced article anytime anyone tries to explain something to them. The more a new idea is unrelated to any prior idea or concept the more it must appear as a squawling bastard, naked and alone, appearing de novo and lacking any respectable pedigree or family to vouch for its acceptability.

I have a copy of the paper apparently made shortly after the first rejection, which includes revisions to make it so obvious that even the "cryptography expert" would be able to understand it. It is dated December 7th 1975.

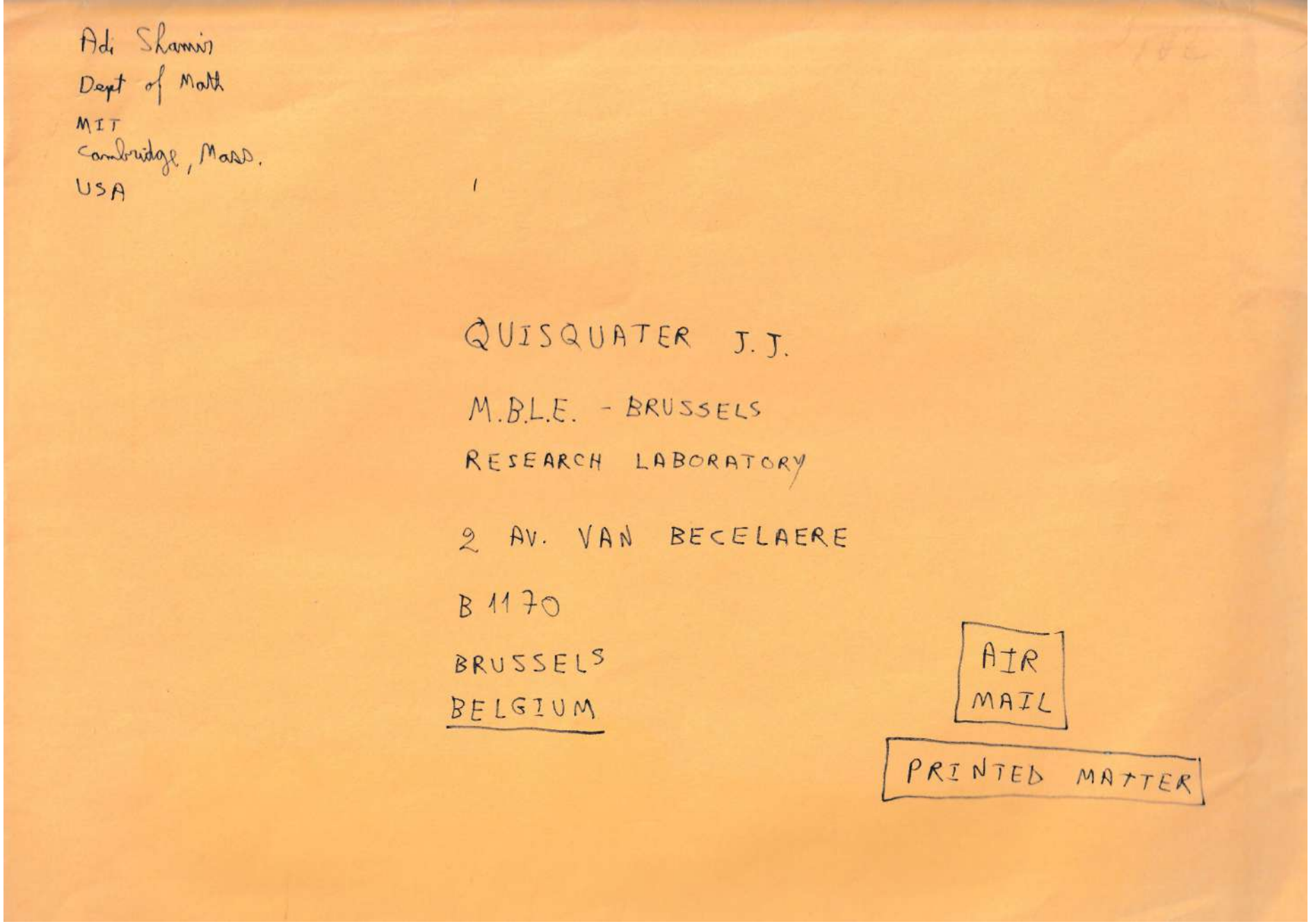
The first rejection by CACM left me confident that no one had previously investigated this approach, as the "experienced cryptography expert" had rather obviously failed to understand what was being proposed and private conversations suggested that no one else had heard of the idea, either. So I persisted for the simple reason that (a) the idea was sound, so CACM would eventually have to concede this fact and publish the article and (b) they would then have to include the original submission date -- which I would lose if I re-submitted anywhere else, even if that somewhere else miraculously had a clearer understanding of the concept.

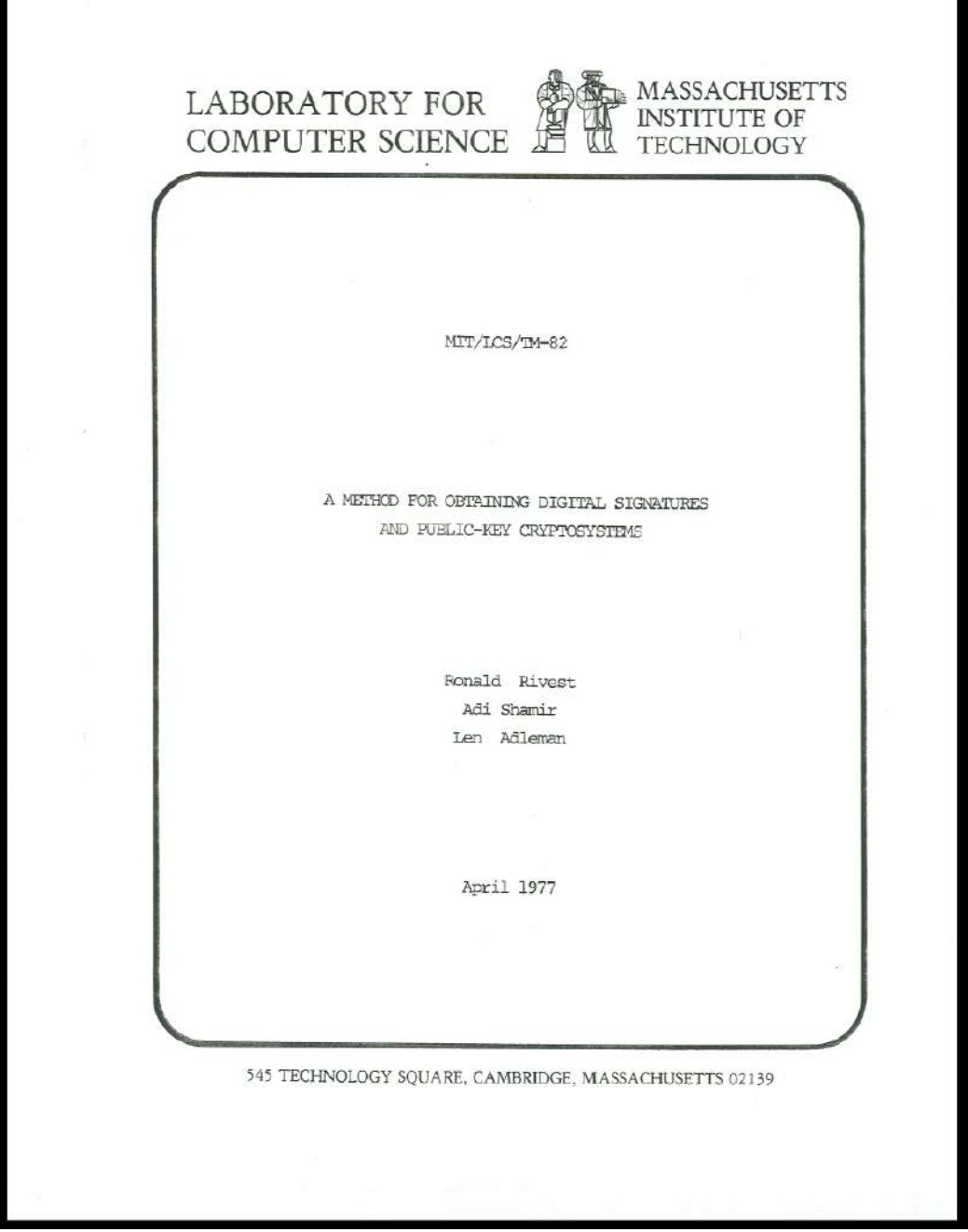
And so it proved. CACM eventually published the paper, though only after almost three years of delay, and only after others (who were better able to persuade their editors to publish in a timely fashion).

For historical background, see *The First Ten Years of Public-Key Cryptography*, by Whitfield Diffie, Proc. IEEE, Vol. 76, No. 5, May 1988, pages 560-577.

MIT-TM-82

RSA


Ad. Shamir
Dept of Math
MIT
Cambridge, Mass.
USA
QUISQUATER J. J.
M.B.L.E. - BRUSSELS
RESEARCH LABORATORY
2 AV. VAN BECELAERE
B 1170
BRUSSELS
BELGIUM
AIR MAIL
PRINTED MATTER



LABORATORY FOR COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT/LCS/TM-82

A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS

Ronald Rivest
Adi Shamir
Len Adleman

April 1977

545 TECHNOLOGY SQUARE, CAMBRIDGE, MASSACHUSETTS 02139

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*

by R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science
Technical Memo LCS/TM82
Cambridge, Mass. 02139
April 4, 1977 (Revised December 12,1977)

Abstract

We present an encryption method with the novel property that publicly revealing an *encryption* key does not thereby reveal the corresponding *decryption* key. This has two important consequences:

(1) Couriers or other *secure* means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

(2) A message can be "signed" using a privately-held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

A message is encrypted by representing it as a number M, raising M to a publicly-specified power e, and then taking the remainder when the result is divided by the publicly specified product n of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $ed \equiv 1 (\mathrm{mod} (p-1)\times(q-1))$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

Key words and phrases: digital signatures, public-key cryptosystems, privacy, authentication, security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.

CR categories: 5.25, 3.15, 3.50, 3.81, 2.12

* This research was supported by National Science Foundation grant MCS76-14294, and the Office of Naval Research grant number N00014-67-A-0204-0063.

- A-B : Alice et Bob
- Preuve
- Preuve que j’ai une preuve
- Alors on ne peut pas me copier
- Prouveur et vérifieur
-

preuve

- Une preuve est un élément matériel, un témoignage ou un raisonnement servant à établir de manière certaine la vérité ou la réalité d'un fait, d'un acte ou d'un sentiment. Elle permet de démontrer, de vérifier ou d'attester une affirmation. (Larousse)

- vraisemblance

Preuve par 9

N		R
24		6
x 12		x 3
48		
24		
288	⇨ 9 ⇨ 0	18 ⇨ 0

Si preuve est OK,
le résultat peut être faux

Si la preuve rate,
le résultat est faux.

298 ?

Autre exemple : Algorithme de Luhn

Luhn Algorithm

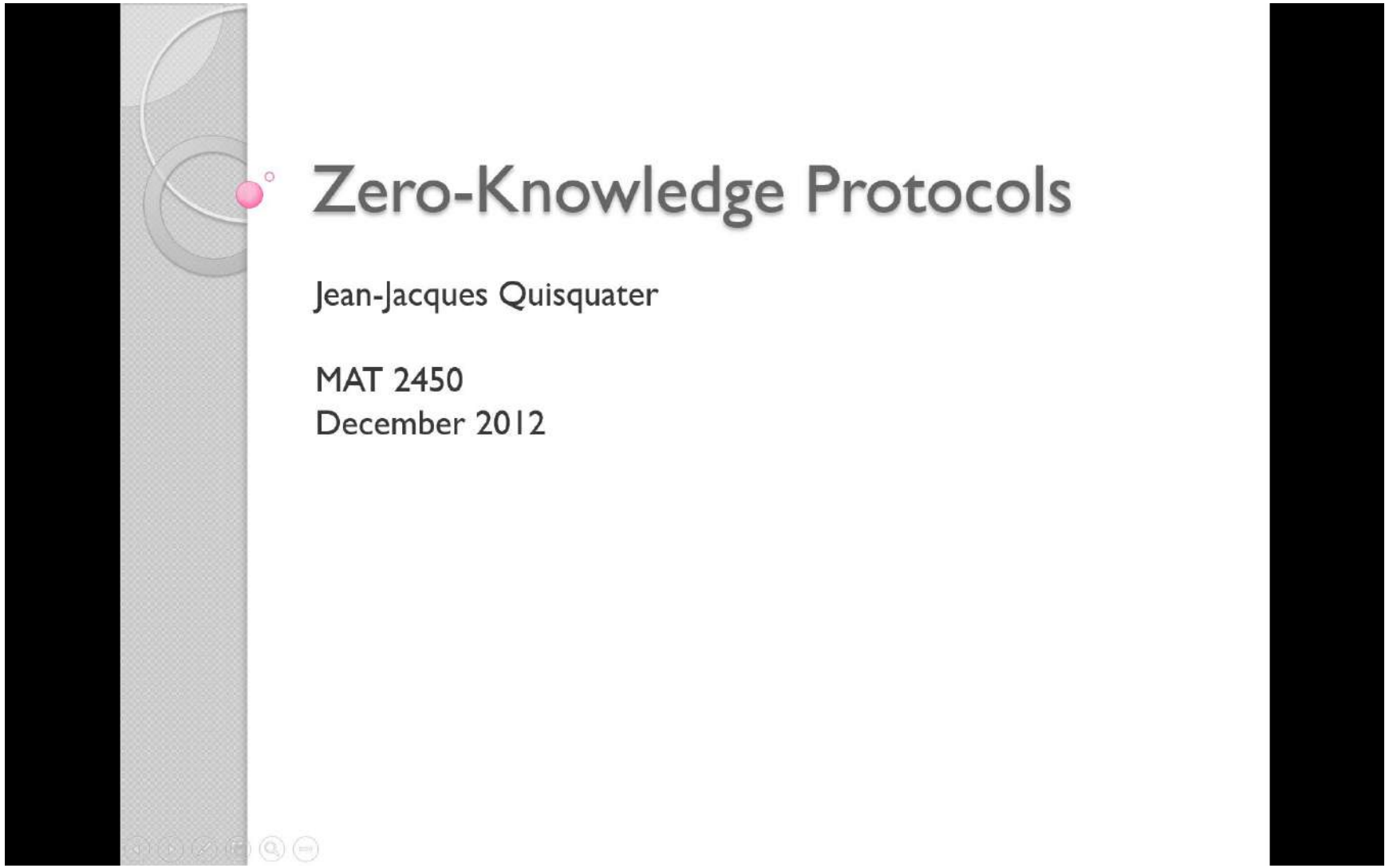
4	2	6	3	9	8	2	6	4	0	2	6	9	2	9	9
x2		x2		x2		x2		x2		x2		x2		x2	
8	2	12	3	18	8	4	6	8	0	4	6	18	2	18	9
8	2	2+1	3	1+8	8	4	6	8	0	4	6	1+8	2	1+8	9
8	2	3	3	9	8	4	6	8	0	4	6	9	2	9	9

rightmost digit, double the value of every second digit

8 + 2 + 3 + 3 + 9 + 8 + 4 + 6 + 8 + 0 + 4 + 6 + 9 + 2 + 9 + 9 = 90

90 Modulo(%) 10 = 0 Then **4263982640269299** Valid Number

Cours de math : MAT 2450 : UCLouvain



Access control
(login: Baran, 1963)

User (prover)
visitor
driver
card

Computer (verifier)
warden
car
terminal

- ☹ spy (on-line)
- ☹ fake prover (copy or false identity)
- ☹ fake verifier
- ☹ database of users and passwords (hash or ?)

Problems: **prover** side

- Copy of the password (stealing, coercion, radiations, …), and use in another context,

- Spying during the communication, …

Problems: **verifier** side

- Terminal side: (fake terminal, coercion, radiations, …),
- Several terminals for verification,
- How to verify? Need of some initial reference!

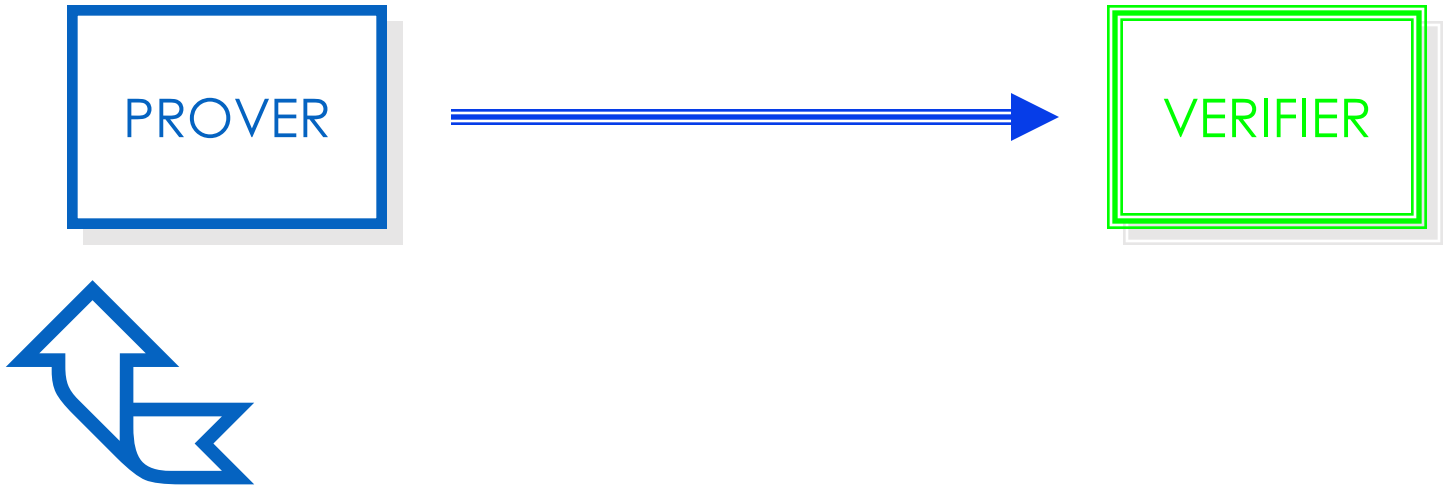
Better?

- One-time password! Any copy is not useful anymore,
- Solution: don’t use the password!
- Implementations!

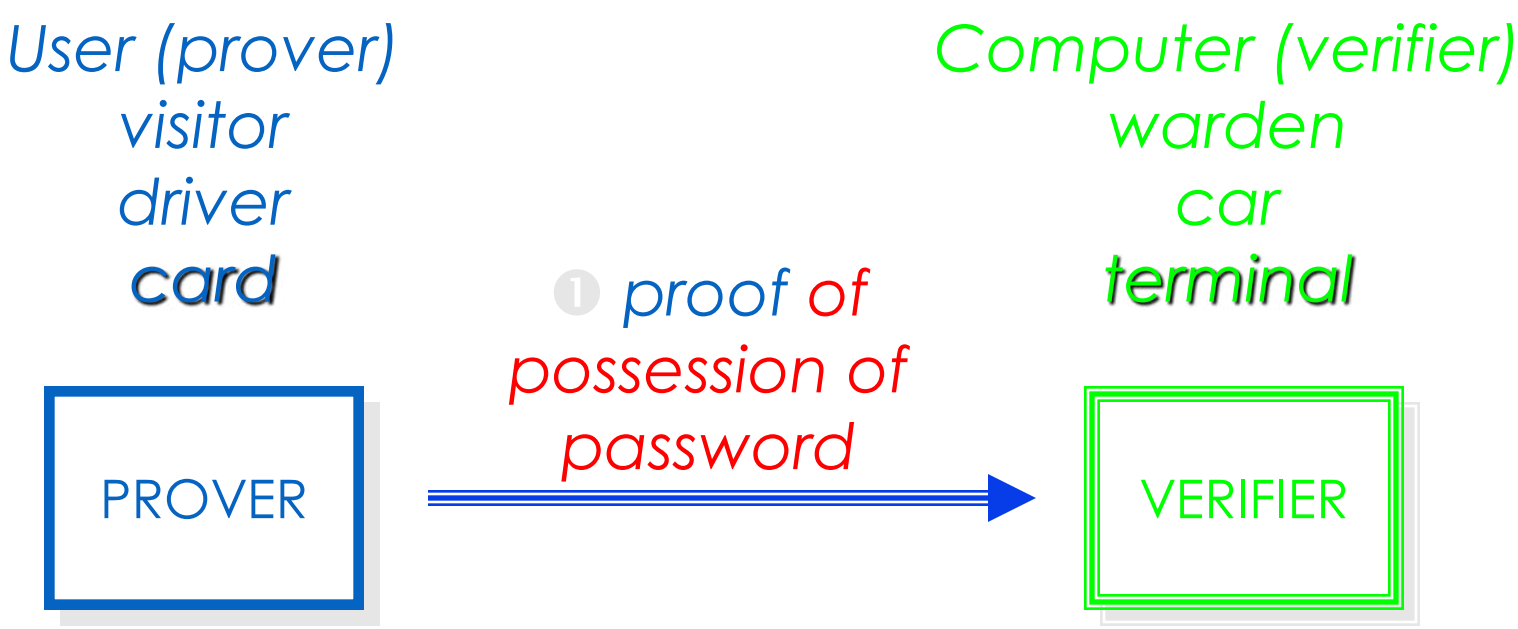
solutions

User (prover)
visitor
driver
card

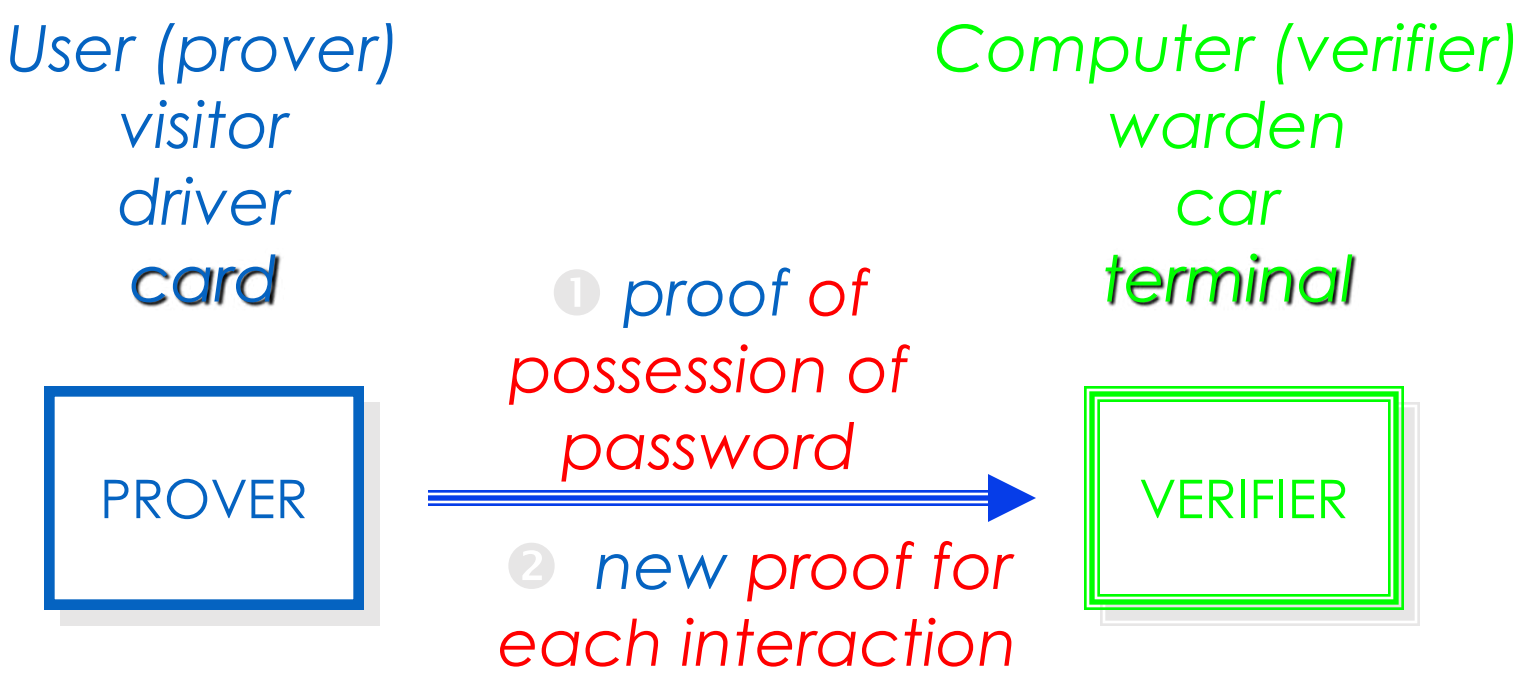
Computer (verifier)
warden
car
terminal



solutions


User (prover)
visitor
driver
card
Computer (verifier)
warden
car
terminal
1 proof of possession of password
PROVER
VERIFIER

solutions


User (prover)
visitor
driver
card
Computer (verifier)
warden
car
terminal
PROVER
1 proof of possession of password
2 new proof for each interaction
VERIFIER

solutions

User (prover)
visitor
driver
card

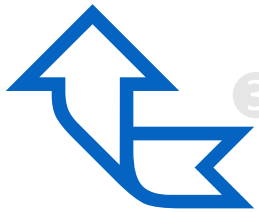
Computer (verifier)
warden
car
terminal

PROVER

❶ *proof of possession of password*

❷ *new proof for each interaction*

VERIFIER



❸ no possible copy of password (always inside) and tamperresistant object

Smart cards

- Physically secure object (permament memory, …),
- Computing power for cryptography,
- Related to people (PIN, biometry?, possession, …)

What is a Zero- Knowledge Proof?

A **zero−knowledge proof** is a way that a “**prover**” can prove possession of a certain piece of information (bits) to a “**verifier**” without revealing it.

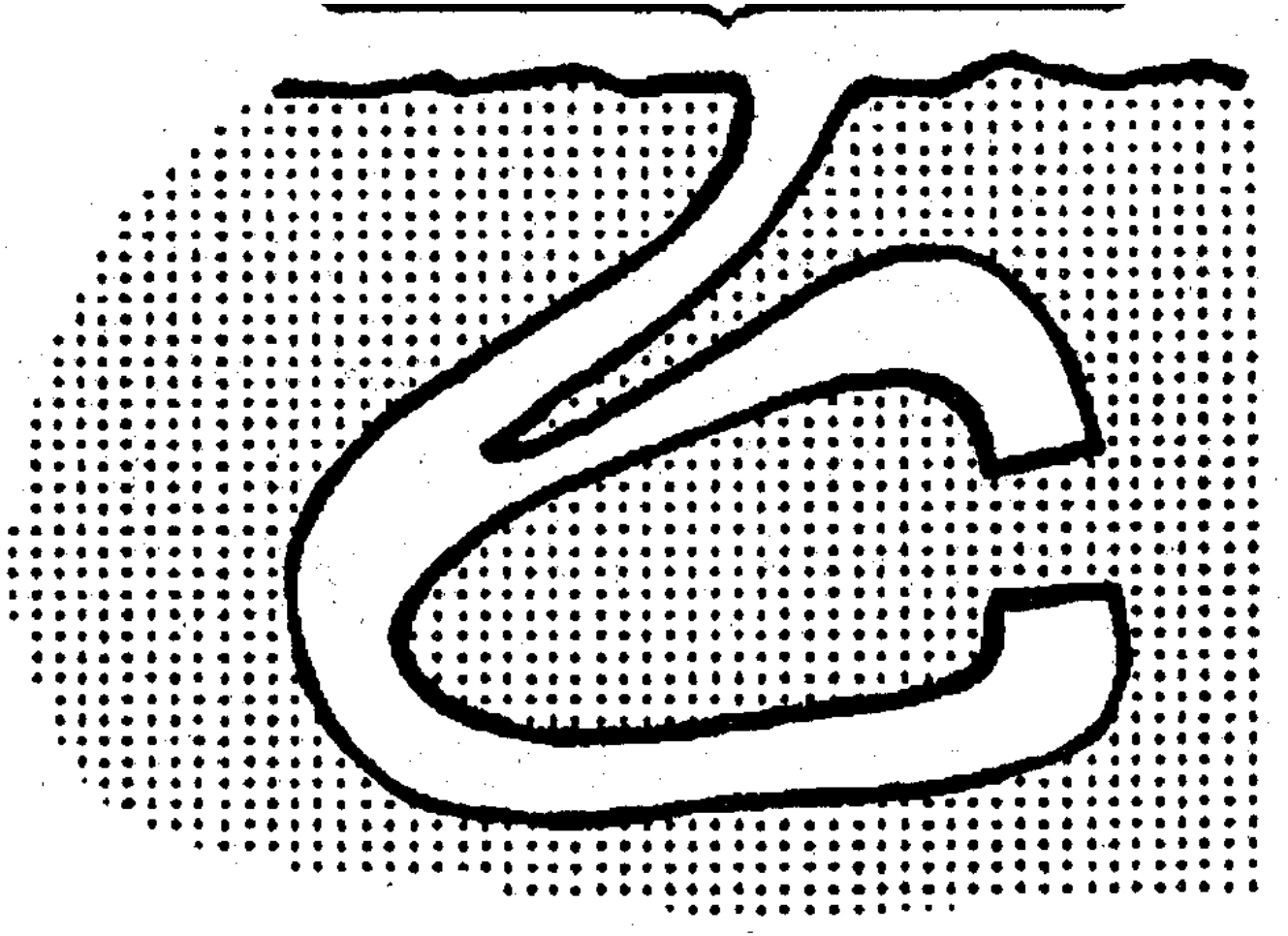
This is done by manipulating data provided by the verifier in a way that would be impossible without the secret information in question.

A third party, reviewing the transcript created, cannot be convinced that either prover or verifier knows the secret.

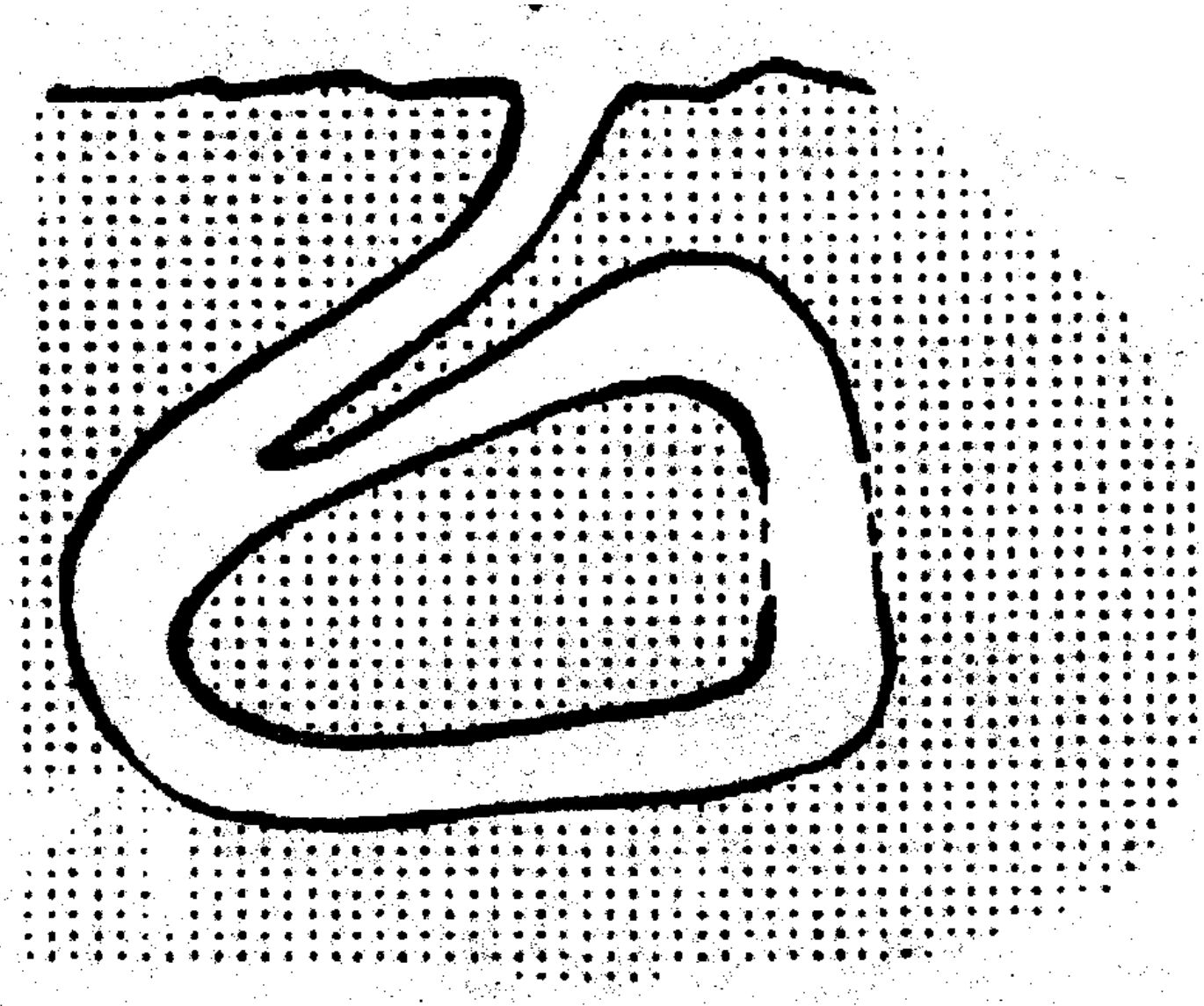
Proof of possession of password

- Protocols zero-knowledge (Fiat-Shamir, GQ, …)
- Only using the password in an internal computation
- Verification of the proof is very specific

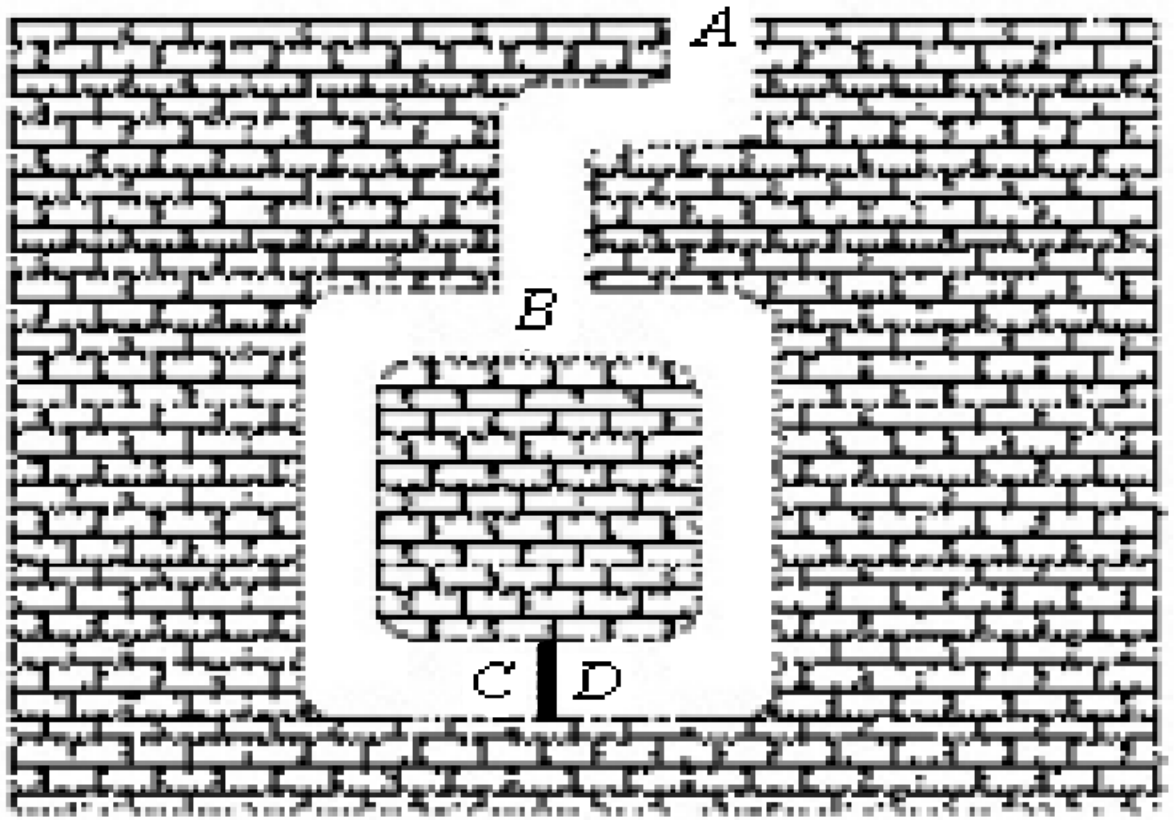
The Cave of the Forty Thieves (Ali-Baba) : original



The Cave of the Forty Thieves



Une autre



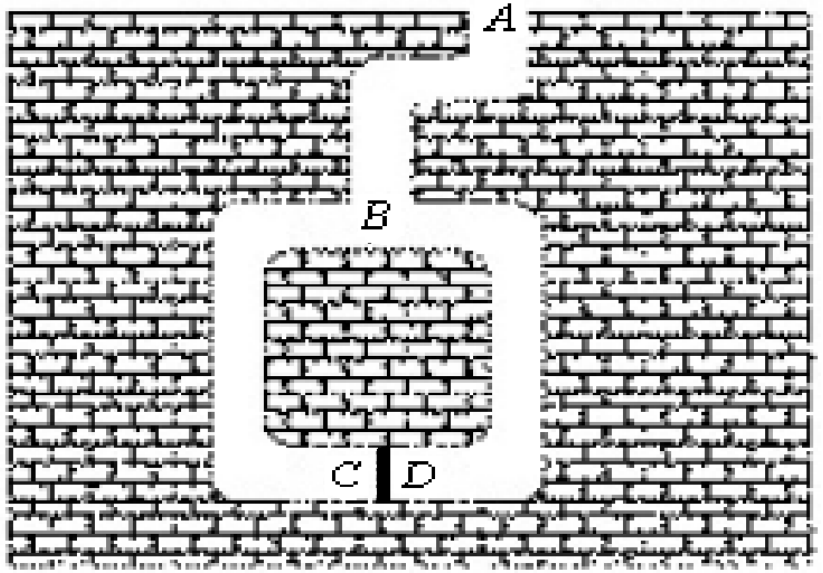
Peggy knows the secret of the cave. She wants to prove her knowledge to Victor, but she doesn't want to reveal the magic words.

Here's how she convinces him:

(1) Victor stands at point *A*.

(2) Peggy walks all the way into the cave, either to point *C* or point *D*.

(3) After Peggy has disappeared into the cave, Victor walks to point *B*.



(4) Victor shouts to Peggy, asking her either to:

(4.1) come out of the left passage or

(4.2) come out of the right passage.

(5) Peggy complies, using the magic words to open the secret door if she has to.

(6) Peggy and Victor repeat steps (1) through (5) *n* times.

Comment.

The technique used in this protocol is called cut and choose, because of its similarity to the classic protocol for dividing anything fairly:

(1) Peggy cuts the thing in half.

(2) Victor chooses one of the halves for himself.

(3) Peggy takes the remaining half.

It is in Peggy's best interest to divide fairly in step (1), because Victor will choose whichever half he wants in step (2).

Properties of Zero-Knowledge Proofs

- **Completeness** – A prover who knows the secret information can prove it with probability 1.
- **Soundness** – The *probability* that a prover who does not know the secret information can get away with it can be made *arbitrarily small*.

Computational Assumptions

- A zero-knowledge proof assumes the prover possesses unlimited computational power.
- It is more practical in some cases to assume that the prover's computational abilities are bounded. In this case, we have

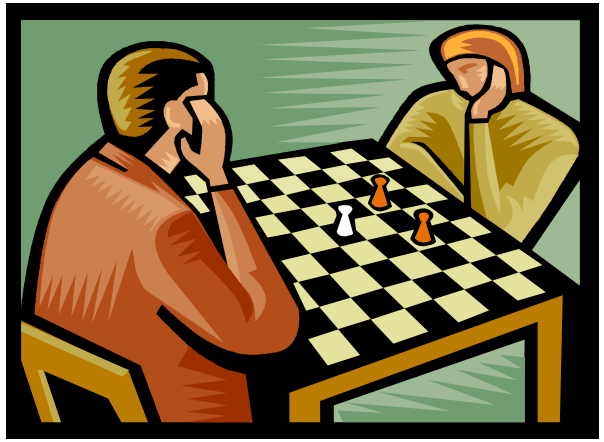
a zero-knowledge argument.

Applications

- Zero-knowledge proofs can be applied where secret knowledge too sensitive to reveal needs to be verified
- Key authentication
- PIN numbers
- Smart cards

Limitations

- A zero-knowledge proof is only as good as the secret it is trying to conceal
- Zero-knowledge proofs of identities in particular are problematic
- The Grandmaster Problem
- The Mafia Problem
- etc.



Identification Tokens — or: Solving The Chess Grandmaster Problem

Thomas Beth
Fakultät für Informatik
Universität Karlsruhe
Germany

*Yvo Desmedt**
Dept. EE & CS
Univ. of Wisconsin – Milwaukee, U.S.A.

Abstract. *Fiat and Shamir have proposed to use zero-knowledge interactive proofs to obtain secure identification mechanisms. Real time attacks in which active eavesdroppers relay questions and answers or in which the prover helps deliberately an impersonator have been described [4]. In this paper a solution against such frauds is given and (based on some physical assumptions) it is proved that the solution protects against the real-time attacks.*

1 Introduction

The use of zero-knowledge interactive proof systems for identification purposes was proposed by Fiat and Shamir [7]. Later Fiat and Shamir [8] have extended this idea to the process of identification *without* having to rely on physical description (see also [6]).

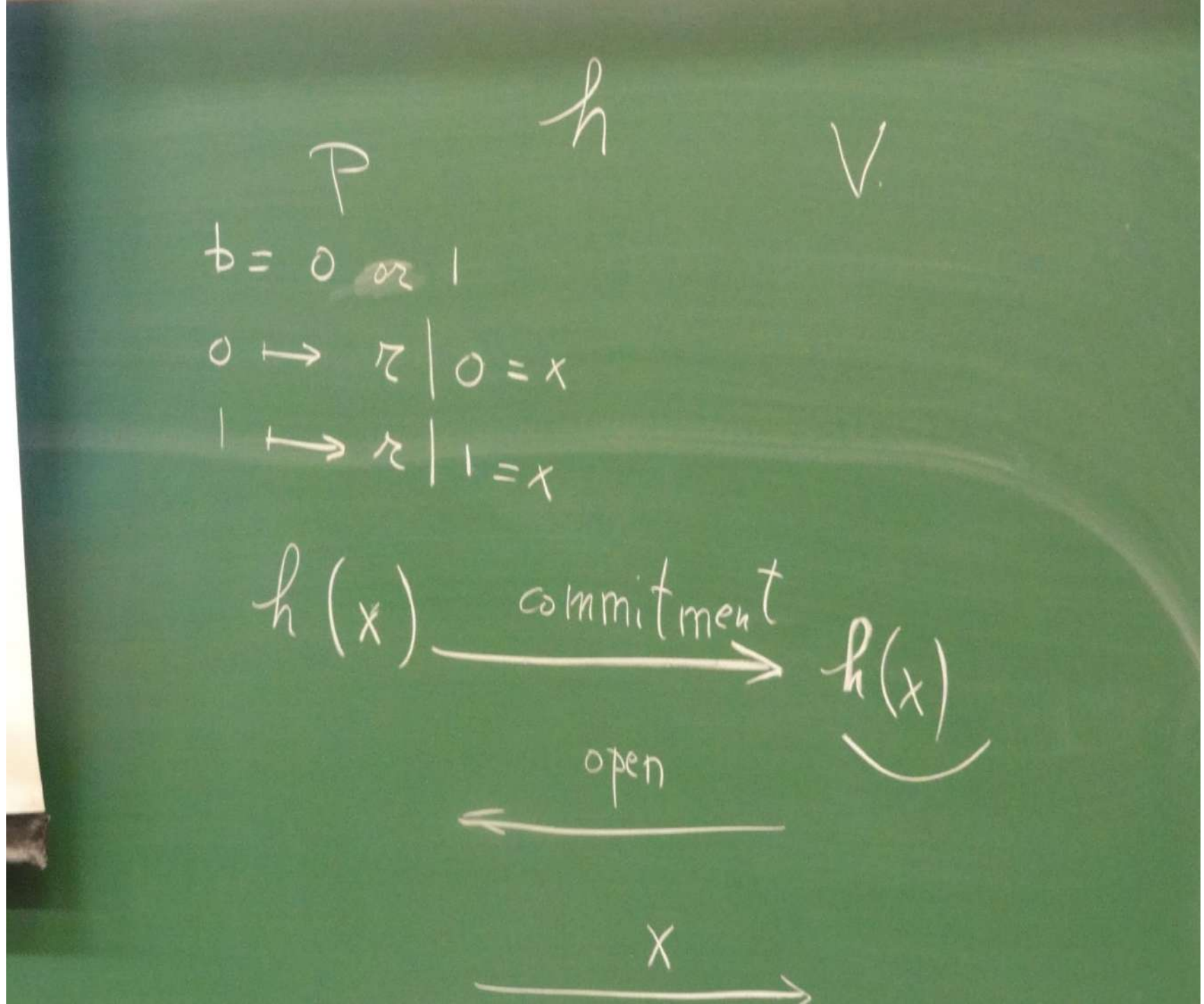
In this paper we will describe interactive proof systems and the process of identification from a game theoretic viewpoint. The game model is an essential tool in this paper. It will allow us to formalize the concept of the so called *mafia* and *terrorist* fraud [4] based on the idea of simultaneous display [2]. The *purpose* of this paper is to present a model which allows to *solve* the "Chess Grandmaster" problem, into which the identification problem will be converted. Such a model enables us to present an identification scheme which is provably secure against the aforementioned real-time attacks. This scheme does not rely on physical description of the individual who is identifying himself. We are not concerned about the rental fraud [4], but we will discuss it briefly at the end.

*Work done while visiting the EISS, University of Karlsruhe, West Germany.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 169-176, 1991.

GQ protocol (1988)

- **System Parameters**
  - Private: p, q, $s=v^{-1} \bmod \phi(n)$
  - $n = pq$, $v > 2$
- **User Parameters**
  - The secret of A with $J_A=f(I_A)$ is $J_A^{-s} \bmod n$
- **Protocol Messages** *(Repeat t times)*
  - A sends to B(Commit): I_A, $x=r^v \bmod n$ for a random r
  - B sends to A(Challenge): a random *e* with $1=<e=<v$
  - A sends to B(Response): $y=r\, s_A^e \bmod n$
- **Verify**
  - B computes $z = J_A^e y^v \bmod n$
  - Accept A's proof of identity if $z = x$ and $z \neq 0$


h
P
V
b = 0 or 1
0 ⟼ r | 0 = x
1 ⟼ r | 1 = x
h(x)
commitment
h(x)
open
x

h : r

"RSA" $n = p \cdot q$, $\underset{\sim}{s}$, $\underset{\sim}{v}$

n, v : public

$$r^v \bmod n = x$$

GQ Identification Protocol

A *B*

$I_A, x \equiv r^v \pmod{n}$

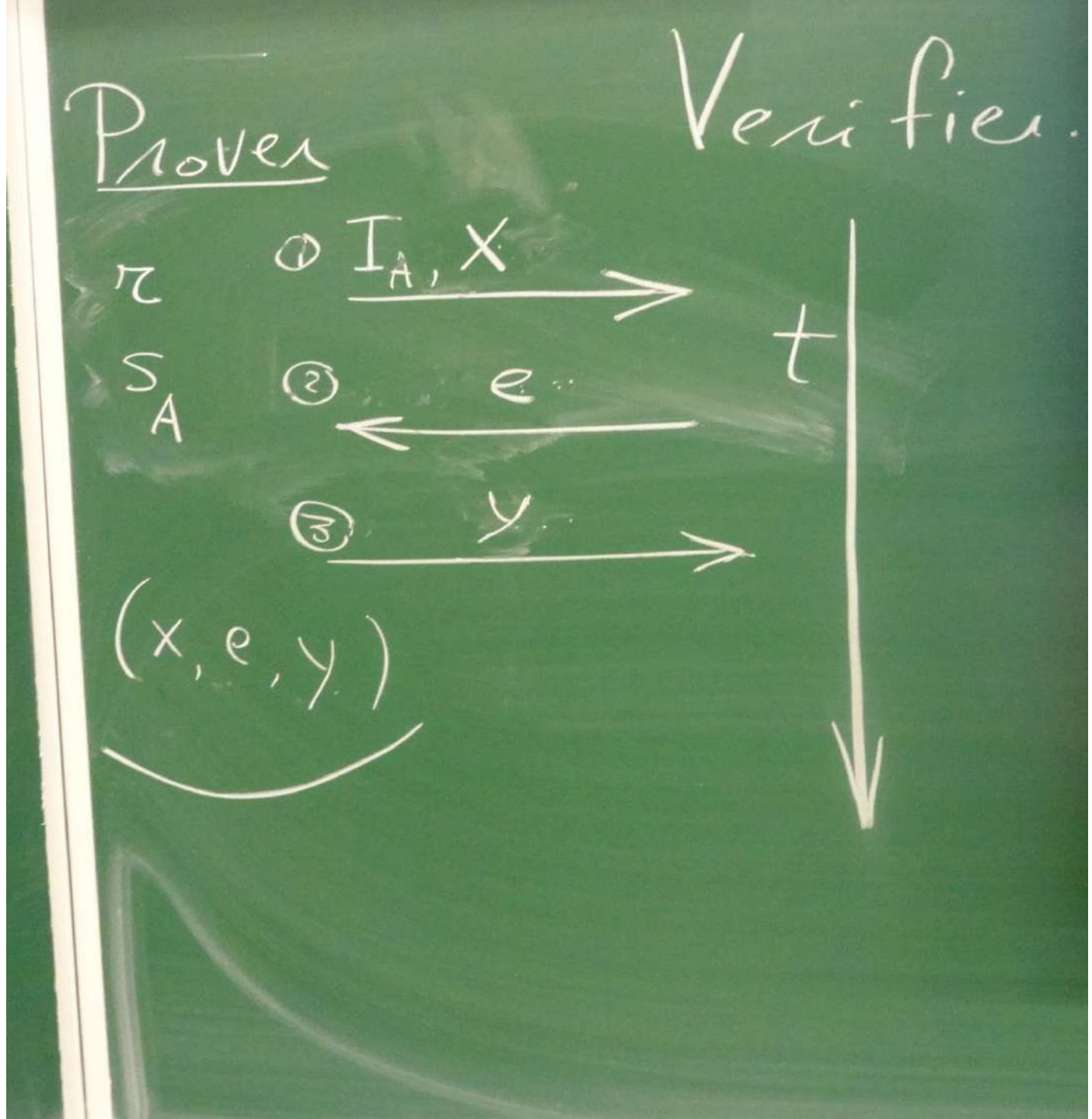
e, where $1 \le e \le v$

$y \equiv r \cdot s_A^e \pmod{n}$

If $z \equiv J_A^e \cdot y^v \not\equiv 0 \pmod{n}$ and $z \equiv x$,

then B accepts the proof;

otherwise, B rejects the proof.


Prover
Verifier
r
① I_A, X
s_A
② e
t
③ y
(x, e, y)

Goldwasser, Micali et Rackoff (GMR)

- Manuscrit de 1982 (!), pas accepté facilement : refusé 3 fois (FOCS 83 et 84, STOC 84), accepté à STOC 85 (extended abstract), et finalement publié en 1989, dans SIAM J. Computing,

- Donc, pas présenté à une conférence CRYPTO,

ARTICLE | FREE ACCESS

The knowledge complexity of interactive proof-systems

Authors: S Goldwasser, S Micali, C Rackoff | Authors Info & Claims

STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing • Pages 291 - 304
https://doi.org/10.1145/22145.22178

Published: 01 December 1985 Publication History | Check for updates

The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser, MIT
Silvio Micali, MIT
Charles Rackoff, University of Toronto

1. Introduction

In the first part of the paper we introduce a new theorem-proving procedure, that is a new *efficient method of communicating a proof*. Any such method implies, directly or indirectly, a definition of proof. Our "proofs" are probabilistic in nature. On input an n-bits long statement, we may erroneously be convinced of its correctness with very small probability, say, $\frac{1}{2^n}$, and rightfully be convinced of its correctness with very high probability, say, $1 - \frac{1}{2^n}$. Our proofs are *interactive*. To efficiently verify the correctness of a statement, the "recipient" of the proof must actively ask questions and receive answers from the "prover".

In the second part of the paper, we address the following question:

How much knowledge should be communicated

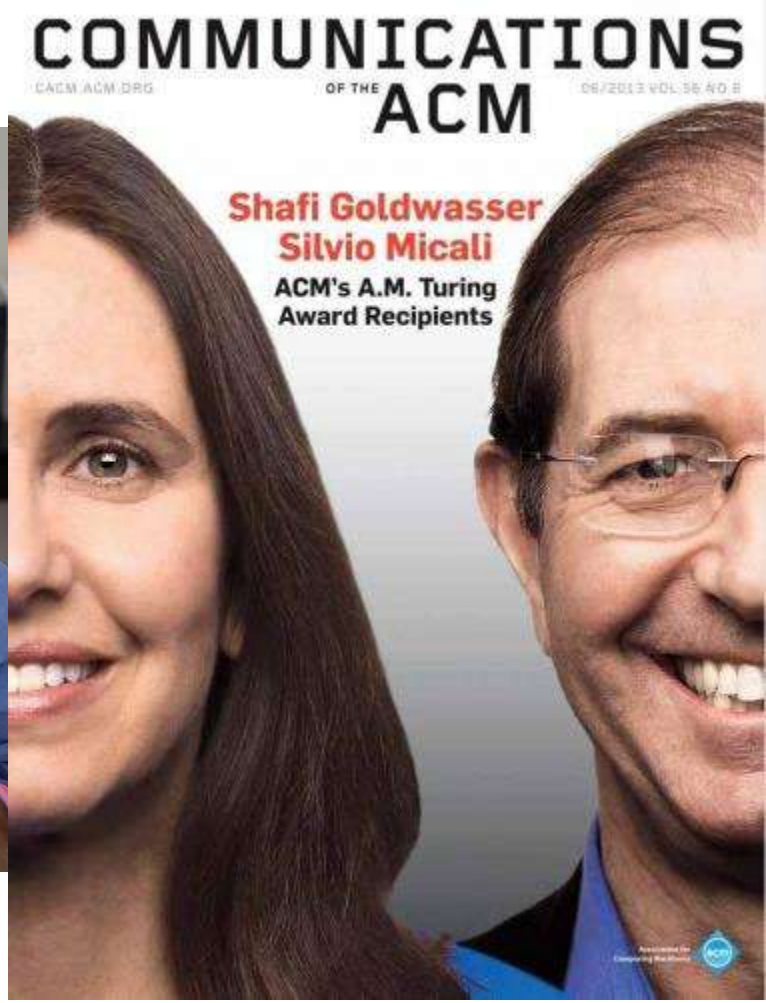
We propose to classify languages according to the amount of additional knowledge that must be released for proving membership in them.

Of particular interest is the case where this additional knowledge is essentially 0 and we show that is possible to interactively prove that a number is quadratic non residue mod m releasing 0 additional knowledge. This is surprising as no efficient algorithm for deciding quadratic residuosity mod m is known when m's factorization is not given. Moreover, all known NP proofs for this problem exhibit the prime factorization of m. This indicates that adding interaction to the proving process, may decrease the amount of knowledge that must be communicated in order to prove a theorem.

2. Interactive Proof Systems

Much effort has been previously devoted to make precise the notion of a theorem-proving pro-

Du doctorat à Berkeley (1982) au Prix Turing (2012) via le MIT (1983-…)



Rencontres

- Premier CRYPTO 81 : je n’y vais pas
- A CRYPTO 82, Louis rencontre Shafi et Silvio
- « coup de foudre scientifique » de la part de Louis
- Je les rencontre à CRYPTO 83 : jeu subtil sur la plage SB avec Silvio
- Et je comprends très vite qu’ils ont découvert une pépite sans en savoir bien plus

Gilles Brassard et Philips Research

- 3 mois au printemps 1988
- Élaboration de la caverne d’Alibaba
- Éditeur des proceedings de CRYPTO 89 où se trouve le papier original de la caverne

Gilles Brassard et la France (ENS)

- 1994 (CNRS, ENS-Ulm)

- Donne cours au DEA

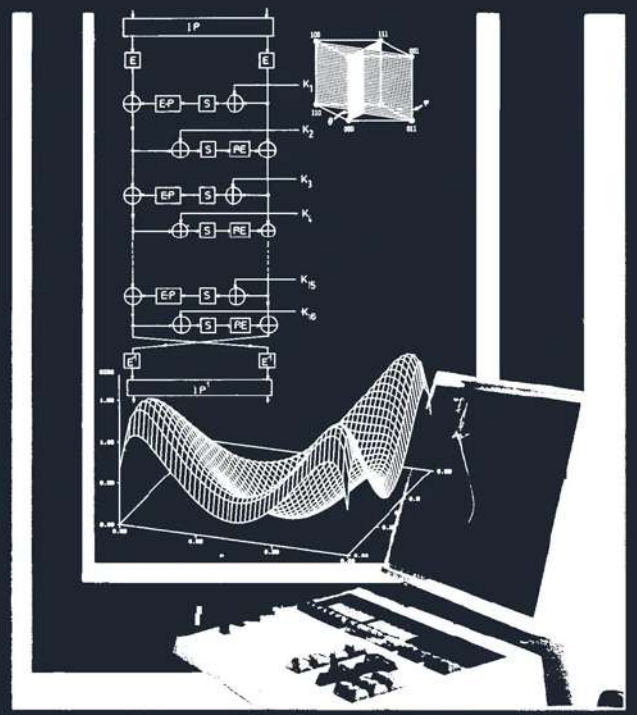
Claude Crépeau et ZK

- Cours commun à l'ENS-Ulm : 1995 (?)

- Idée du clavier pour code secret

ADVANCES IN CRYPTOLOGY

Proceedings of Crypto 83



Edited by David Chaum

Brevets

RSA Lab

6.3.5 WHAT ARE THE IMPORTANT PATENTS IN CRYPTOGRAPHY?

Here is a selection of some of the important and well established patents in cryptography, including several expired patents of historical interest. The expiration date for patents used to be 17 years after issuing, but for outstandning patents as of June 8, 1995 (the day the United States ratified the GATT patent treaty), the expiration date is 17 years after the date of issue or 20 years after the date of filing, whichever is later. Today, the expiration date for U.S. patents is 20 years from filing, pursuant to the international standard.

DES
U.S. Patent 3,962,539
Filed: February 24, 1975
Issued: June 8, 1976
Inventors: Ehrsam et al.
Assignee: IBM

This patent covered the DES cipher and was placed in the public domain by IBM. It is now expired.

Diffie-Hellman
U.S. Patent 4,200,770
Filed: September 6, 1977
Issued: April 29, 1980
Inventors: Hellman, Diffie, and Merkle
Assignee: Stanford University

This is the first patent covering a public-key cryptosystem. It describes Diffie-Hellman key agreement, as well as a means of authentication using long-term Diffie-Hellman public keys. This patent is now expired.

Public-key cryptosystems
U.S. Patent 4,218,582
Filed: October 6, 1977
Issued: August 19, 1980
Inventors: Hellman and Merkle
Assignee: Stanford University

The Hellman-Merkle patent covers public-key systems based on the knapsack problem and now known to be insecure. Its broader claims cover general methods of public-key encryption and digital signatures using public keys. This patent is expired.

RSA
U.S. Patent 4,405,829
Filed: December 14, 1977
Issued: September 20, 1983
Inventors: Rivest, Shamir, and Adleman
Assignee: MIT

This patent describes the RSA public-key cryptosystem as used for both encryption and signing. It served as the basis for the founding of RSADSI.

Fiat-Shamir identification
U.S. Patent 4,748,668
Filed: July 9, 1986
Issued: May 31, 1988
Inventors: Shamir and Fiat
Assignee: Yeda Research and Development (Israel)

This patent describes the Fiat-Shamir identification scheme.

Control vectors
U.S. Patent 4,850,017
Filed: May 29, 1987
Issued: July 18, 1989
Inventors: Matyas, Meyer, and Brachtl
Assignee: IBM

Patent 4,850,017 is the most prominent among a number describing the use of control vectors for key management. This patent describes a method enabling a description of privileges to be bound to a cryptographic key, serving as a deterrent to the key's misuse.

GQ identification
U.S. Patent 5,140,634
Filed: October 9, 1991
Issued: August 18, 1992
Inventors: Guillou and Quisquater
Assignee: U.S. Phillips Corporation

This patent describes the GQ identification scheme.

Protocole Fiat-Shamir

(CRYPTO 86)

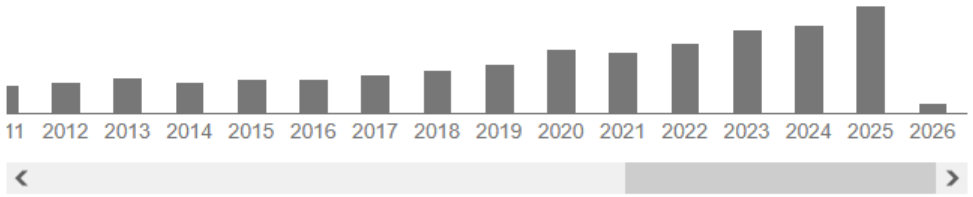
avec citations

← View article

Amos Fiat

How to prove yourself: Practical solutions to identification and signature problems

Authors	Amos Fiat, Adi Shamir
Publication date	1987
Journal	Advances in Cryptology—Crypto'86
Pages	186-194
Publisher	Springer Berlin/Heidelberg
Description	In this paper we describe simple identification and signature schemes which enable any user to prove his identity and the authenticity of his messages to any other user without shared or public keys. The schemes are provably secure against any known or chosen message attack if factoring is difficult, and typical implementations require only 1% to 4% of the number of modular multiplications required by the RSA scheme. Due to their simplicity, security and speed, these schemes are ideally suited for microprocessor-based devices such as smart cards, personal computers, and remote control systems.
Total citations	Cited by 7010



Scholar articles

How to prove yourself: Practical solutions to identification and signature problems
A Fiat, A Shamir - Conference on the theory and application of ..., 1986
Cited by 7009 Related articles All 19 versions

How to Prove Yourself, Practical Solutions to Identification and Signature Problems, proc. of Crypto 86 *
A Fiat, A Shamir - Springer Verlag LNCS series
Cited by 2 Related articles

How To Prove Yourself: Practical Solutions to Identification and Signature Problems

Amos Fiat and Adi Shamir
Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot 76100, Israel

Abstract.

In this paper we describe simple identification and signature schemes which enable any user to prove his identity and the authenticity of his messages to any other user without shared or public keys. The schemes are provably secure against any known or chosen message attack if factoring is difficult, and typical implementations require only 1% to 4% of the number of modular multiplications required by the RSA scheme. Due to their simplicity, security and speed, these schemes are ideally suited for microprocessor-based devices such as smart cards, personal computers, and remote control systems.

1. Introduction

Creating unforgeable ID cards based on the emerging technology of smart cards is an important problem with numerous commercial and military applications. The problem becomes particularly challenging when the two parties (the prover A and the verifier B) are adversaries, and we want to make it impossible for B to misrepresent himself as A even after he witnesses and verifies arbitrarily many proofs of identity generated by A. Typical applications include passports (which are often inspected and photocopied by hostile governments), credit cards (whose numbers can be copied to blank cards or used over the phone), computer passwords (which are vulnerable to hackers and wire tappers) and military command and control systems (whose terminals may fall into enemy hands). We distinguish between three levels of protection:

1) Authentication schemes: A can prove to B that he is A, but someone else cannot prove to B that he is A.

2) Identification schemes: A can prove to B that he is A, but B cannot prove to someone else that he is A.

3) Signature schemes: A can prove to B that he is A, but B cannot prove even to himself that he is A.

Authentication schemes are useful only against external threats when A and B cooperate. The distinction between identification and signature schemes is subtle, and manifests itself mainly when the proof is interactive and the verifier later wants to prove its existence to a judge: In identification schemes B can create a credible transcript of an imaginary communication by carefully choosing both the questions and the answers in the dialog, while in signature schemes only real communication with A could generate a credible transcript. However, in many commercial and military applications the main problem is to detect forgeries in real time and to deny the service,

A.M. Odlyzko (Ed.): Advances in Cryptology - CRYPTO '86, LNCS 263, pp. 186-194, 1987.

Août 1986

How To Prove Yourself: Practical Solutions to Identification and Signature Problems

Conference paper | First Online: 01 January 2000

pp 186–194 | Cite this conference paper

Advances in Cryptology — CRYPTO' 86

(CRYPTO 1986)

Amos Fiat & Adi Shamir

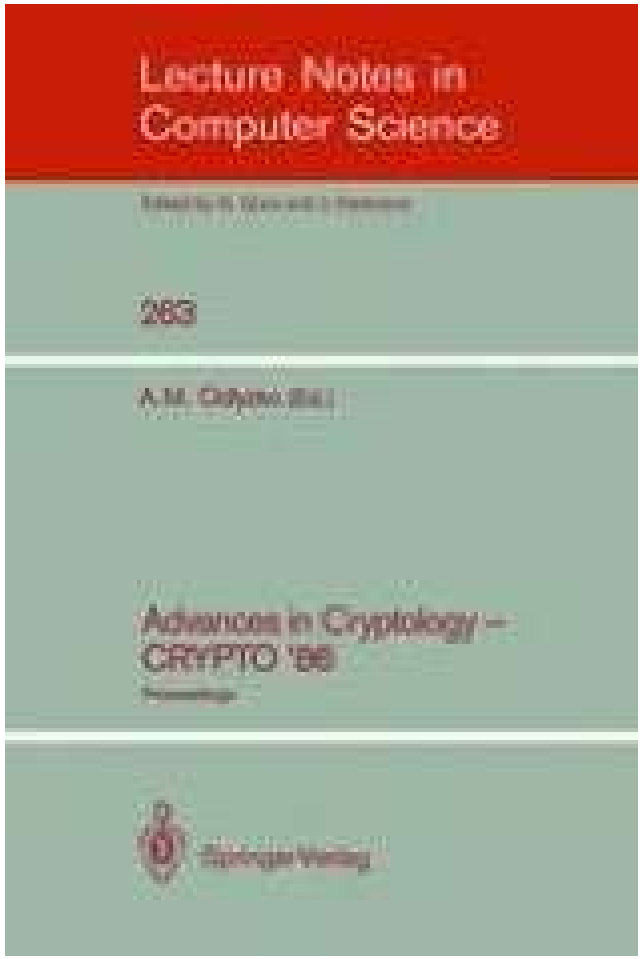
Part of the book series: Lecture Notes in Computer Science ((LNCS,volume 263))

Included in the following conference series:
Conference on the Theory and Application of Cryptographic Techniques

Abstract

In this paper we describe simple identification and signature schemes which enable any user to prove his identity and the authenticity of his messages to any other user without shared or public keys. The schemes are provably secure against any known or chosen message attack if factoring is difficult, and typical implementations require only 1% to 4% of the number of modular multiplications required by the RSA scheme. Due to their simplicity, security and speed, these schemes are ideally suited for microprocessor-based devices such as smart cards, personal computers, and remote control systems.

Quelle chance que ces proceedings existent !



Special Uses and Abuses of the Fiat-Shamir Passport Protocol (extended abstract)

Conference paper | First Online: 01 January 2000

pp 21–39 | Cite this conference paper

Advances in Cryptology — CRYPTO '87

(CRYPTO 1987)

Yvo Desmedt, Claude Goutier & Samy Bengio

Part of the book series: Lecture Notes in Computer Science ((LNCS,volume 293))

Included in the following conference series:
Conference on the Theory and Application of Cryptographic Techniques

Abstract

If the physical description of a person would be unique and adequately used and tested, *then* the security of the Fiat-Shamir scheme is *not* based on *zero-knowledge*. *Otherwise* some new frauds exist. The Feige-Fiat-Shamir scheme always suffers from these bauds. Using an extended notion of subliminal channels, several other *undetectable* abuses of the Fiat-Shamir protocol, *which are not possible with ordinary passports*, are discussed. This technique can be used by a terrorist sponsoring country to communicate 500 new words of secret information each time a tourist passport is verified. A non-trivial solution to avoid these subliminal channel problems is presented. The notion of *relative zero-knowledge* is introduced.

J. Cryptology (1991) 4: 175–183

Journal of Cryptology

Secure Implementation of Identification Systems[1]

Samy Bengio and Gilles Brassard
Département IRO, Université de Montréal,
Montréal, Québec, Canada H3C 3J7

Yvo G. Desmedt
Department of EE & CS, University of Wisconsin–Milwaukee,
Milwaukee, WI 53201, U.S.A.

Claude Goutier
Centre de calcul, Université de Montréal,
Montréal, Québec, Canada H3C 3J7

Jean-Jacques Quisquater
Département de Génie électrique (FAI), Université de Louvain
B-1348 Louvain-la-Neuve, Belgium

Abstract. In this paper we demonstrate that widely known identification systems, such as the public-file-based Feige–Fiat–Shamir scheme, can be *insecure* if proper care is not taken with their implementation. We suggest possible solutions. On the other hand, identity-based versions of the Feige–Fiat–Shamir scheme are conceptually more complicated than necessary.

Vers GQ

- Louis et moi avons eu la chance d'assister au CIRM (Marseille) au premier exposé « public » du protocole de Fiat-Shamir en **juin 1986**

(il y a eu un exposé un peu avant, à Londres, mais interne)

- Fiat et Shamir déposent un brevet en **juillet 1986**
- Validité donc contestée : dépend de la notion de public (< 30 personnes dans une audience …)

United States Patent [19]

Shamir et al.

[11] **Patent Number: 4,748,668**

[45] **Date of Patent: May 31, 1988**

[54] **METHOD, APPARATUS AND ARTICLE FOR IDENTIFICATION AND SIGNATURE**

[75] Inventors: **Adi Shamir; Amos Fiat**, both of Rehovot, Israel

[73] Assignee: **Yeda Research and Development Company Limited**, Rehovot, Israel

[21] Appl. No.: **883,247**

[22] Filed: **Jul. 9, 1986**

[51] **Int. Cl.**[4] **H04L 9/00**

[52] **U.S. Cl.** **380/30**; 380/28

[58] **Field of Search** 380/30, 28

[56] **References Cited**

PUBLICATIONS

"Use of the Signature Token to Create a Negotiable Document", by Donald W. Davies, Aug. 1983.

"Digitalized Signatures and Public-Key Functions as Intractable as Factorization", by Michael O. Rabin, Jan. 1979.

"A Fast Signature Scheme Based on Quadratic Inequalities", by Okamoto et al., IEEE, 1985.

"The Knowledge Complexity of Interactive Proof-Systems," by Shafi Goldwasser, ACM, 1985.

"Identity-Based Cryptosystems and Signature Schemes," by Adi Shamir, Dept. of Applied Mathematics, The Weizmann Institute of Science, Isreal.

Primary Examiner—Salvatore Cangialosi

Assistant Examiner—Aaron J. Lewis

Attorney, Agent, or Firm—Fleit, Jacobson, Cohn & Price

[57] **ABSTRACT**

A method and apparatus for simple identification and signature which enable any user to prove his identity and the authenticity of his messages to any other user. The method and apparatus are provably secure against any known or chosen message attack if factoring is difficult, and require only 1% to 4% of the number of modular multiplications previously required. The simplicity, security and speed of the method and apparatus derive from microprocessor-based devices which may be incorporated into smart cards, personal computers, passports, and remote control systems.

42 Claims, 2 Drawing Sheets

United States Patent [19]

Shamir et al.

[11] **Patent Number: 4,748,668**

[45] **Date of Patent: May 31, 1988**

[54] **METHOD, APPARATUS AND ARTICLE FOR IDENTIFICATION AND SIGNATURE**

[75] Inventors: **Adi Shamir; Amos Fiat**, both of Rehovot, Israel

[73] Assignee: **Yeda Research and Development Company Limited**, Rehovot, Israel

[21] Appl. No.: **883,247**

[22] Filed: **Jul. 9, 1986**

[51] **Int. Cl.**[4] **H04L 9/00**

[52] **U.S. Cl.** **380/30**; 380/28

[58] **Field of Search** 380/30, 28

[56] **References Cited**

PUBLICATIONS

"Use of the Signature Token to Create a Negotiable Document", by Donald W. Davies, Aug. 1983.

"Digitalized Signatures and Public-Key Functions as Intractable as Factorization", by Michael O. Rabin, Jan. 1979.

"A Fast Signature Scheme Based on Quadratic Inequalities", by Okamoto et al., IEEE, 1985.

"The Knowledge Complexity of Interactive Proof-Systems," by Shafi Goldwasser, ACM, 1985.

"Identity-Based Cryptosystems and Signature Schemes," by Adi Shamir, Dept. of Applied Mathematics, The Weizmann Institute of Science, Isreal.

Primary Examiner—Salvatore Cangialosi

Assistant Examiner—Aaron J. Lewis

Attorney, Agent, or Firm—Fleit, Jacobson, Cohn & Price

[57] **ABSTRACT**

A method and apparatus for simple identification and signature which enable any user to prove his identity and the authenticity of his messages to any other user. The method and apparatus are provably secure against any known or chosen message attack if factoring is difficult, and require only 1% to 4% of the number of modular multiplications previously required. The simplicity, security and speed of the method and apparatus derive from microprocessor-based devices which may be incorporated into smart cards, personal computers, passports, and remote control systems.

42 Claims, 2 Drawing Sheets

Autres chercheurs de FT (Caen)

Google Patents

AUTHENTICATION OR SIGNATURE PROCESS WITH REDUCED NUMBER OF CALCULATIONS

Abstract

Authentication and signature process with reduced number of calculations. The process involves a first entity called the "prover", which possesses a public key v and a secret key s, these keys verify the relation v=s−t (mod n), where n is an integer called modulus and t is a parameter, and a second entity called a "verifier", which knows the public key v. This process implies exchange of information following a "zero-knowledge protocol" between the verifier and the prover and cryptographic calculations on this information, some calculations being carried out "modulo n". The process of the invention is characterised by the fact that the modulus n is specific to the prover that communicates this modulus to the verifier.

Classifications

H04L9/3247 Cryptographic mechanisms or cryptographic arrangements for secret or secure communications; Network security protocols including means for verifying the identity or authority of a user of the system or for message authentication, e.g. authorization, entity authentication, data integrity or data verification, non-repudiation, key authentication or verification of credentials involving digital signatures

View 1 more classifications

Landscapes

Engineering & Computer Science

Computer Security & Cryptography

Show more

FR2788909B1
France

Find Prior Art Similar

Other languages: French

Inventor: Marc Girault, Jean Claude Pailles

Current Assignee : Orange SA

Worldwide applications

1999 • FR 2000 • EP JP US ES DE AT CA US WO

Application FR9900887A events

1999-01-27 • Priority to FR9900887A

1999-01-27 • Application filed by France Telecom SA

2000-07-28 • Publication of FR2788909A1

2004-02-20 • Application granted

2004-02-20 • Publication of FR2788909B1

2019-01-27 • Anticipated expiration

Status • Expired - Lifetime

Show all events

Info: Patent citations (12), Cited by (13), Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Patent Citations (12)

Publication number	Priority date	Publication date	Assignee	Title

Comment « prouver » qu'un nombre est aléatoire ?

- Question que Yvo Desmedt et moi nous nous posons suite à un article de Gus Simmons (1983) lié au contrôle des essais nucléaires (un nombre qui contient une information subliminale n'est pas aléatoire)

Timeworld 2021 : le hasard au CNAM

01/07/2021
15:15 – 16:00

Crespin Ludwig
Les rêves sont-ils le produit du hasard ?

01/07/2021
16:00 – 16:45

Dole Hervé
Le hasard se niche t-il en cosmologie ?

01/07/2021
16:00 – 16:45

Quisquater Jean-Jacques
Comment prouver qu'un nombre a bien été tiré au hasard ?

01/07/2021
16:00 – 17:30

CLIMAT

Dufresne J.-L., Huet S., Legras B., Le Treut H., Mélières M.-A., Mignot J., Ramstein G., Yiou P.
Le hasard gouverne-t-il le temps qu'il fait ?

01/07/2021
16:45 – 17:30

Dowek Gilles
Sommes-nous plus libres parce que le monde va au hasard ?

01/07/2021
16:45 – 17:30

Bobillier Chaumon Marc-Eric
Quelle est le rôle du hasard dans la dispersion numérique au travail ?

01/07/2021
19:30 – 20:15

LES JEUX DU PIANO ET DU HASARD

Schütz Bella

02/07/2021
09:15 – 10:00

Chevrier Raphaël
Un lancement spatial laisse-t-il la place au hasard ?

02/07/2021
09:15 – 10:00

Kupiec Jean-Jacques
Le développeme n embryon se fait-il au hasa

02/07/2021
09:15 – 10:00

Besson Nathalie
Le boson de Higgs, je suppose ?

02/07/2021
10:00 – 10:45

Paldi Andràs
L'ordre cellulaire se fonde-t-il sur le hasard moléculaire ?

02/07/2021
10:00 – 10:45

Delahaye Jean-Paul
Qu'est-ce qu'une source publique de hasard ?

Découverte d'un protocole qui prouve que l'on connait l'input d'une fonction de hash sans la donner

- But : prouver que l'on connait un nombre, sans le donner, et le résultat, l'output, s'approche d'un nombre aléatoire, mas pas totalement : basé sur l'exponentielle discrète et le RSA

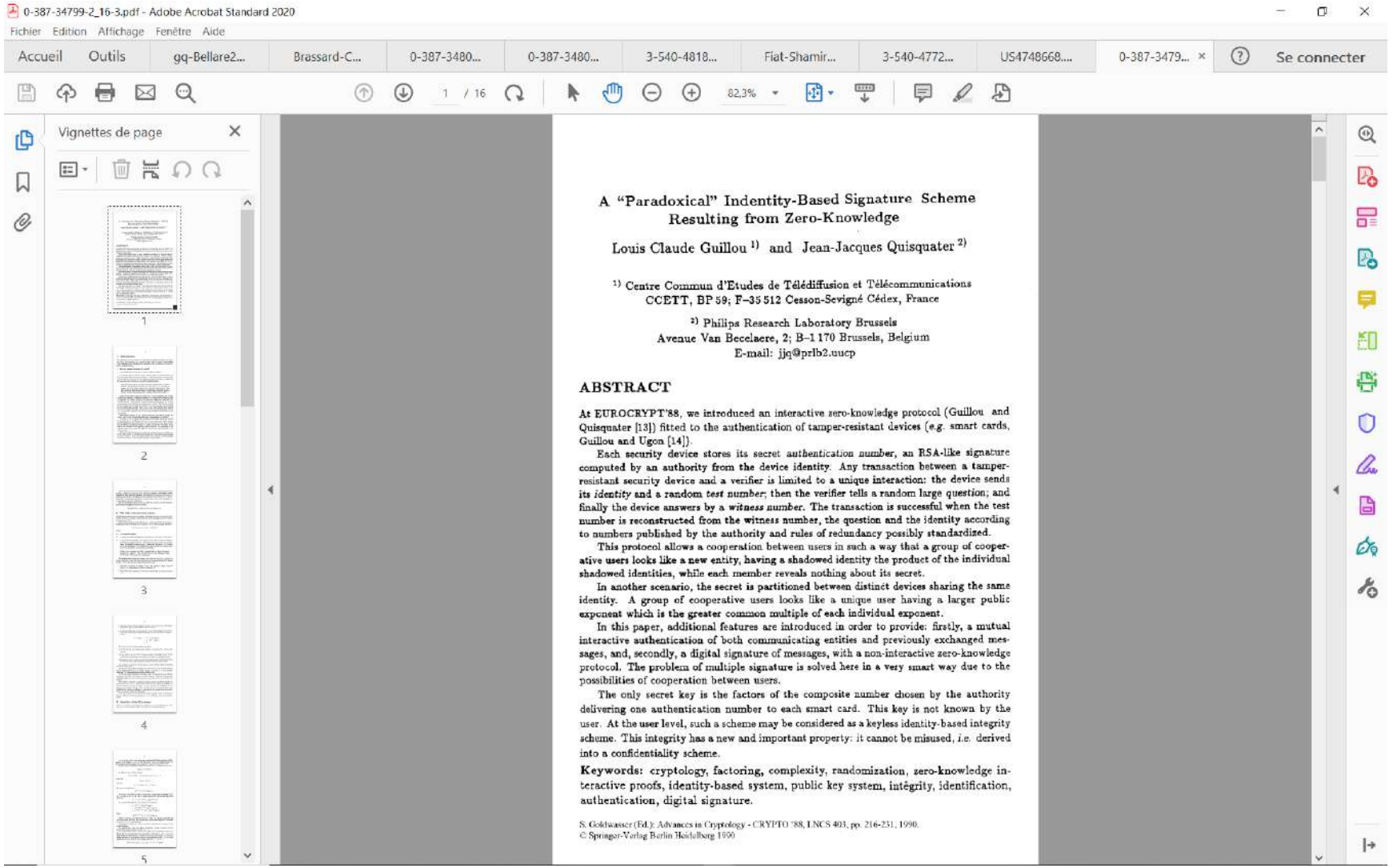
- J'explique cela à Louis : « Tu as généralisé Fiat-Shamir ! »

- On écrit vite, un brevet, un article soumis à EUROCRYPT 88 (Louis n'y sera pas) et, vu les conditions, je rédige les slides dans le train

Le premier article GQ : ping-pong

- Ayant rédigé l'article avec Louis (un résumé), je l'envoie à EUROCRYPT '88 (Davos)
- Hélas, l'envoi revient un mois après sans avoir été reçu,
- Le délai de soumission est passé,
- Après contact avec le program chair, je renvoie l'article et … il est accepté

A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge. CRYPTO 1988: 216-231 Editeur : Shafi Goldwasser



Titre

Publication mal agencée, hélas! Pas de chance.

- 2 papiers soumis à CRYPTO 88, chair person : Shafi Goldwasser
  - L'un par Louis seul suite à l'article (FOCS 84)

  A "paradoxical" solution to the signature problem

  Shafi Goldwasser, Silvio Micali, Ronald L. Rivest
  - L'autre à nous deux : l'article complet sur le protocole GQ, y compris multisignatures et identifications
- Un seul papier accepté à condition de combiner : impossible, nous ajoutons seulement le mot paradoxical dans le titre !
- Springer modifie le titre en **indentity**
- Dawn Crowel (MIT) édite mal cet article … (assemblage de 2 versions !)

Venue de Amos Fiat en moto de SFO

- Pour nous serrer la main devant Adi Shamir ☺

La suite de GQ : le brevet

- Le brevet se fait correctement
- Et très vite, RSA inc nous demande la possibilité de l'utiliser et des licences pour les USA
- Philips et France Telecom nous chargent de négocier le contrat (!)
- Nous reprenons les termes de RSA inc pour l'usage du RSA là où leur brevet est valable (en industriel, 30 $ par licence)
- RSA inc fournit une (oui 1) licence à Novell, pour test
- Grâce à Dorothy Denning, nous découvrons que Novell l'utilise pour obtenir une certification haute en sécurité … dans leur OS NDS

Report of Novell to sec.gov (à trouver)

NetWare 4.x

As a network operating system providing basic file and print services, NetWare provides security comparable to NT's. Like Unix, NetWare 4.0 and Novell Directory Service (NDS) store user passwords hashed with a salt value, which is the user's 32-bit user ID. Unlike NT and Unix, NetWare employs public key cryptography to fully authenticate the user to servers under NDS control and to maintain data integrity during login sessions. The password serves as an encryption key to protect the user's private key. A user logs in to NDS by proving to NDS that he or she knows the password through encrypted challenge-response exchange, at which point NDS securely conveys the user's private key to the user's workstation. Instead of using this permanent private key for data signatures, the workstation uses it to compute a temporary Gillou-Quisquater (GQ) key, which has two advantages. First, it's faster to use for signatures and second it's valid for only a defined period of time, thus limiting the amount of damage that rogue workstation software could do if it got possession of the key. The workstation doesn't store either the user password or the private key. Once the user logs in and his or her workstation generates a session GQ key, the workstation and the servers under NDS can mutually authenticate themselves through their public keys. They also safeguard the integrity of much of the data exchanged between them by digitally signing the first 52 bytes of each packet. Like NT, NetWare maintains Access Control Lists for the network objects (files, directories, printers, servers, etc.) under its control. Each of these Access Control Lists can grant or deny a variety of access rights either to individual users or to various groups. However, NetWare's security differs from NT's in that NDS supports multiple hierarchical levels from the tree root down through organizational units (including subsidiary organizational units) and multiple servers, each containing directories, files, printers, and other network resources. NDS allows the administrator to define security privileges at any of the levels, while NT 4.0's directory structure supports only domains at the top level and servers within each domain. (We discussed NT 5.0's more advanced distributed security earlier in this report.)

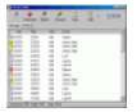
1st Security Agent

Mail Bomber

Security Administrator

PC Lockup

Access Lock



Access Administrator Pro

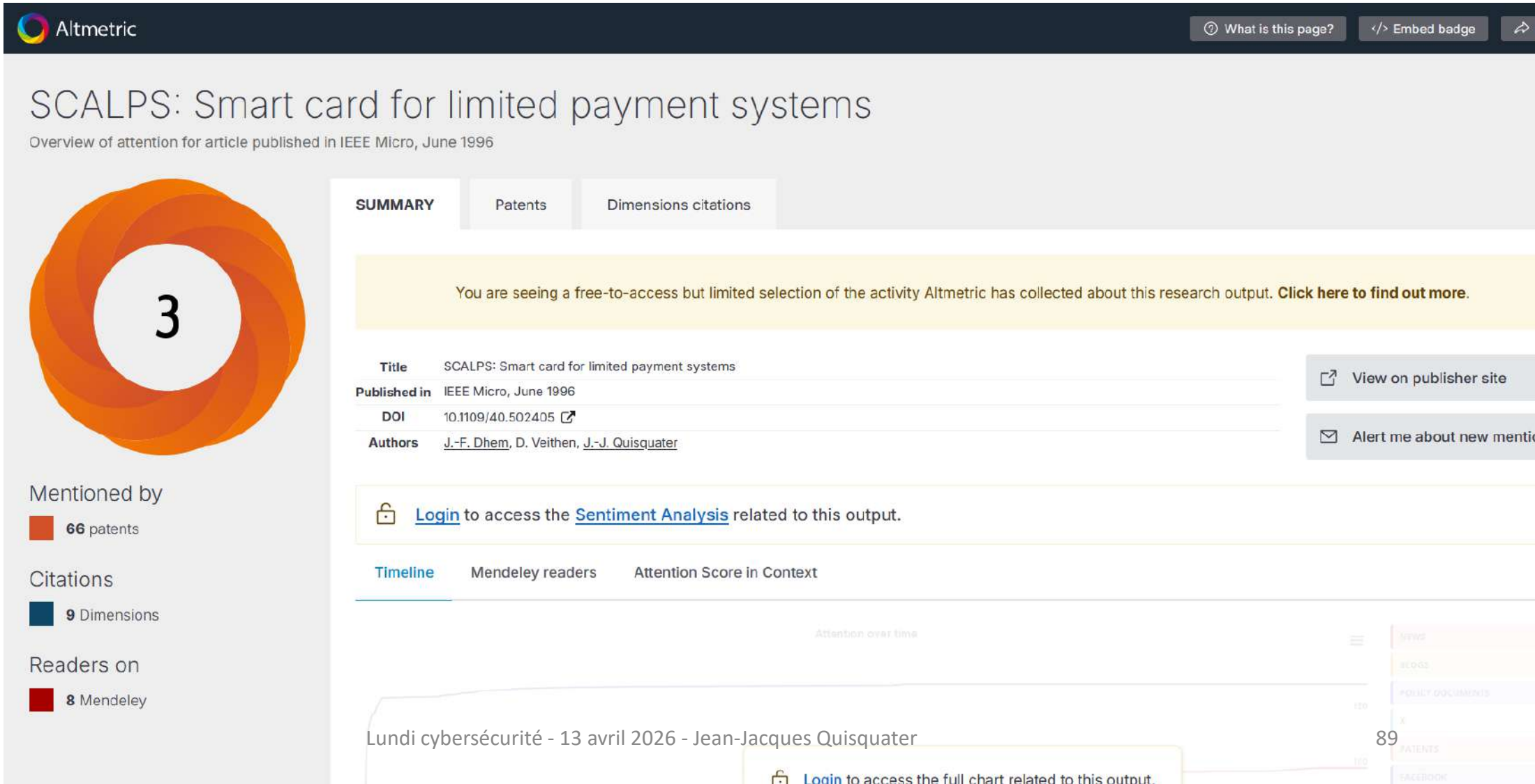
ABC Security Protector

http//www.softheap.com

Novell décline et devient opentext

- Il y a toujours des versions en cours et de la maintenance

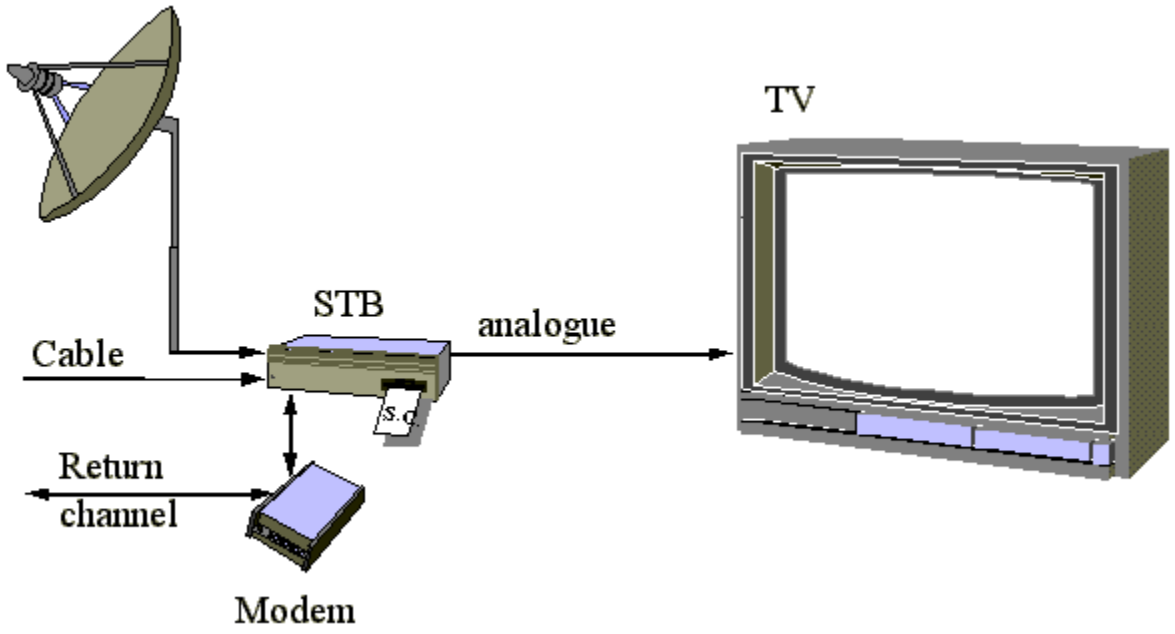
Une puce belge ZK pour cryptomonnaie (1996)



ZK est vraiment utilisé très tôt

- Voir l'usage par Novell dans le cadre de NDS

- Utilisation en TV à péage pour authentifier la carte de l'abonné vis-à-vis du décodeur (Fiat-Shamir)



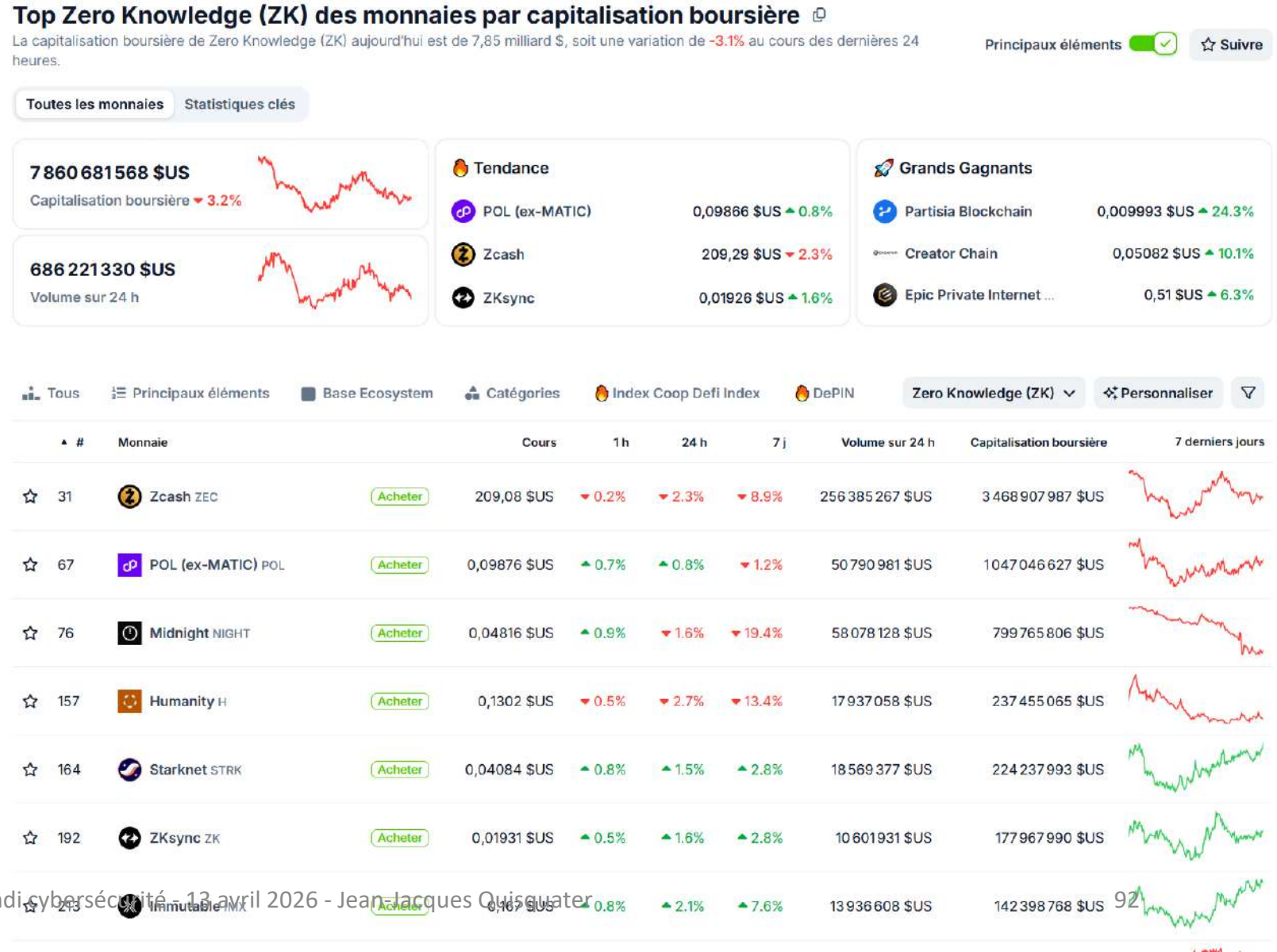
Au Japon aussi, et en Afrique du Sud

- En pur piratage

- Le brevet n’est toujours pas approuvé au Japon (!)

https://www.coingecko.com/fr/categories/zero-knowledge-zk

ZK et cryptomonnaies



Top Zero Knowledge (ZK) des monnaies par capitalisation boursière

La capitalisation boursière de Zero Knowledge (ZK) aujourd'hui est de 7,85 milliard $, soit une variation de -3.1% au cours des dernières 24 heures.

Principaux éléments | Suivre

Toutes les monnaies | Statistiques clés

7 860 681 568 $US
Capitalisation boursière ▼ 3.2%

686 221 330 $US
Volume sur 24 h

Tendance

POL (ex-MATIC)	0,09866 $US	▲ 0.8%
Zcash	209,29 $US	▼ 2.3%
ZKsync	0,01926 $US	▲ 1.6%

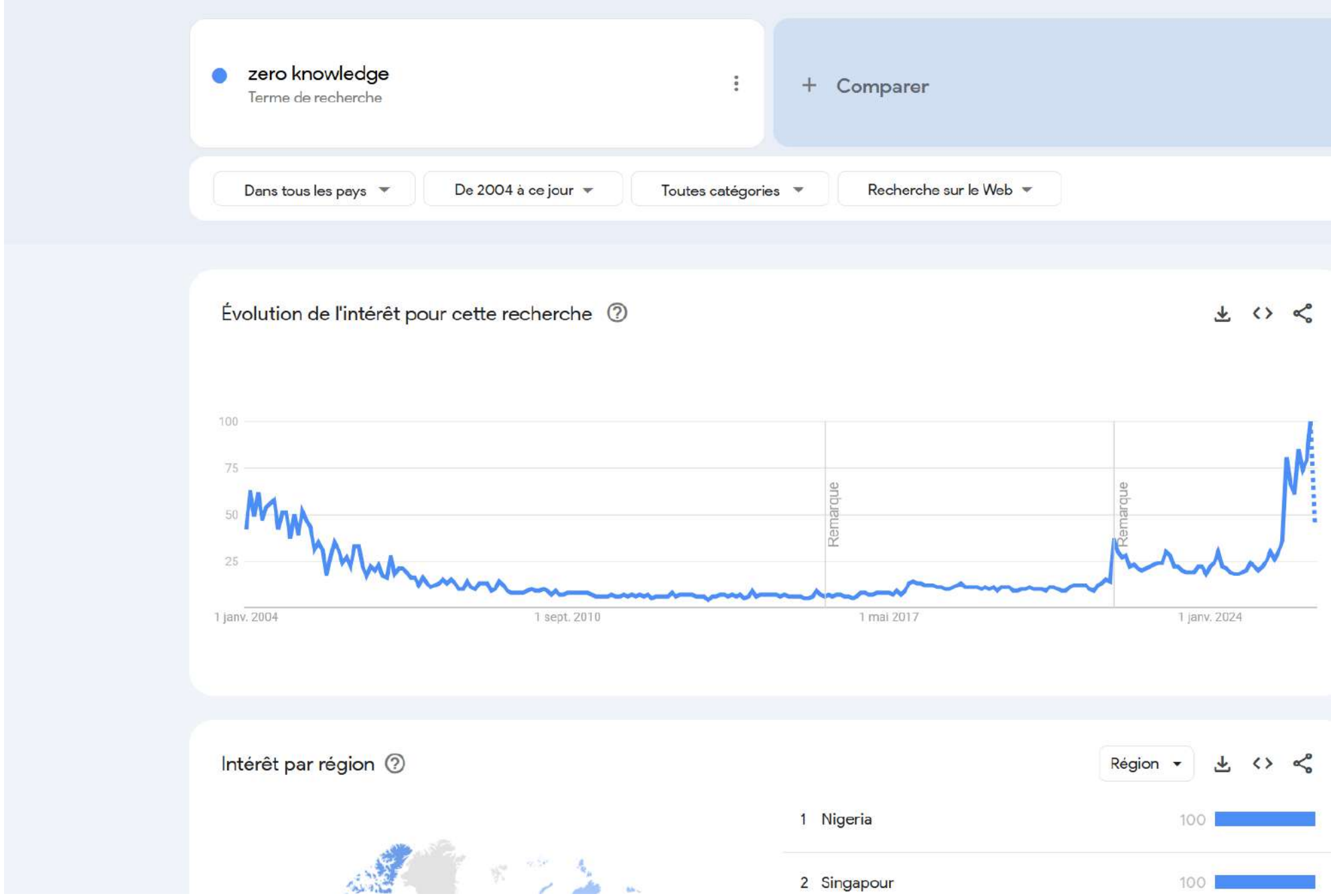
Grands Gagnants

Partisia Blockchain	0,009993 $US	▲ 24.3%
Creator Chain	0,05082 $US	▲ 10.1%
Epic Private Internet ...	0,51 $US	▲ 6.3%

Tous | Principaux éléments | Base Ecosystem | Catégories | Index Coop Defi Index | DePIN | Zero Knowledge (ZK) | Personnaliser

#	Monnaie		Cours	1 h	24 h	7 j	Volume sur 24 h	Capitalisation boursière	7 derniers jours
31	Zcash ZEC	Acheter	209,08 $US	▼ 0.2%	▼ 2.3%	▼ 8.9%	256 385 267 $US	3 468 907 987 $US	
67	POL (ex-MATIC) POL	Acheter	0,09876 $US	▲ 0.7%	▲ 0.8%	▼ 1.2%	50 790 981 $US	1 047 046 627 $US	
76	Midnight NIGHT	Acheter	0,04816 $US	▲ 0.9%	▼ 1.6%	▼ 19.4%	58 078 128 $US	799 765 806 $US	
157	Humanity H	Acheter	0,1302 $US	▼ 0.5%	▼ 2.7%	▼ 13.4%	17 937 058 $US	237 455 065 $US	
164	Starknet STRK	Acheter	0,04084 $US	▲ 0.8%	▲ 1.5%	▲ 2.8%	18 569 377 $US	224 237 993 $US	
192	ZKsync ZK	Acheter	0,01931 $US	▲ 0.5%	▲ 1.6%	▲ 2.8%	10 601 931 $US	177 967 990 $US	
213	Immutable IMX	Acheter	0,167 $US	▲ 0.8%	▲ 2.1%	▲ 7.6%	13 936 608 $US	142 398 768 $US	

Google Trends



Google Trends Accueil Explorer Tendances actuelles

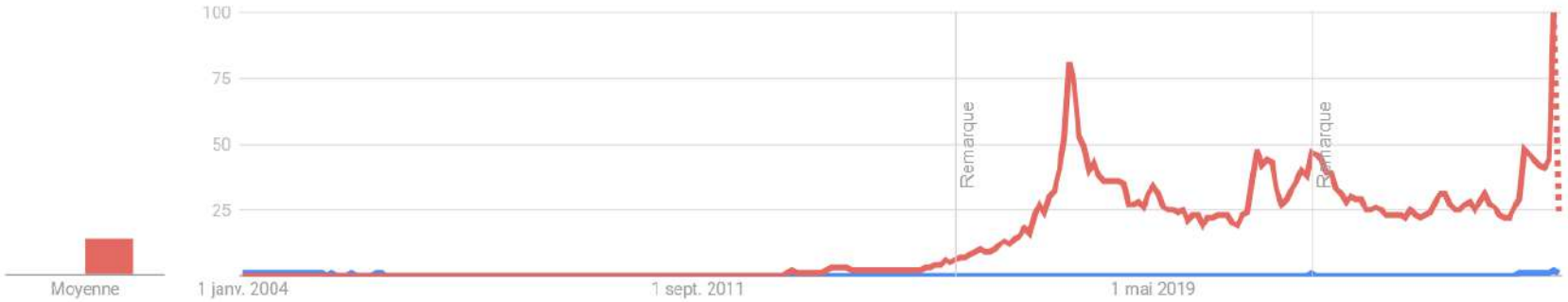
zero knowledge
Terme de recherche

blockchain
Terme de recherche

+ Ajouter une comparaison

Dans tous les pays | De 2004 à ce jour | Toutes catégories | Recherche sur le Web

Évolution de l'intérêt pour cette recherche



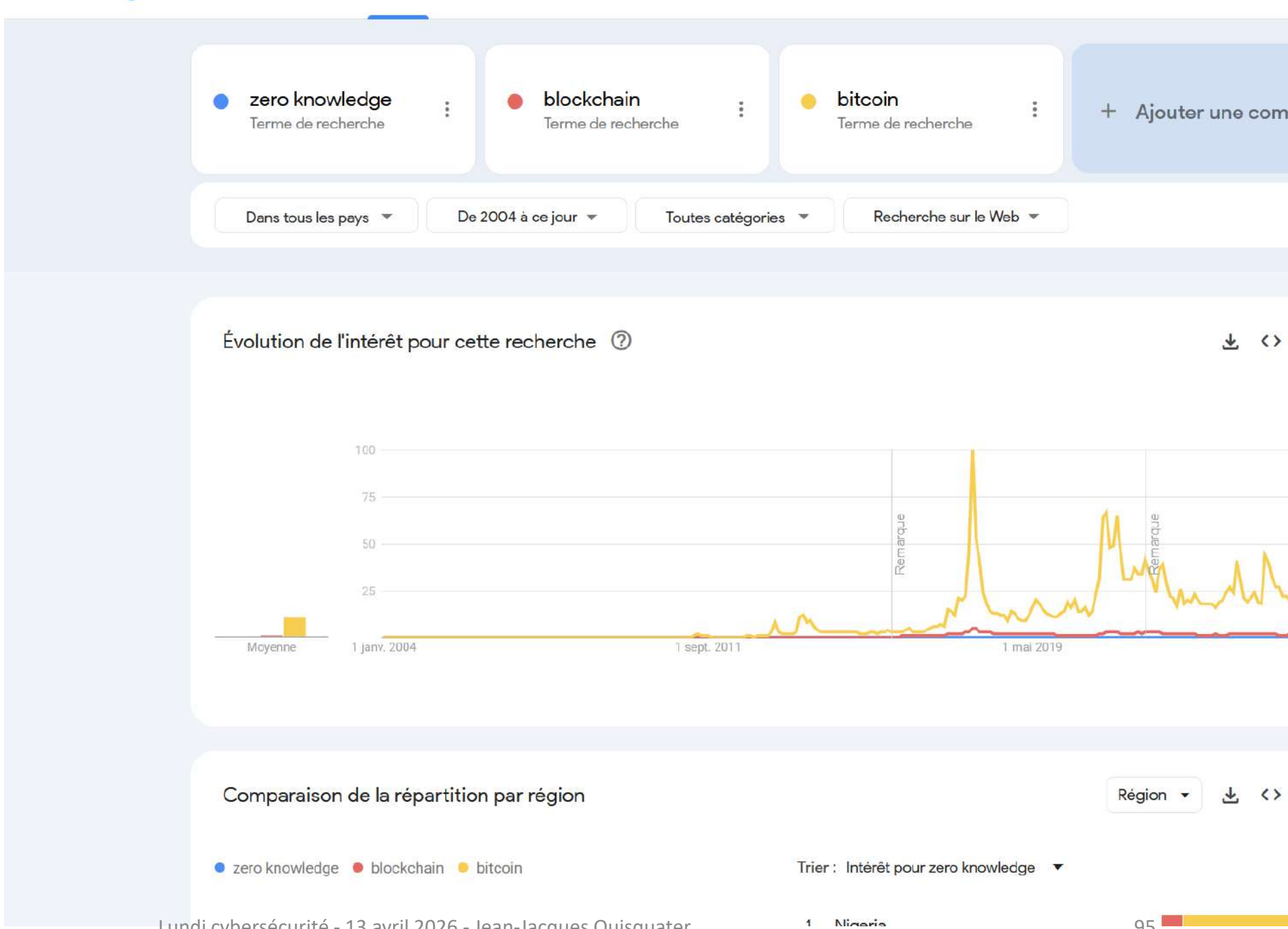
Comparaison de la répartition par région

Région

zero knowledge blockchain

Trier : Intérêt pour zero knowledge

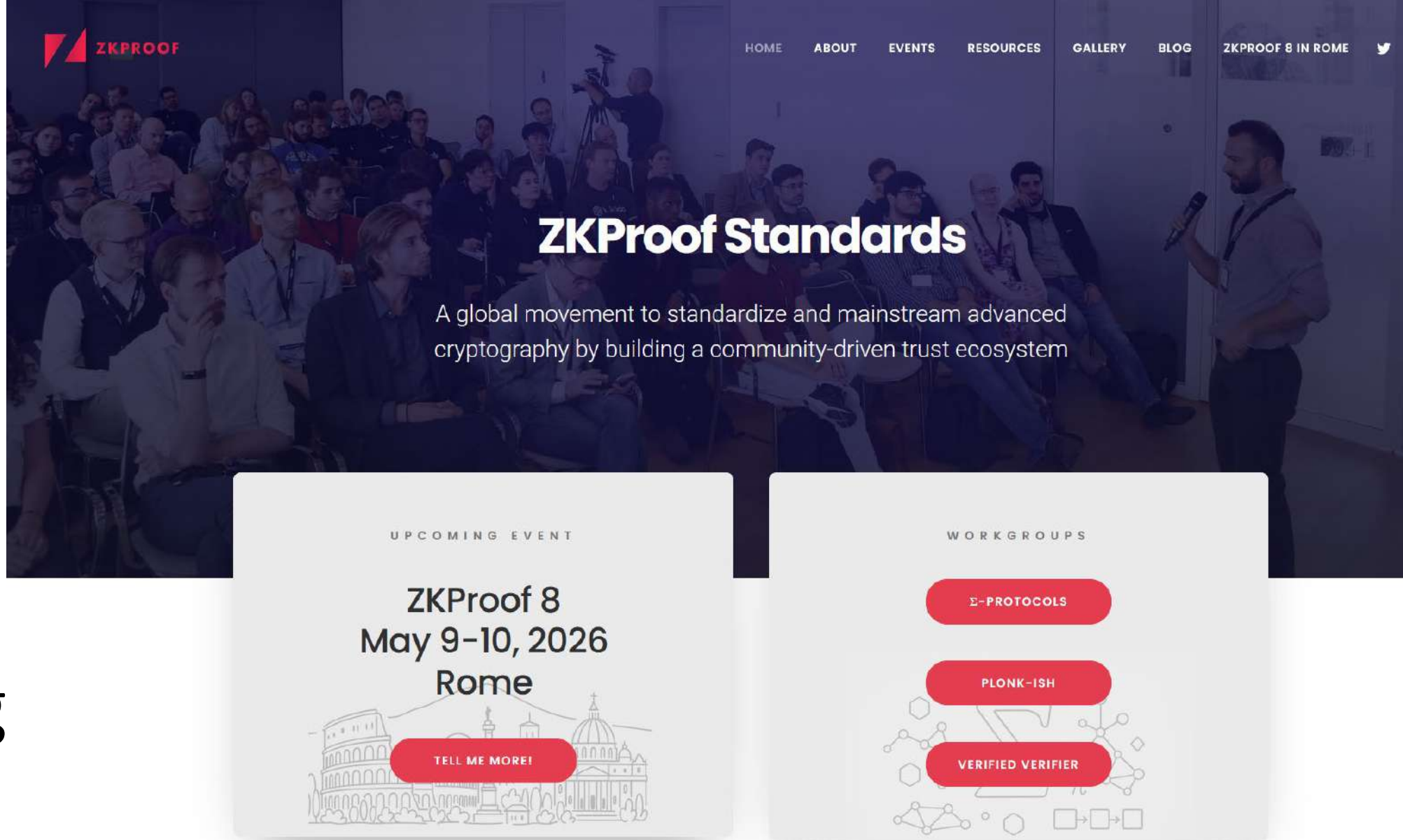
1 Israël


zero knowledge
Terme de recherche
blockchain
Terme de recherche
bitcoin
Terme de recherche
+ Ajouter une com
Dans tous les pays
De 2004 à ce jour
Toutes catégories
Recherche sur le Web
Évolution de l'intérêt pour cette recherche
100
75
50
25
Moyenne
1 janv. 2004
1 sept. 2011
1 mai 2019
Remarque
Remarque
Comparaison de la répartition par région
Région
zero knowledge
blockchain
bitcoin
Trier : Intérêt pour zero knowledge
1 Nigeria

Standards -

- ISO
- NIST
- GSMA
- IETF
- W3C
- ZKproof.org

zkproof.org


ZKPROOF
HOME
ABOUT
EVENTS
RESOURCES
GALLERY
BLOG
ZKPROOF 8 IN ROME
ZKProof Standards
A global movement to standardize and mainstream advanced cryptography by building a community-driven trust ecosystem
UPCOMING EVENT
ZKProof 8
May 9-10, 2026
Rome
TELL ME MORE!
WORKGROUPS
Σ-PROTOCOLS
PLONK-ISH
VERIFIED VERIFIER

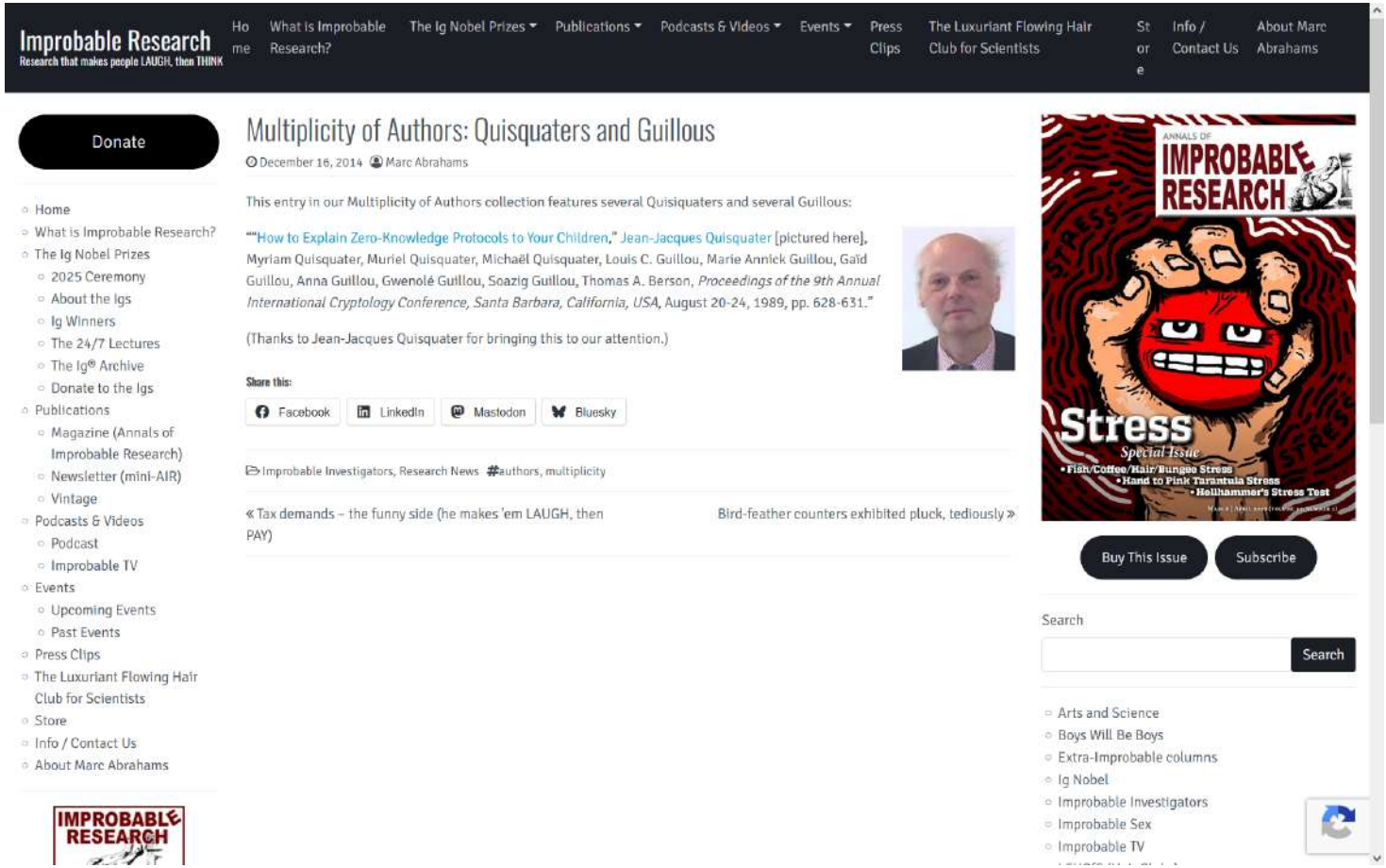
Ali-baba et la caverne

- Très tôt Philips France voudrait utiliser GQ pour leurs cartes à puce
- Reste à convaincre leurs directeurs …
- Mission : 15 minutes pour convaincre des directeurs qui ne connaissent rien à la cryptographie
- Avec Louis nous avions déjà pensé à cela en utilisant des variantes de l'isomorphisme de graphes (avec des élastiques et des clous) mais cela s'éloigne d'une idée simple, aussi avec un labyrinthe
- J'imagine alors la caverne d'Alibaba et comme testeur, j'ai d'abord Gilles Brassard

Visite chez Louis

- Je raconte cela à Louis, et, de loin, à sa famille
- Et nous décidons de présenter cela à CRYPTO 89 : trop tard, ce sera pour la rump session
- Tom Berson, aussi un écrivain pour livres d'enfants, se propose pour mettre l'histoire sous forme de conte
- Et ce fut accepter pour les proceedings (à cette époque, postérieur) avec max 4 pages
- J'ai encore le fichier LaTeX et les figures en postscript

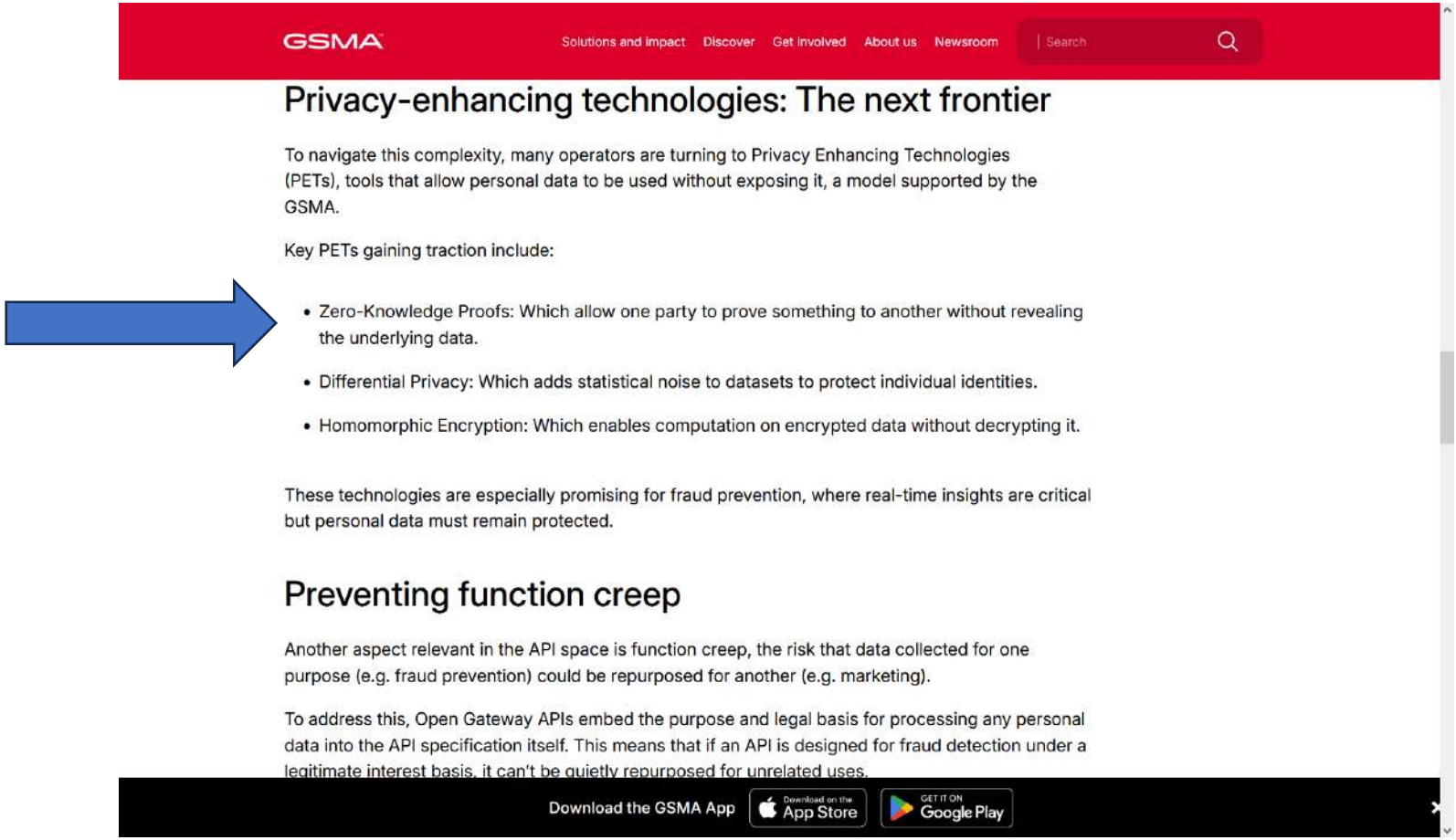

B
Bob does not know what path Alice took inside the cave, but randomly chooses a path to ask Alice to take back to the entrance. This process repeats multiple times.
B
A
Alice selected a path randomly within the cave to get to the passcode locked door


Improbable Research
Research that makes people LAUGH, then THINK
Home
What is Improbable Research?
The Ig Nobel Prizes
Publications
Podcasts & Videos
Events
Press Clips
The Luxuriant Flowing Hair Club for Scientists
Store
Info / Contact Us
About Marc Abrahams
Donate
Multiplicity of Authors: Quisquaters and Guillous
December 16, 2014 Marc Abrahams
This entry in our Multiplicity of Authors collection features several Quisquaters and several Guillous:
""How to Explain Zero-Knowledge Protocols to Your Children," Jean-Jacques Quisquater [pictured here], Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, Thomas A. Berson, Proceedings of the 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, pp. 628-631."
(Thanks to Jean-Jacques Quisquater for bringing this to our attention.)
Share this:
Facebook
LinkedIn
Mastodon
Bluesky
Improbable Investigators, Research News #authors, multiplicity
« Tax demands – the funny side (he makes 'em LAUGH, then PAY)
Bird-feather counters exhibited pluck, tediously »
ANNALS OF IMPROBABLE RESEARCH
Stress
Special Issue
• Fish/Coffee/Hair/Bungee Stress
• Hand to Pink Tarantula Stress
• Hellhammer's Stress Test
Buy This Issue
Subscribe
Search
Search
Arts and Science
Boys Will Be Boys
Extra-Improbable columns
Ig Nobel
Improbable Investigators
Improbable Sex
Improbable TV

Article CERN sur la découverte du boson

- 2100 auteurs !

GSMA : le futur des PETs



GSMA Solutions and impact Discover Get involved About us Newsroom Search

Privacy-enhancing technologies: The next frontier

To navigate this complexity, many operators are turning to Privacy Enhancing Technologies (PETs), tools that allow personal data to be used without exposing it, a model supported by the GSMA.

Key PETs gaining traction include:

- Zero-Knowledge Proofs: Which allow one party to prove something to another without revealing the underlying data.
- Differential Privacy: Which adds statistical noise to datasets to protect individual identities.
- Homomorphic Encryption: Which enables computation on encrypted data without decrypting it.

These technologies are especially promising for fraud prevention, where real-time insights are critical but personal data must remain protected.

Preventing function creep

Another aspect relevant in the API space is function creep, the risk that data collected for one purpose (e.g. fraud prevention) could be repurposed for another (e.g. marketing).

To address this, Open Gateway APIs embed the purpose and legal basis for processing any personal data into the API specification itself. This means that if an API is designed for fraud detection under a legitimate interest basis, it can't be quietly repurposed for unrelated uses.

Download the GSMA App Download on the App Store GET IT ON Google Play

Ma part dans les brevets GQ

- GQ1 : par contrat, 25 % des revenus (royalties)
  - Rien vu car pratiquement pas de revenus (cependant procès Novell)

- GQ2 : par contrat, 15 %
  - UCLouvain refuse de participer
  - Vendu comme partie d'une famille de brevets : j'ai eu ma part, dépensée pour aller à des conférences scientifiques

Propriétaire du brevet GQ2

WIKIPEDIA
25 years of the free encyclopedia

Search Wikipedia | Search

Nathan Myhrvold

10 languages

Article | Talk | Read | Edit | View history | Tools

From Wikipedia, the free encyclopedia

Contents hide

- (Top)
- Early life and education
- Career
  - Early career
  - Intellectual Ventures
  - Nuclear power
  - Science
  - Cooking
  - Advocacy
  - Affiliations and awards
- Personal life
  - Relationship with Jeffrey Epstein
- References
- Further reading
- External links

This article's lead section **may be too short to adequately summarize the key points.** Please consider expanding the lead to provide an accessible overview of all important aspects of the article. *(October 2021)*

Nathan Paul Myhrvold (born August 3, 1959) is an American inventor, scientist, and businessman, former Chief Technology Officer at Microsoft, co-founder of Intellectual Ventures and TerraPower, and the principal author of *Modernist Cuisine* and its successor books.

Early life and education [edit]

Myhrvold was born on August 3, 1959, in Seattle, Washington, to Norwegian American parents. He was raised in Santa Monica, California,[1] where he attended Mirman School[2] and Santa Monica High School, graduating in 1974,[3] and began college at age 14.[4]

Transferring from Santa Monica College, he studied mathematics (B.Sc.), and geophysics and space physics (Master's) at UCLA.[5] He was awarded a Hertz Foundation Fellowship for graduate study and studied at Princeton University, where he earned a master's degree in mathematical economics and completed a Ph.D. in applied mathematics after completing a doctoral dissertation titled "Vistas in curved space-time quantum field theory" under the supervision of Malcolm Perry.[6] For one year, he held a postdoctoral fellowship at the University of Cambridge working under Stephen Hawking.

Career [edit]

Early career [edit]

Myhrvold left Cambridge to co-found a computer startup in Oakland, California. The company, Dynamical Systems Research Inc., sought to produce Mondrian, a clone of IBM's TopView multitasking environment for DOS. Myhrvold served as Dynamical

Nathan Paul Myhrvold

Myhrvold in 2016

Born	August 3, 1959 (age 66) Seattle, Washington, US
Alma mater	University of California, Los Angeles (BS, MS) Princeton University (MS, PhD)
Spouse	Rosemarie Havranek
	Scientific career
Institutions	Intellectual Ventures, University of Cambridge, Microsoft Research
Website	nathanmyhrvold.com

Math RiZK (fondé en novembre 1991)

Cryptomonnaies et ZK

1. Blockchains de Confidentialité (Privacy Coins)

- Zcash (ZEC) : Pionnier dans l'utilisation des preuves ZK (zk-SNARKs) pour offrir des transactions anonymes et sécurisées.
- Concordium (CCD) : Une blockchain de couche 1 axée sur la confidentialité et l'identité, utilisant des preuves ZK pour la conformité.

2. Solutions de mise à l'échelle ZK-Rollups (Layer 2)

visent à alléger le réseau Ethereum en traitant les transactions hors chaîne (off-chain) tout en garantissant leur sécurité via des preuves ZK.

- zkSync (ZK) : Un ZK-Rollup compatible avec l'EVM (Ethereum Virtual Machine) qui permet des transactions rapides et peu coûteuses.
- Starknet (STRK) : Développé par StarkWare, il utilise la technologie ZK-STARKs pour la scalabilité.
- Immutable X (IMX) : Axé sur les NFT et les jeux, utilisant la technologie ZK pour des échanges sans frais de gaz.
- Linea : Un ZK-Rollup de type zkEVM qui a lancé son propre token.
- Scroll (SCR) : Un autre zkEVM majeur qui se développe fortement.
- Polygon zkEVM : Solution de mise à l'échelle de Polygon s'appuyant sur les preuves ZK.

3. Autres Écosystèmes ZK

- Orochi Network : Axé sur des solutions de preuve ZK.
- Loopring (LRC) : Un protocole d'échange décentralisé (DEX) utilisant les ZK-Rollups.

Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations

Ryan Babbush · Adam Zalcman · Craig Gidney · Michael Broughton · Tanuj Khattar · Hartmut Neven · Thiago Bergamaschi · Justin Drake · Dan Boneh · arXiv:2603.28846 (2026)

Abstract

This whitepaper seeks to elucidate implications that the capabilities of developing quantum architectures have on blockchain vulnerabilities and mitigation strategies. First, we provide new resource estimates for breaking the 256-bit Elliptic Curve Discrete Logarithm Problem, the core of modern blockchain cryptography. We demonstrate that Shor's algorithm for this problem can execute with either <1200 logical qubits and <90 million Toffoli gates or <1450 logical qubits and <70 million Toffoli gates. In the interest of responsible disclosure, we use a zero-knowledge proof to validate these results without disclosing attack vectors. On superconducting architectures with 1e-3 physical error rates and planar connectivity, those circuits can execute in minutes using fewer than half a million physical qubits. We introduce a critical distinction between fast-clock (such as superconducting and photonic) and slow-clock (such as neutral atom and ion trap) architectures. Our analysis reveals that the first fast-clock CRQCs would enable on-spend attacks on public mempool transactions of some cryptocurrencies. We survey major cryptocurrency vulnerabilities through this lens, identifying systemic risks associated with advanced features in some blockchains such as smart contracts, Proof-of-Stake consensus, and Data Availability Sampling, as well as the enduring concern of abandoned assets. We argue that technical solutions would benefit from accompanying public policy and discuss various frameworks of digital salvage to regulate the recovery or destruction of dormant assets while preventing adversarial seizure. We also discuss implications for other digital assets and tokenization as well as challenges and successful examples of the ongoing transition to Post-Quantum Cryptography (PQC). Finally, we urge all vulnerable cryptocurrency communities to join the ongoing migration to PQC without delay.

Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations

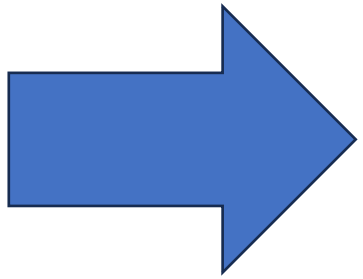
Ryan Babbush,[1,*] Adam Zalcman,[1,†] Craig Gidney,[1,‡] Michael Broughton,[1]
Tanuj Khattar,[1] Hartmut Neven,[1] Thiago Bergamaschi,[1,2] Justin Drake,[3] and Dan Boneh[4]

[1] *Google Quantum AI, Santa Barbara, CA 93111, United States*
[2] *Department of Computer Science, University of California Berkeley, Berkeley, CA 94720, United States*
[3] *Ethereum Foundation, Zeughausgasse 7a, 6300 Zug, Switzerland*
[4] *Department of Computer Science, Stanford University, Stanford, CA 94305, United States*

(Dated: April 1, 2026)

The expected emergence of cryptographically relevant quantum computers (CRQCs) will represent a singular discontinuity in the history of digital security, with wide ranging impacts. This whitepaper seeks to elucidate specific implications that the capabilities of developing quantum architectures have on blockchain vulnerabilities and potential mitigation strategies. First, we provide new resource estimates for breaking the 256-bit Elliptic Curve Discrete Logarithm Problem over the secp256k1 curve, the core of modern blockchain cryptography. We demonstrate that Shor's algorithm for this problem can execute with either $\leq$ 1200 logical qubits and $\leq$ 90 million Toffoli gates or $\leq$ 1450 logical qubits and $\leq$ 70 million Toffoli gates. In the interest of responsible disclosure, we use a zero-knowledge proof to validate these results without disclosing attack vectors. On superconducting architectures with 10^{-3} physical error rates and planar connectivity, those circuits can execute in minutes using fewer than half a million physical qubits. We introduce a critical distinction between "fast-clock" (such as superconducting and photonic) and "slow-clock" (such as neutral atom and ion trap) architectures. Our analysis reveals that the first fast-clock CRQCs would enable "on-spend" attacks on public mempool transactions of some cryptocurrencies. We survey major cryptocurrency vulnerabilities through this lens, identifying systemic risks associated with advanced features in some blockchains such as smart contracts, Proof-of-Stake consensus, and Data Availability Sampling mechanism, as well as the enduring concern of "abandoned" assets. We argue that technical solutions would benefit from accompanying public policy and discuss various frameworks of "digital salvage" to regulate the recovery or destruction of dormant assets while preventing adversarial seizure. We also discuss implications for other digital assets and tokenization as well as challenges and successful examples of the ongoing transition to Post-Quantum Cryptography (PQC). Finally, we urge all vulnerable cryptocurrency communities to join the migration to PQC without delay.

3 refs pour ZK



[32] K. Fukuda, S. Matsuo, Y. Suga, and T. Ito, The grand challenge of PQC migration: Analysis of modern blockchain and intertwined human egoisms, Cryptology ePrint Archive, Paper 2025/1626 (2025).

[33] D. B. C. Costa, *Post-Quantum Financial Infrastructure Framework (PQFIF): A Roadmap for the Quantum-Safe Transition of Global Financial Infrastructure*, Regulatory Submission (U.S. Securities and Exchange Commission (SEC), 2025) prepared for the U.S. Crypto Assets Task Force – SEC.

[34] A. Maurushat, *Disclosure of Security Vulnerabilities: Legal and Ethical Issues* (Springer London, 2013).

[35] ISO/IEC, *ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure*, Standard (International Organization for Standardization and International Electrotechnical Commission, Geneva, Switzerland, 2018).

[36] D. C. North, Institutions, Journal of Economic Perspectives **5**, 97–112 (1991).

[37] D. C. North, *Institutions, Institutional Change and Economic Performance*, Political Economy of Institutions and Decisions (Cambridge University Press, 1990).

[38] CoinMarketCap, FUD, CoinMarketCap Glossary (2021), accessed 2026-03-28.

[39] BTSE, *Crypto Trading Psychology: Dealing with FUD and FOMO in the Cryptocurrency Market*, Special Report (BTSE, 2023) BTSE Trading Psychology Series. Accessed March 28, 2026.

[40] R. Harris and A. McIntyre, *The Complete Sales Letter Book: Model Letters for Every Selling Situation*, Sharpe Professional (Sharpe Professional, 1998).

[41] S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof-systems, in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85 (Association for Computing Machinery, New York, NY, USA, 1985) pp. 291–304.

[42] J.-J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. C. Guillou, M. A. Guillou, G. Guillou, A.-C. Guillou, G. Guillou, S. Guillou, and T. A. Berson, How to explain zero-knowledge protocols to your children, in *Annual International Cryptology Conference* (1989).

[43] S. Cu'ellar Gempeler, B. Harris, J. Parker, S. Pernsteiner, I. Sweet, and E. Tromer, Cheesecloth: Zero-knowledge proofs of real-world vulnerabilities, ACM Trans. Priv. Secur. **28**, 10.1145/3747589 (2025).

[44] D. Litinski, How to compute a 256-bit elliptic curve private key with only 50 million toffoli gates, arXiv:2306.08585 (2023).

[45] C. Gidney and M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum **5**, 433 (2021).

[46] C. Gidney, How to factor 2048 bit RSA integers with less than a million noisy qubits, arXiv:2505.15917 (2025).

[47] M. Habov stiak, Hashed keys are actually fully quantum secure, Bitcoin Development Mailing List (Google Groups) (2025), mailing list thread featuring contributions from Lloyd Fournier, Agustin Cruz, Antoine Poinsot, and others. Proposes a commit-reveal scheme to protect hashed pubkeys from mempool-snatching by quantum adversaries.

[48] D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-Quantum Cryptography*, edited by D. J. Bernstein, J. Buchmann, and E. Dahmen (Springer Berlin Heidelberg, Berlin, Heidelberg, 2009) pp. 1–14.

ZK et post-quantiques …

- A discuter !