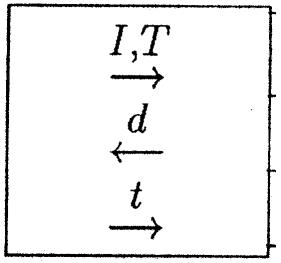
Less known facts about an identification protocol

Jean-Jacques Quisquater

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Less known facts about an identification protocol

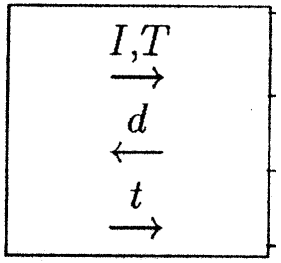


Jean-Jacques Quisquater

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Less known facts about an identification protocol

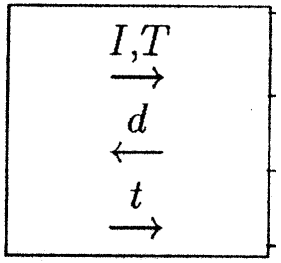


Jean-Jacques Quisquater
playing as Q

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Less known facts about an identification protocol



Jean-Jacques Quisquater

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

1984 George Orwell big brother

Identity-based public-key cryptosystem: in order to have few public keys

Adi Shamir: Identity-Based Cryptosystems and Signature Schemes. CRYPTO 1984: 47-53

Identity-based secret-key cryptosystem: *Louis Guillou*, for French smart cards in order to avoid problems with French law for using cryptography in civilian uses

Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: **A "Paradoxical" Solution to the Signature Problem (Abstract). CRYPTO 1984**, 467

1986 Fiat-Shamir protocol …

« not enough efficient for smart cards »

And beginning of my research about pseudo random generators with minimal subliminal channel (question by Gus Simmons and work with Yvo Desmedt)

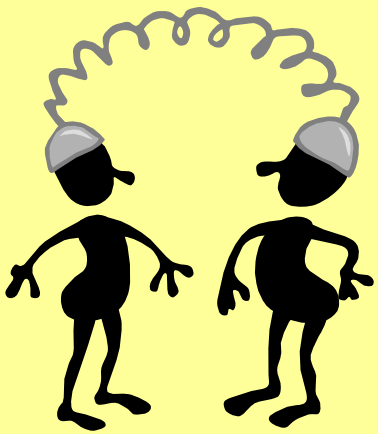
Basic idea: generate a random number, use it as input of an one-way function and give the output, then prove you know the input without giving it

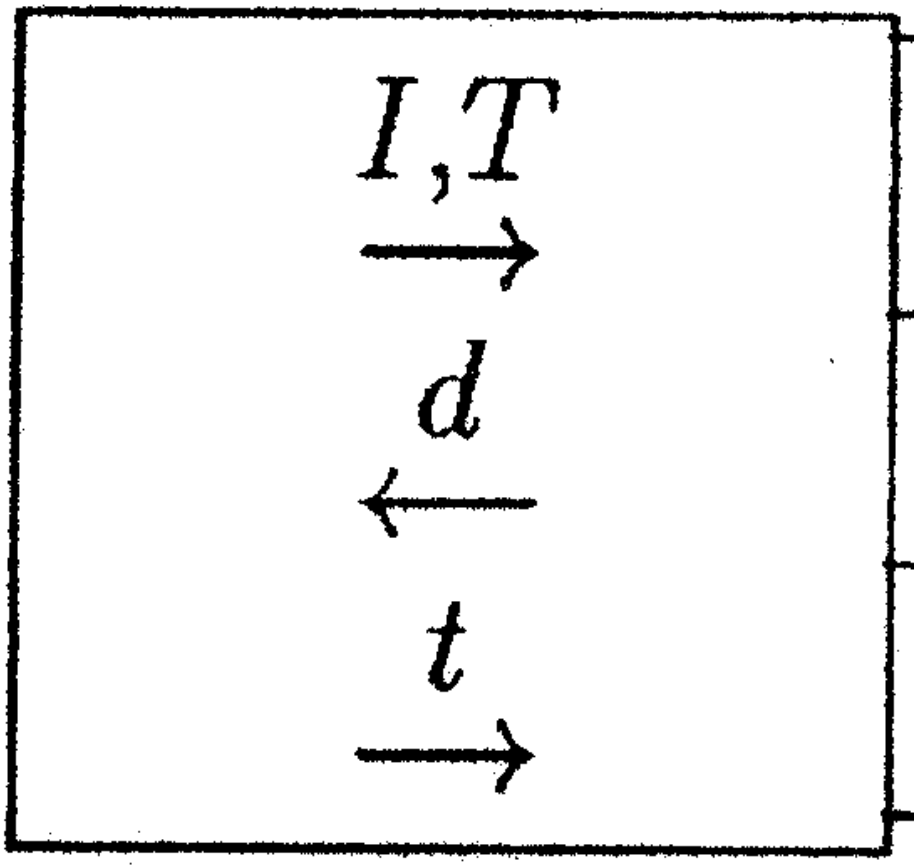
1987

I described that one day to Louis Guillou and he said « That's the right generalization of Fiat-Shamir ». Surprise

We wrote a memo for a patent …

I wanted to go at CRYPTO '87: some lawyers wanted to avoid because I had the new protocol in my head before the filling of a patent …
I was at CRYPTO '87.





September 7, 1987: war arms of second category (missil, cryptography, …)

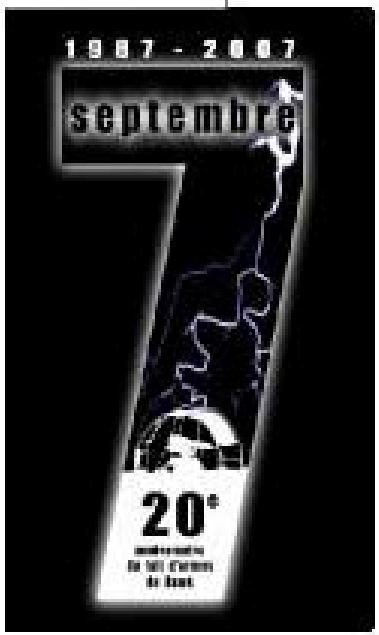
See septembre7.fr
The only time the French army really uses such arms (in Tchad)

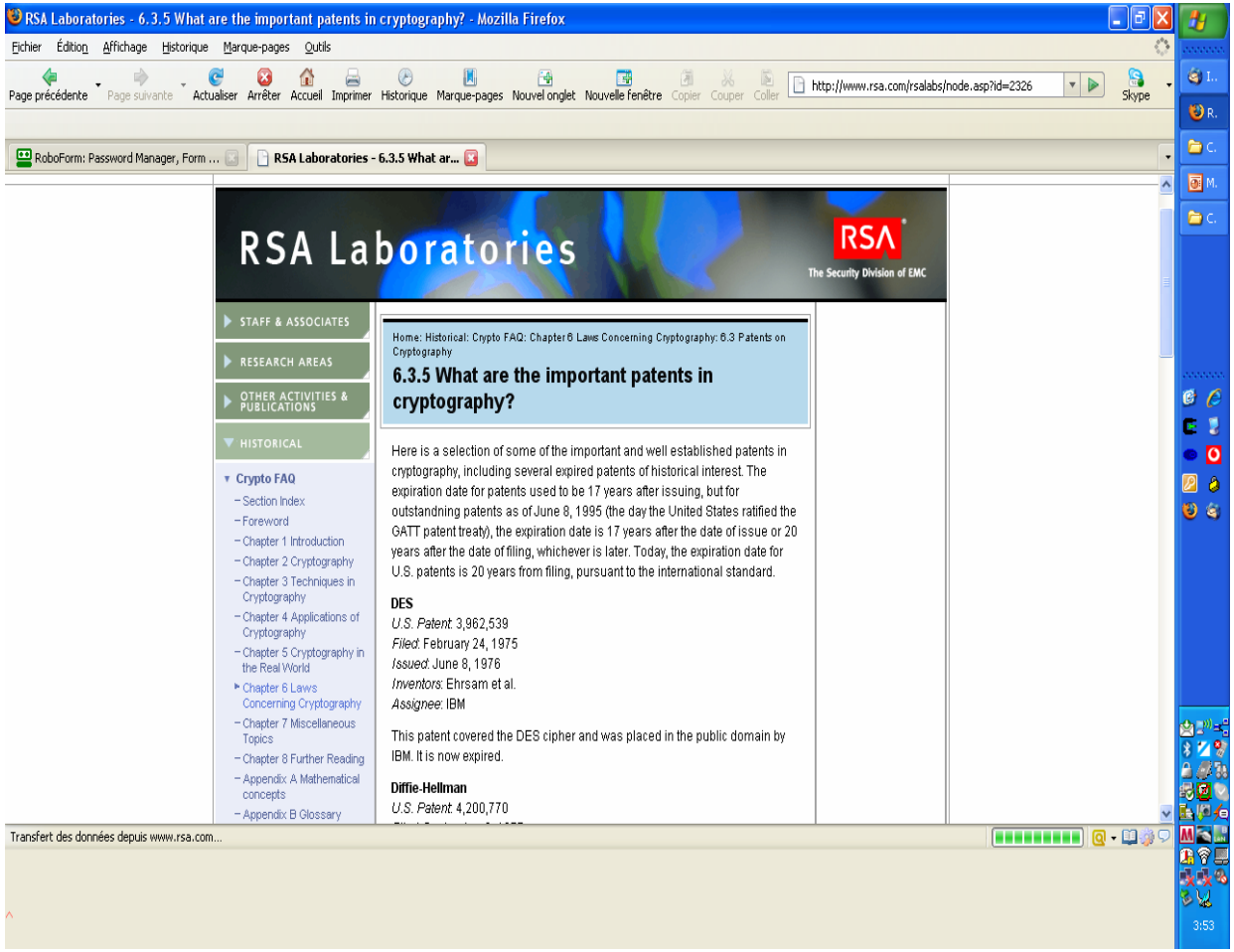
Filing of a French patent

We received very soon a letter with the order of not speaking about that application

Thanks: we obtain the permission to patent it publicly in few months.

Ads by onetimepadsense





Ads by onetimepadsense

papers

EUROCRYPT 1988:

we obtain the permission to publish very late. Then, I sent our paper on time for submission. One month later the letter coming back not distributed … Too late. I sent it again with an explanation and …

CRYPTO 1988:

Curious title: in fact, 2 papers accepted, one about the identification protocol and another one, only by Louis Guillou, about paradoxical signatures. The chair asked to combine, an impossible task. More: the published paper is not the submitted paper, nor the final paper, but a mixing of both … And another surprise:

CRYPTO '88

A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge

Louis Claude Guillou [1] and Jean-Jacques Quisquater [2]

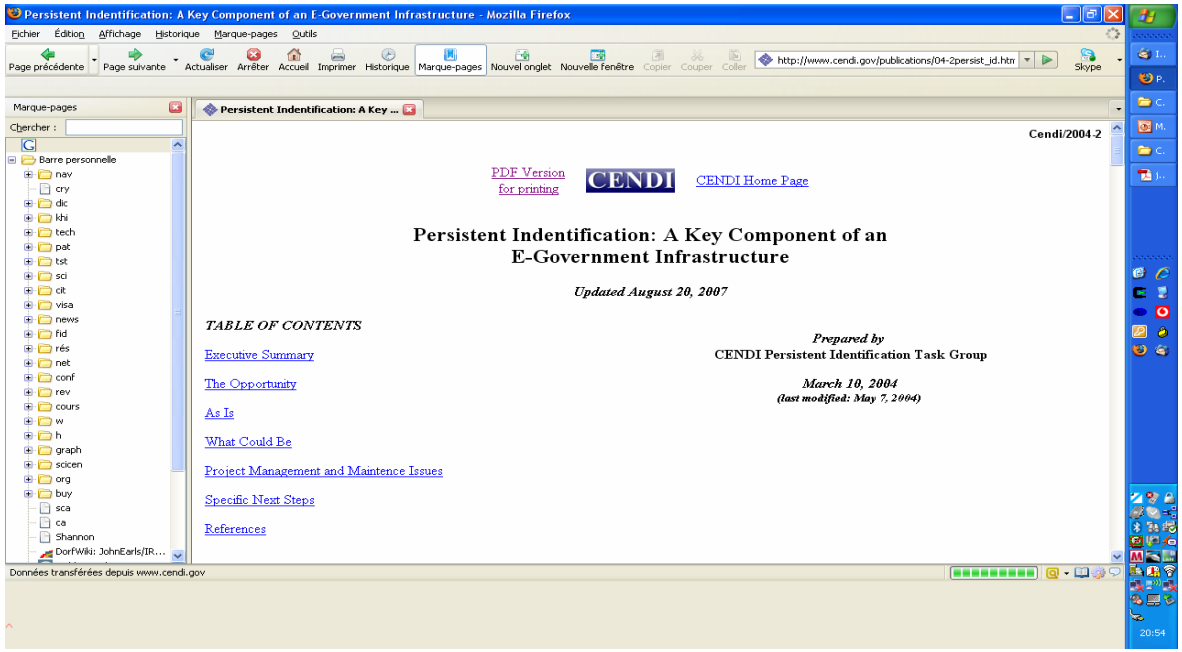
[1] Centre Commun d'Etudes de Télédiffusion et Télécommunications
CCETT, BP 59; F–35 512 Cesson-Sevigné Cédex, France

[2] Philips Research Laboratory Brussels
Avenue Van Becelaere, 2; B–1 170 Brussels, Belgium
E-mail: jjq@prlb2.uucp

ABSTRACT

At EUROCRYPT'88, we introduced an interactive zero-knowledge protocol (Guillou and Quisquater [13]) fitted to the authentication of tamper-resistant devices (*e.g.* smart cards, Guillou and Ugon [14]).

Another recent indentity



Ads by onetimepadsense

Used?

Contract with RSA, inc

Novell uses the protocol for NDS and Netware (100 million clients and about 4 millions of servers) in identification process

Serge Vaudenay and al. just proposed to use it for current electronic passports (RFIDsec 2007)

How much did you receive for this patent?

How much did you receive for this patent?

From the patent writing office:

Ads by onetimepadsense

Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« *The Onion* on Terr

June 25, 2007

Cocktail Condoms

They're protective covers that go over your drink a Mickey Finn (or whatever they're called these d

> The concept behind the cocktail cover is fai it can be used to cap a drink that goes una beverage, there is a layer that can be pulle protecting the cocktail. That can be punctu either way the drinker will know that the c

I'm sure there are many ways to defeat this secu affixing a new cover after you tamper with the dr rare risk we're likely to overreact to. But to me, th

Expiration: September 7, 2007

Enjoy the desserts I sponsor during this rump session (thanks also to Markus Jacobsson, Alfred Menezes and Dan Bernstein)

Then use the so-called GQ protocol (identification and signature) only for your pleasure and mine.

THANKS