

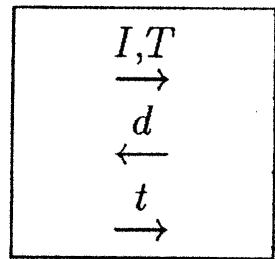
Less known facts about an identification protocol

Jean-Jacques Quisquater

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Less known facts about an indentification protocol

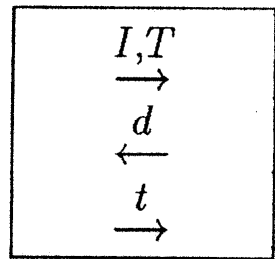


Jean-Jacques Quisquater

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Less known facts about an indentification protocol



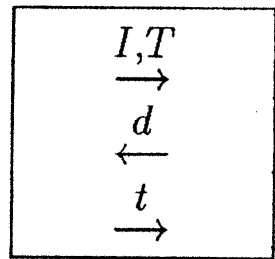
Jean-Jacques Quisquater
playing as Q

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Ads by
onetimepadsense

Less known facts about an identification protocol

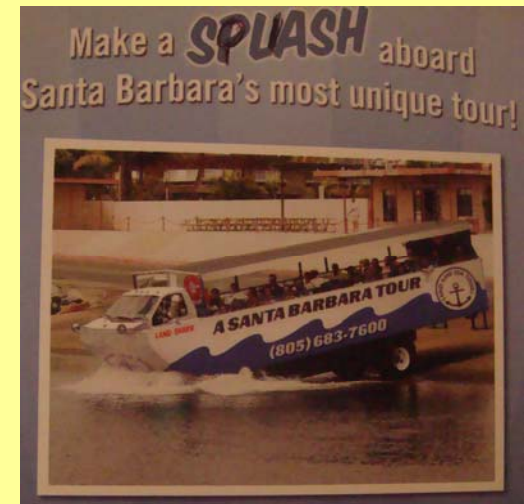


Jean-Jacques Quisquater

1987: jjq@prlb2.uucp

2007: jean-jacques.quisquater@UCLouvain.be

Ads by
onetimepadsense



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

Ads by
onetimepadsense

Bruce Schneier

Schneier on Security

A blog covering security and security technology.

[« The Most Secure Car Pa](#)

May 11, 2007

Is Big Brother a Big Deal?

Big Brother isn't what he used to be. George Orwell's 1940s. Today's information society looks nothing like Orwell's. Intimidating a population today isn't anything like

Data collection in 1984 was deliberate; today's is incidental. People generate data naturally. In Orwell's world, people leave digital footprints everywhere.

1984's police state was centralized; today's is decentralized. When you talk to your credit card company, they know who you are. When you watch TV, your ISP can read your email, your cell phone company can monitor your purchasing patterns. Bringing this together, but there doesn't have to be a single Big Brother, but instead thousands of Little Brothers.

1984's Big Brother was run by the state; today's is run by the market.

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

Ads by
onetimepadsense

Yvo Desmedt Dancing at 2007 RSA Conference



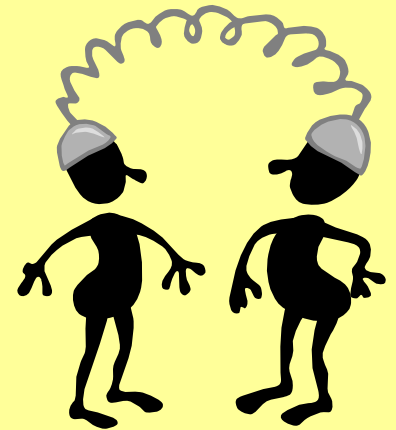
1987

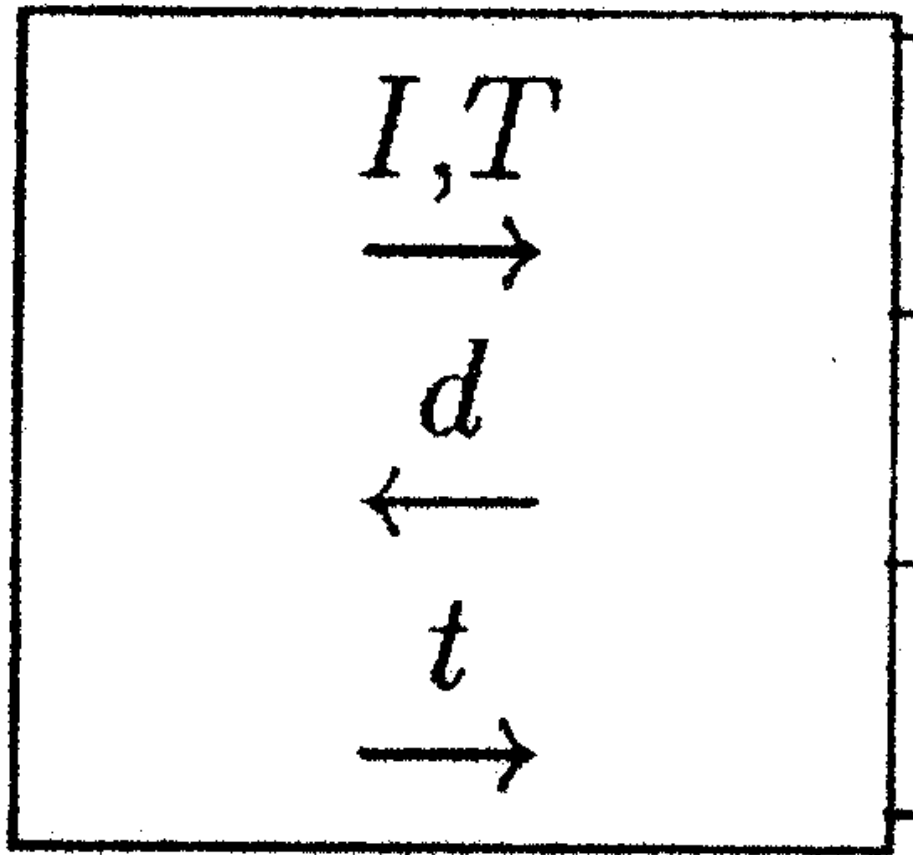
I described that one day to Louis Guillou and he said « That's the right generalization of Fiat-Shamir ». Surprise

We wrote a memo for a patent ...

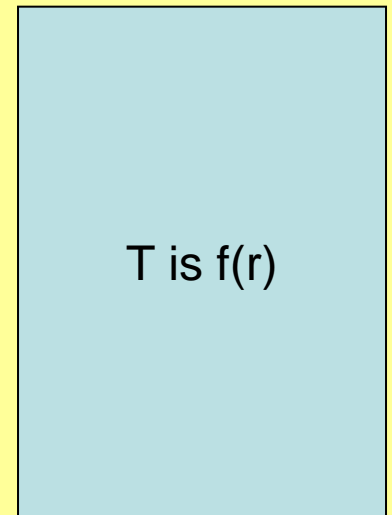
I wanted to go at CRYPTO '87: some lawyers wanted to avoid because I had the new protocol in my head before the filling of a patent ...
I was at CRYPTO '87.

Ads by
onetimepadsense





Ads by
onetimesense



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



RSA Laboratories - 6.3.5 What are the important patents in cryptography? - Mozilla Firefox

Page précédente Page suivante Actualiser Arrêter Accueil Imprimer Historique Marque-pages Nouvel onglet Nouvelle fenêtre Copier Couper Coller http://www.rsa.com/rsalabs/node.asp?id=2326 Skype

RoboForm: Password Manager, Form ... RSA Laboratories - 6.3.5 What ar...

RSA Laboratories

The Security Division of EMC

- STAFF & ASSOCIATES
- RESEARCH AREAS
- OTHER ACTIVITIES & PUBLICATIONS
- HISTORICAL
 - Crypto FAQ
 - Section Index
 - Foreword
 - Chapter 1 Introduction
 - Chapter 2 Cryptography
 - Chapter 3 Techniques in Cryptography
 - Chapter 4 Applications of Cryptography
 - Chapter 5 Cryptography in the Real World
 - Chapter 6 Laws Concerning Cryptography
 - Chapter 7 Miscellaneous Topics
 - Chapter 8 Further Reading
 - Appendix A Mathematical concepts
 - Appendix B Glossary

6.3.5 What are the important patents in cryptography?

Home: Historical: Crypto FAQ: Chapter 6 Laws Concerning Cryptography: 6.3 Patents on 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 outstanding 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

Transfert des données depuis www.rsa.com...

3:53

Ads by
onetimepadsense

papers

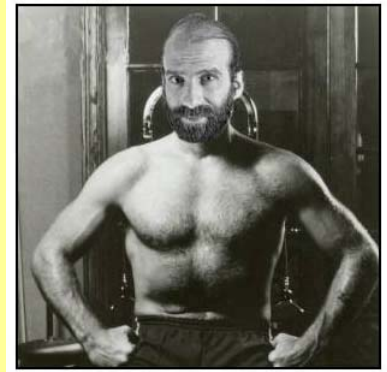
EUROCRYPT 1988:

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:

Ads by
onetimepadsense



Contrary to the popular belief,
Ali Baba didn't say "Open, Sesame"
to open his magic cave.
He only had to say "Bruce Schneier".

CRYPTO '88

A “Paradoxical” Identity-Based Signature Scheme Resulting from Zero-Knowledge

Louis Claude Guillou ¹⁾ and Jean-Jacques Quisquater ²⁾

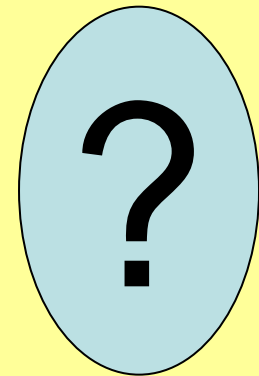
¹⁾ Centre Commun d'Etudes de Télédiffusion et Télécommunications
CCETT, BP 59; F-35 512 Cesson-Seigné Cédex, France

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

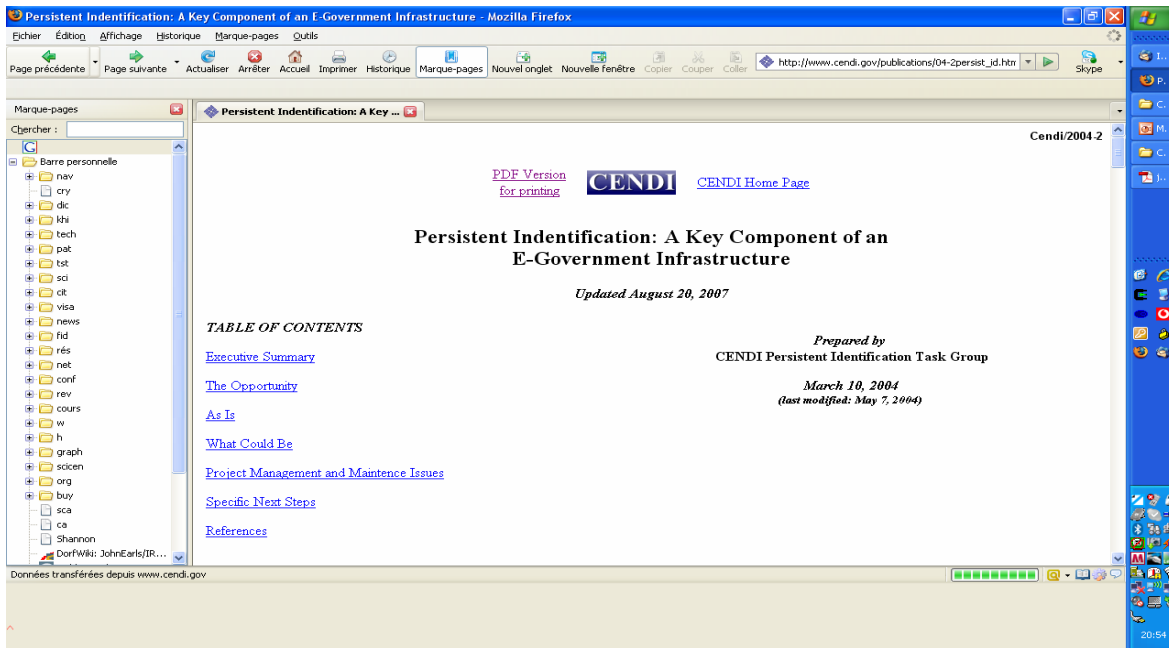
ABSTRACT

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]).

Ads by
onetimepadsense



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)

Ads by
onetimepadsense

How much did you receive for this patent?

Ads by
onetimepadsense

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 pulled protecting the cocktail. That can be punctur 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



Ads by
onetimepadsense

