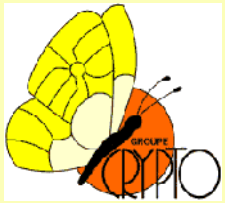
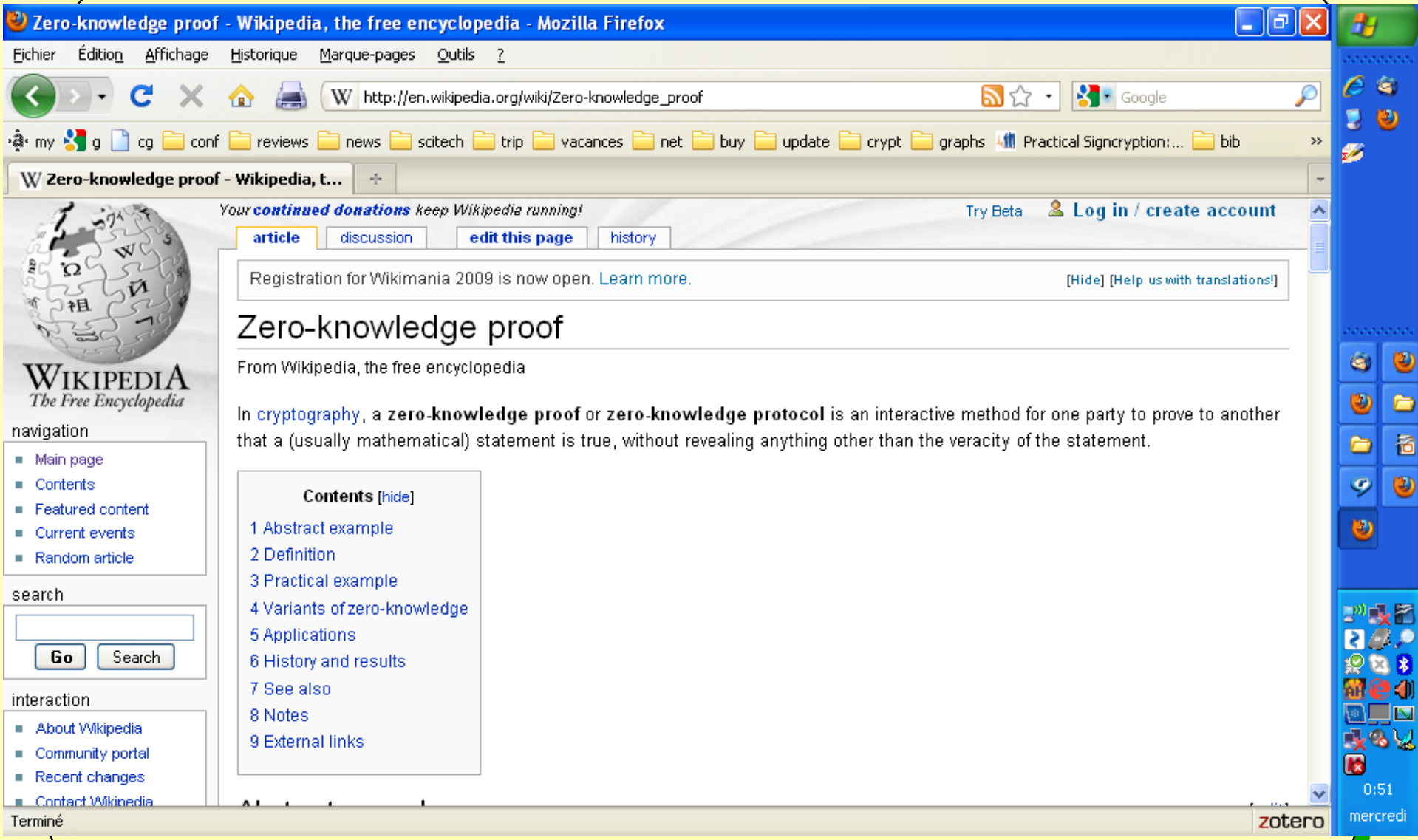
How to explain algorithms and cryptography to your (old) children II

Erik Demaine (MIT)
Martin Demaine (MIT)
Jean-Jacques Quisquater (UCLouvain)
Michaël Quisquater (UVSQ)



20 years ago : CRYPTO 1989

- **Rump session and proceedings**
- **Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou Thomas A. Berson**
- **How to Explain Zero-Knowledge Protocols to Your Children.**
  - **CRYPTO 1989: LNCS 435, pp. 628-631**
  - **Thanks to Gilles Brassard**
  - **55 refs in Google scholar**
  - **Translated in 12 languages (at least)**
  - **Really in use for teaching**



Rump session CRYPTO 2009

Zero-knowledge proof - Wikipedia, the free encyclopedia - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

http://en.wikipedia.org/wiki/Zero-knowledge_proof

Zero-knowledge proof - Wikipedia, t...

- Contact Wikipedia
- Donate to Wikipedia
- Help

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Cite this page

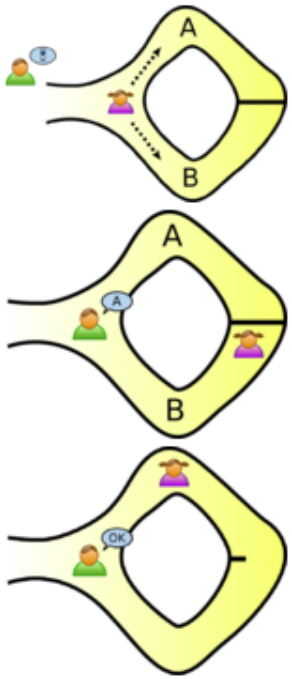
languages

- Dansk
- Deutsch
- Français
- עברית
- Italiano
- Polski
- Русский

Abstract example

[edit]

There is a well-known story presenting some of the ideas of zero-knowledge proofs, first published by Jean-Jacques Quisquater and others in their paper "How to Explain Zero-Knowledge Protocols to Your Children".[1] It is common practice to label the two parties in a zero-knowledge proof as Peggy (the prover of the statement) and Victor (the verifier of the statement).



In this story, Peggy has uncovered the secret word used to open a magic door in a cave. The cave is shaped like a circle, with the entrance on one side and the magic door blocking the opposite side. Victor says he'll pay her for the secret, but not until he's sure that she really knows it. Peggy says she'll tell him the secret, but not until she receives the money. They devise a scheme by which Peggy can prove that she knows the word without telling it to Victor.

First, Victor waits outside the cave as Peggy goes in. We label the left and right paths from the entrance A and B. She randomly takes either path A or B. Then, Victor enters the cave and shouts the name of the path he wants her to use to return, either A or B, chosen at random. Providing she really does know the magic word, this is easy: she opens the door, if necessary, and returns along the desired path. Note that Victor does not know which path she has gone down.

However, suppose she did not know the word. Then, she would only be able to return by the named path if Victor were to give the name of the same path that she had entered by. Since Victor would choose A or B at random, he would have a 50% chance of guessing correctly. If they were to repeat this trick many times, say 20 times in a row, her chance of successfully anticipating all of Victor's requests would become vanishingly small.

Terminé

zotero

0:52
mercredi

The project

- Today on the web there are a lot of videos, including many ones by people from cryptography
- Many are funny

Whit Diffie in one of the first webcast (1993)

http://www.youtube.com/watch?v=mZRIh2zYb-M

Ron Rivest recitating a poem

http://www.youtube.com/watch?v=BzEx2uMCGwM

Adi Shamir about privacy in the city hall of Leuven

http://www.youtube.com/watch?v=JrVueibAQyI

Len Adleman boxing

http://www.youtube.com/watch?v=N64ltOBBg2w

Yvo Desmedt dancing (at ULU)

http://www.youtube.com/watch?v=PRzIxSQRXTc

But is it enough?

- We are an young community
- We are enough lucky to meet the inventors, the authors ...
- It is time to share for the next generations
- So ...

HiDalgocrypt project

- Having in HD videos the main (cryptographic) algorithms explained by their authors or by the best teachers in the best possible context (no slides ?)
- So Erik, Martin, Michaël or me will contact you to visit you
- OR send us your proposals