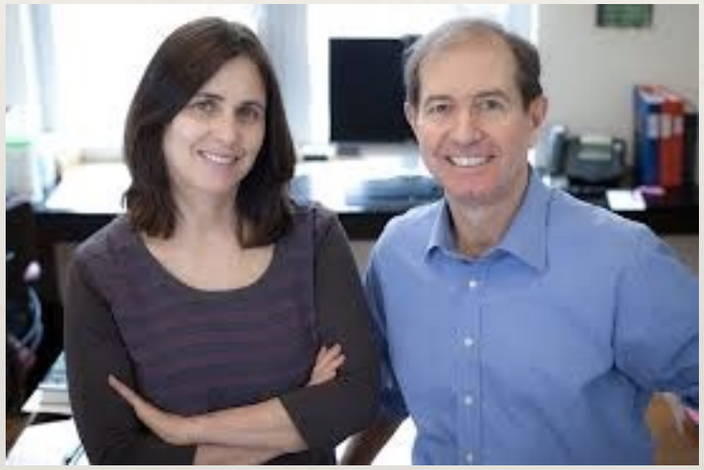
Zero Knowledge

- Invented by Goldwasser, Micali and Rackoff in 1982 (publication in 1985).



- How to prove you know a secret without disclosing it, nor any information about it.

Toy Zero Knowledge

- Vous voulez prouver à une personne daltonienne que vous n'êtes pas daltonien.
- Il y a deux billes identiques sauf leur couleur : une verte et une rouge. Vous voulez montrer que vous savez les différencier mais sans révéler laquelle est la verte.

Solution

- Le daltonien choisit une bille au hasard et vous la montre, puis la cache.
- Ensuite, il tire à pile ou face :
  - Si c'est pile, il vous remontre la même bille.
  - Sinon, il vous montre l'autre bille.
- Il vous demande si vous avez vu la même bille.
  - Il peut déterminer si votre réponse est correcte ou non.
  - Si vous ne savez pas distinguer les billes, vous avez exactement une chance sur deux de répondre correctement.

Zero Knowledge of Discrete Log [Schnorr1989]

- Let G be a cyclic group by some g of prime order q.
  - g and q are public.
- $y=g^x$ where $x \in \{0,\ldots,q-1\}$.
- The prover wants to show that he knows x without disclosing anything else.

Protocole

Prouveur

Vérifieur

Choisit $r \in \{0,\ldots,q-1\}$ au hasard

$R = g^r$

Choisit $c \in \{1,\ldots,q-1\}$ au hasard

c

$a = r - cx \bmod q$

Vérifie que $R = g^a y^c$

Remarques

- Extraction : Si un observateur voit deux exécutions (R,c,a) et (R,c’,a’) utilisant le même r, alors il peut retrouver le secret x.
- Zero Knowledge : Quelqu’un qui ne connaît pas le secret x peut générer des triplets (R,c,a) corrects et qui ont la même distribution que les vrais (R,c,a) !

Signatures

- On peut transformer heuristiquement toute identification zero-knowledge en une signature : comment ?
- C'est la transformation de Fiat-Shamir.
- Les signatures El Gamal, Schnorr, DSA, ECDSA utilisent toutes Fiat-Shamir.