1984 without Big Brother: Anonymous Credential Systems and Variations

Anna Lysyanskaya

Brown University

The Year 1984

- The world without much electronic data

The Year 1984

- The world without much electronic data

The Year 1984

- David Chaum, "A New Paradigm for Individuals in the Information Age" IEEE S&P Oakland

"As the use of computers becomes more pervasive, they are bound to have substantial influence on our relationships with organizations… …Identifying numbers, addresses and references allow the various records relating to a particular individual to be linked and collected together into a "dossier…" A great deal about a person's habits, entertainment, travel, organizational affiliations, information consumption, etc. would be included in the dossier. … A dossier society [is] reminiscent of Orwell's 1984."

The Year 1984

- David Chaum, "A New Paradigm for Individuals in the Information Age" IEEE S&P Oakland

"In a new paradigm, instead of identifying information, individuals … [use] pseudonyms…

Communication: [onion routing, Chaum81]

Payments: [ecash, Chaum82]

Credentials: allow the individual to control the transfer of information about [oneself]. …Each organization knows an individual by a different pseudonym; … can transform a digitally signed credential received from an organization in a way that preserves the digital signature but changes the pseudonym within the credential."

The Year 1984

- David Chaum, "A New Paradigm for Individuals in the Information Age" IEEE S&P Oakland

"Individual protected from organizations"
Individual controls who knows what, even if the rest of the world conspires against her

"Organizations/society protected from individual" Only authorized individuals gain access to resources/individuals cannot lie about their authorization status and other identity attributes; misbehaving individuals can be held accountable

- No contradiction between privacy and authorized access/accountability – cryptography is key to achieving both at the same time!

Specific Questions

- How can you make sure a user is authorized if this user is anonymous?
  - Use anonymous credentials [Chaum85]
- What if an anonymous authorized user does something that's not allowed?
  - Use conditional anonymity (anonymous ecash [CFN88], etokens [CHL05,CHKLM06]): identifying misbehaving users under well-defined conditions
- What if there is an emergency?
  - Use revocable anonymity (group signatures [CvH91] and variants)

James Bond Reads the News

James Bond Reads the News

Today's news?

Show me your subscription.
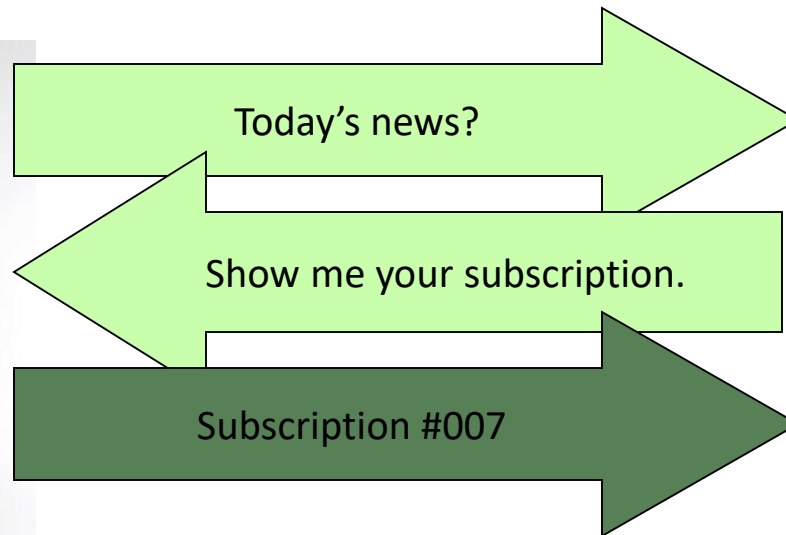
Subscription #007

projo.com

Subscription # is still personally identifiable information, because it allows projo.com to link all of James Bond's transactions together:
- projo.com learns his zip code when he looks up the weather
- learns his date of birth when he reads his horoscope
- learns his gender when he browses the personal ads

85% of US population is uniquely identifiable this way! [Sweeney]

Anonymous Credentials

Today's news?

Prove that you are authorized.

Here is a **zero-knowledge** proof
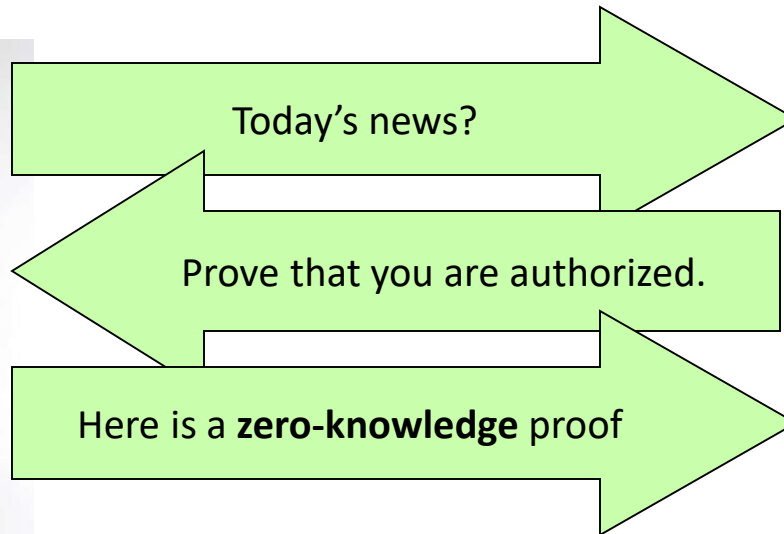
projo.com

Zero-knowledge proof: a proof that a statement is true that does not contain any information as to *why*.

Anonymous Credentials

Today's news?

Prove that you have a subscription,
a Ph.D. and a security clearance.

Here is a zero-knowledge proof

projo.com

Anonymous Credentials

Today's news?

Prove that you are authorized.

Here is a zero-knowledge proof

projo.com

[Chaum84,85,…,LRSW99,CL01,L02,CL04,…,BCCKLS09,…,BL13,…,CL19]
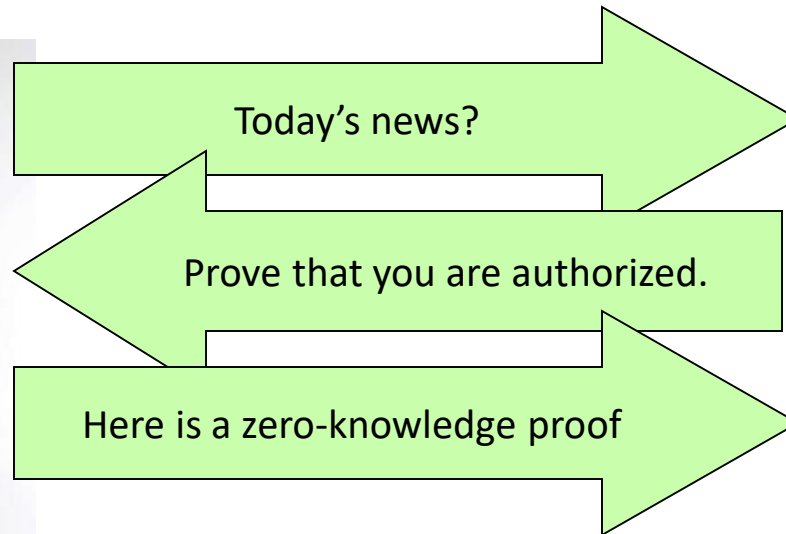
How Does It Work?

Building blocks: digital signatures, protocols, ZK proofs

SETUP: Signature key pair for CA (pk,sk).

SUBSCRIBE:

Bond's SK x

2PC
~Blind sig
[Chaum82]

sk

$\sigma = \sigma_{pk}(x)$

CA
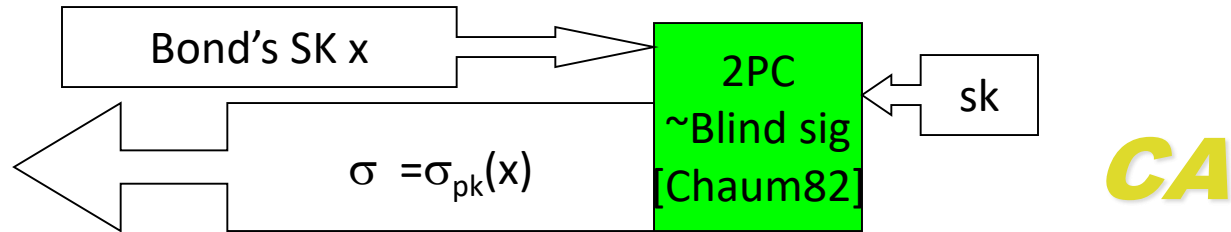
LOGIN:

projo.com

Zero-knowledge proof of knowledge of (x, σ) such that
VerifySig(pk, x, σ) = TRUE

Is It Practical?

- Yes!
  - IBM's Idemix [based on CL01]: works just as I described
  - TCG's Direct Anonymous Attestation [based on CL01,BCC04]
  - Microsoft's uProve [based on Brands99]: slightly different (need a new σ for each login), still very practical
  - Gradient [based on CL19]: hardware root of trust with anonymous attestation

projo.com

σ, ZKPoK of x such that VerifySig(pk,x, σ) = TRUE

Anonymous Credentials

Today's news?

Prove that you are authorized.

Here is a zero-knowledge proof

projo.com

But how can we hold the user accountable if something goes wrong?

Digression: What is identity in this context?
(Never mind privacy!)
How can projo.com know it is talking to James Bond?

Your Identity Online

- When you are online, what makes you <u>you?</u>

I think, therefore I am
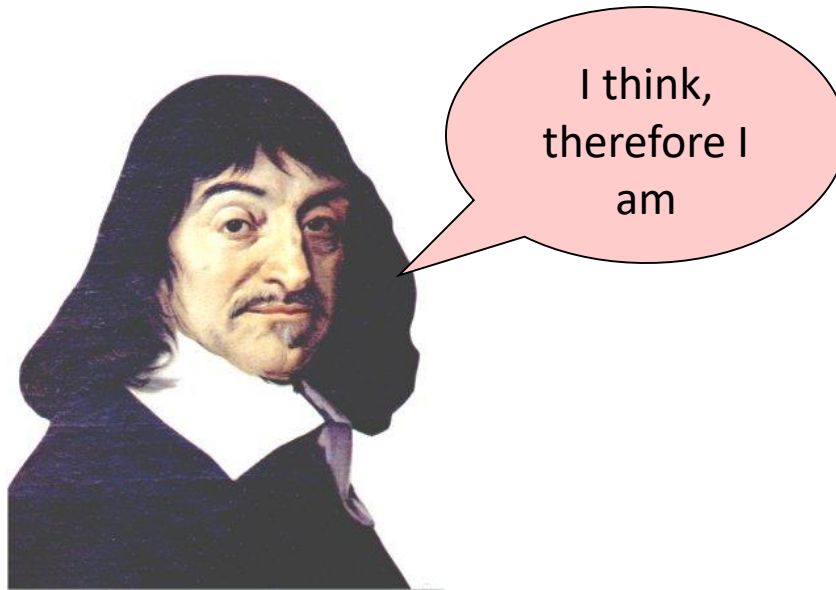
René Descartes

Your Identity Online

- When you are online, what makes you <u>you</u>?

I log in, therefore I am

Disclaimer: provided no one else can log in as me

Anna Lysyanskaya

Conclusion: my password is what makes me <u>me</u>

Your Identity Online

- In general:
  - online, you only have your data to represent you
  - what makes you your online you is a secret that only you or your machine can know

  Your SECRET KEY is YOU.
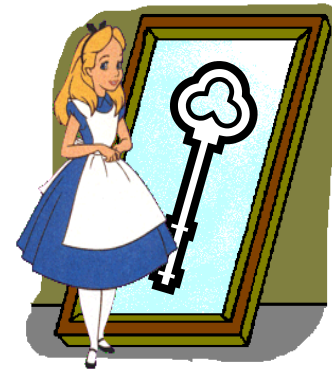
Identity and Accountability

- What are the implications for accountability?

  - Bad news:
    - Identity theft -- someone steals your identity and now you can be held accountable for actions you didn't take.

    - Identity fraud -- you willingly share your identity with your friends, so they can use your credentials and benefits. Hard, but sometimes possible to prevent.

  - Misconception: if all transactions are private, you can't detect and prevent identity fraud. And how do you even know that your identity was stolen?

Identity Fraud/Theft

Today's news?

Who are you? Do you have a subscription?

It's Bond. James Bond.
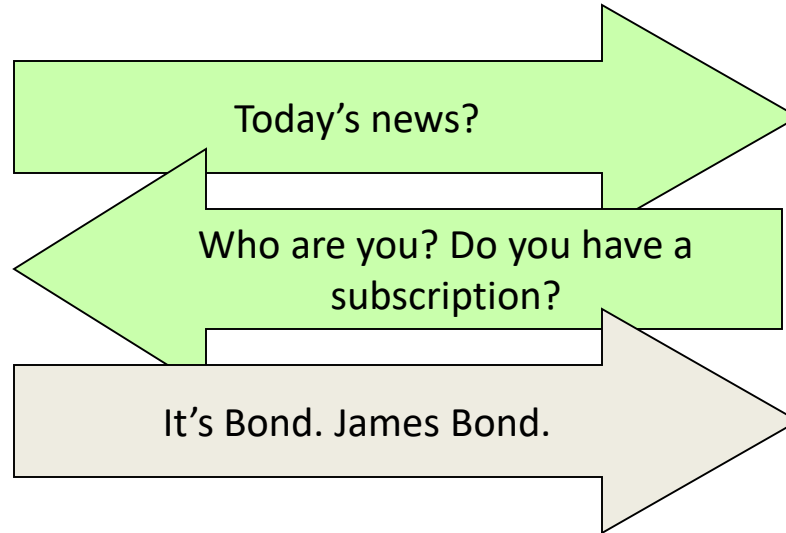
projo.com

Even in this type of login/identification, identity theft/fraud is possible!

Question is: what do providers want to do about it, and how to do it in a privacy-preserving manner.

Conditional Anonymity

Today's news?

Prove that you are authorized.

Here is a zero-knowledge proof, there are only five such proofs for today, and if I use one of them twice, you can add them together and learn my name

projo.com

[CFN88,…,CHL05,CHKLM06]

How Do Single-Use Credentials Work? [ChaumFiatNaor]

- Recall: digital sig... ...oofs of knowledge

- SUBS...

- LOGIN:

Suppose a cred is spent twice.
Same

Privacy for user:
A,T: random,
proof is ZK!

CA

0 < "new" R < Q

A (the credential serial number)
T =x+RB mod Q (double-spending equation)

ZKPOK of (x,B,σ) such that
    1. T = x+RB
    2. VerifySig(pk,(x,A,B), σ) = TRUE

projo.com

Store
(A,R,T,proof)

- SUBSCRIBE to re

Suppose used >N times some day
 =>

Privacy for user:
A,T: psedorandom,
proof is ZK!

-

projo.com

$A=F_s(i,j)$ (the cred serial number)
$T = x+RF_t(i,j) \bmod Q$ (double-spending eq)

ZKPOK of (x,s,t,N,σ) such that
  1. $1 \leq i \leq N$
  2. $A = F_s(i,j)$
  3. $T = x+RF_t(i,j)$
  4. VerifySig(pk,(x,s,t,N), σ) = TRUE
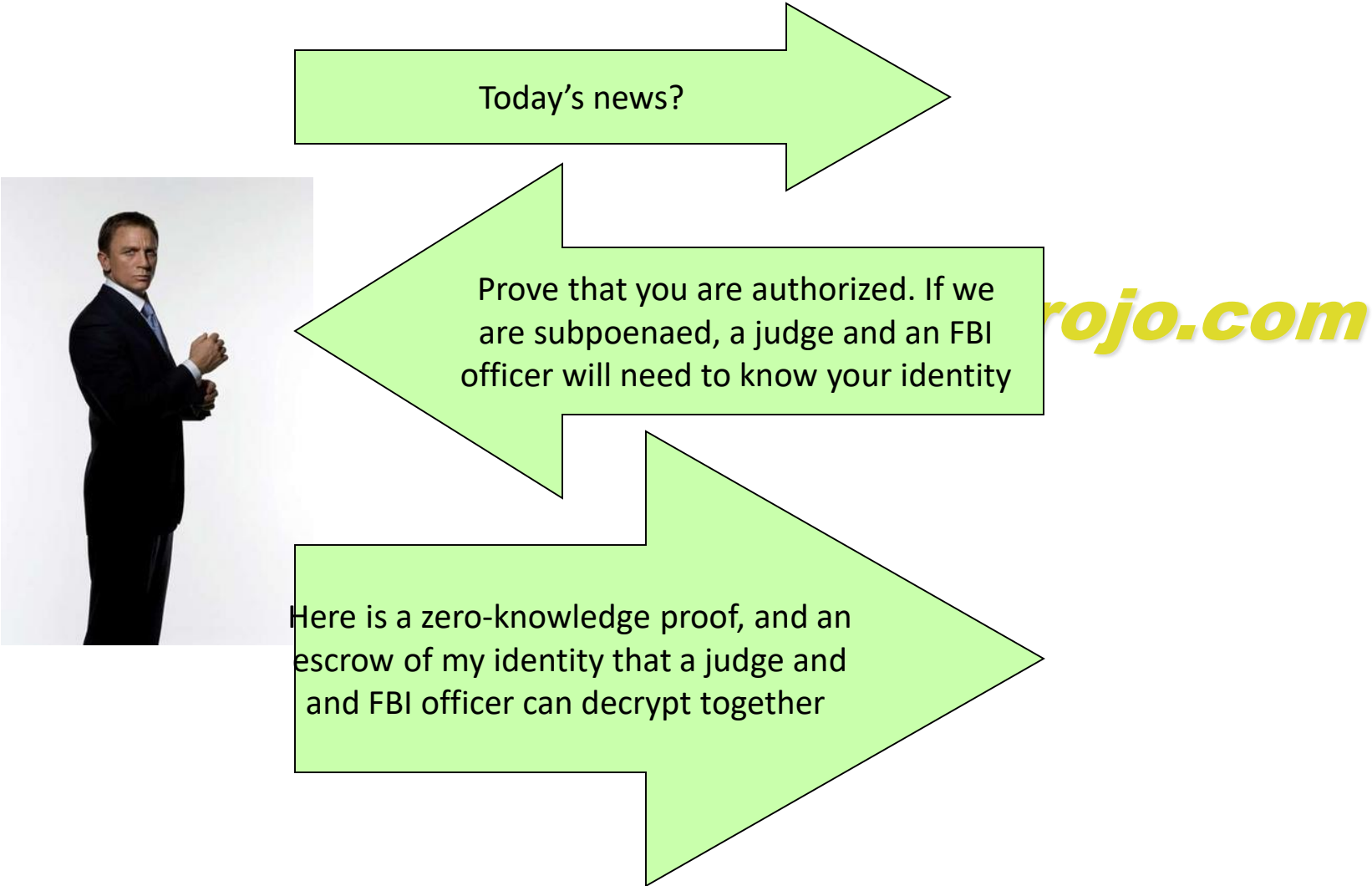
Store
(A,R,T,proof)

But what if something goes very, very wrong, and a thorough investigation is warranted?

Revocable Anonymity [CvH91]

How Does Revocable Anonymity Work?

Building blocks: digital signatures, protocols, ZK proofs, secure encryption

---

SETUP: Signature key pair for CA (pk,sk).

SUBSCRIBE:

Bond's SK x

$\sigma = \sigma_{pk}(x,\text{Bond})$

2PC

sk

CA

LOGIN:

projo.com

$C = \text{Enc}_{FBI+Judge}(\text{Bond})$
ZK proof of knowledge of (x,id,σ) such that
   $\text{VerifySig}(pk,(x,id),\sigma) = \text{TRUE}$
   and C encrypts id
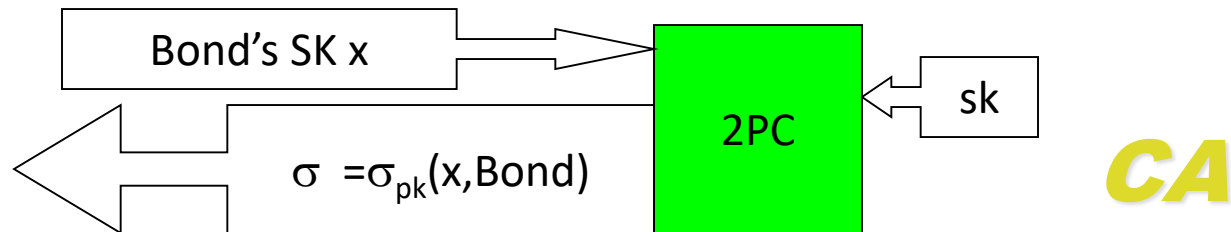
Summary

- No contradiction between anonymity and accountability! Chaum'84 research agenda becoming reality:
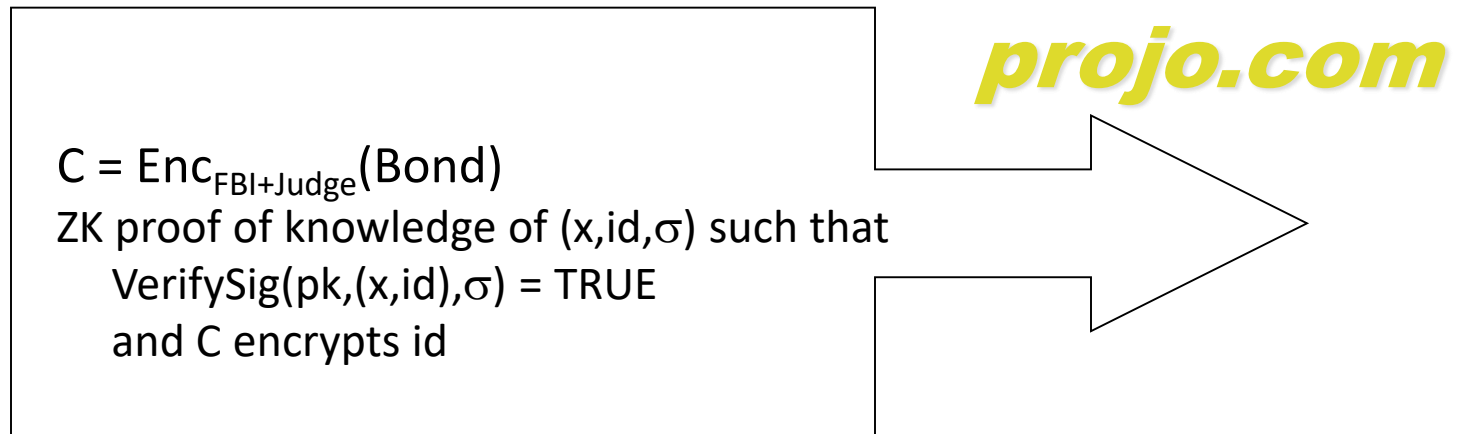 - general architecture [LRSW99,L99,L02,BCL...]
  - specific signature schemes and protocols suited for anonymous credentials [CL02,CL04,BCKL08,BL13,CL19]
  - conditional anonymity [CFN88,CHL05,CHKLM06,BCKL09,...]
  - delegatable anonymous credentials [BCCKLS09,...,CL20]
- Policy and tech communities beginning to catch on
  - Gov't: European Commission, NSTIC
  - Tech giants: TCG, IBM, Microsoft, Google, Apple
- Good vs. evil: cryptography saves the day!