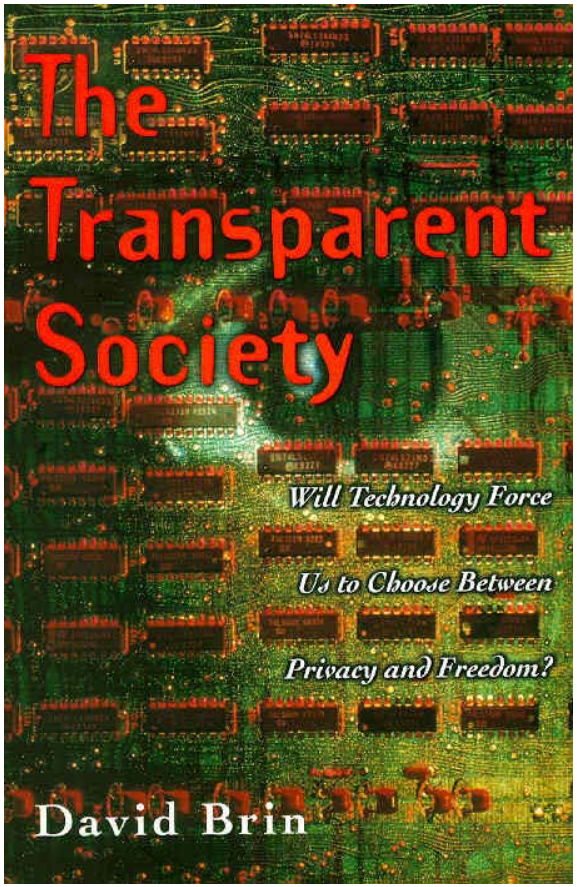
How to Balance Privacy and Key Management in User Authentication

Anna Lysyanskaya
Brown University

Privacy vs. Accountability

- The Transparent Society? (A 1998 book by David Brin)



Privacy vs. Accountability

- Society without electronic data?

Privacy vs. Accountability

- CURRENTLY: The worst of both worlds:
  - Personal data is collected and stored even when it is not needed, and can be accessed by savvy adversaries
  - Personal data cannot be located when you need it
  - (Or cannot be released due to a poorly designed or misunderstood privacy policy)
  - Examples:
    - Your login is your email address
    - Your bank asks for your grandparents' names
    - medical records…
    - RFID passports

Privacy vs. Accountability

- WANT: the BEST of both worlds:
  - Personal attributes collected only when a task cannot be carried out without them
  - Personal data is only disclosed under well-defined conditions, to which the person agrees

Privacy vs. Accountability

- GOVERNMENT'S ROLE:
  - Privacy standards/guidelines/policies
  - Policies for when to grant access to data
  - Identity/key management infrastructure

Privacy vs. Accountability

- What cryptography can do:
  - Everything!
  - Anonymity when you need it
  - Accountability when you need it
  - (Some of this is counter-intuitive)

My Thesis Statement

- No contradiction between personal privacy and accountability/key management/revocation – can achieve the best of both worlds!

Why Is This Good News for Service Providers?

- Cannot be liable for leaking information that you didn’t collect!

Specific Questions

- How can you make sure a user is authorized if this user is anonymous?
  - Use anonymous credentials! [Chaum85,...,CL01,CL04,...]
- What if an anonymous authorized user does something that's not allowed?
  - Use conditional anonymity (anonymous ecash, etokens): identifying misbehaving users under well-defined conditions [CHL05,CHKLM06,BCKL09,...]
- What if there is an emergency?
  - Use revocable anonymity (group signatures and variants) [CvH91,CS97,ACJT00,BBS04,...]
- How to efficiently revoke anonymous credentials?
  - Various cute cryptographic techniques, some of them unexpected [CL02b,...,LPY12]

James Bond Reads the News

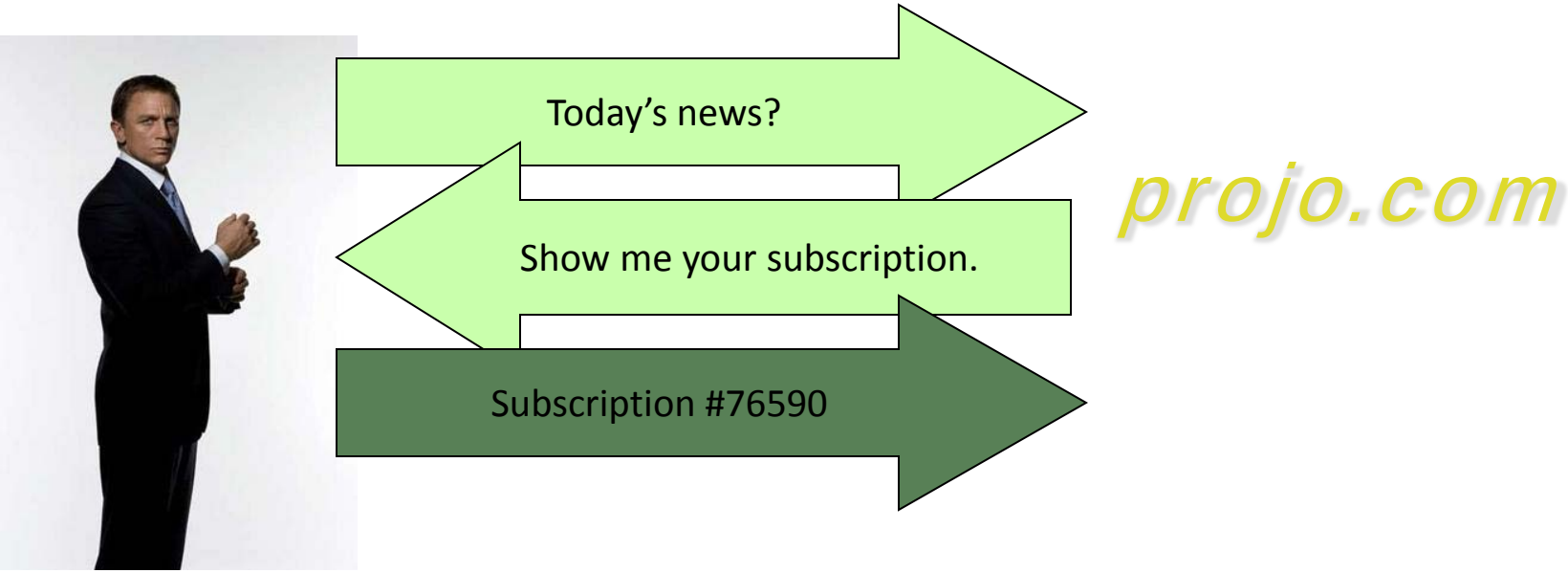
Today's news?

Who are you? Do you have a subscription?

I can tell you, but then I'll have to kill you...

projo.com

Newspaper Subscription

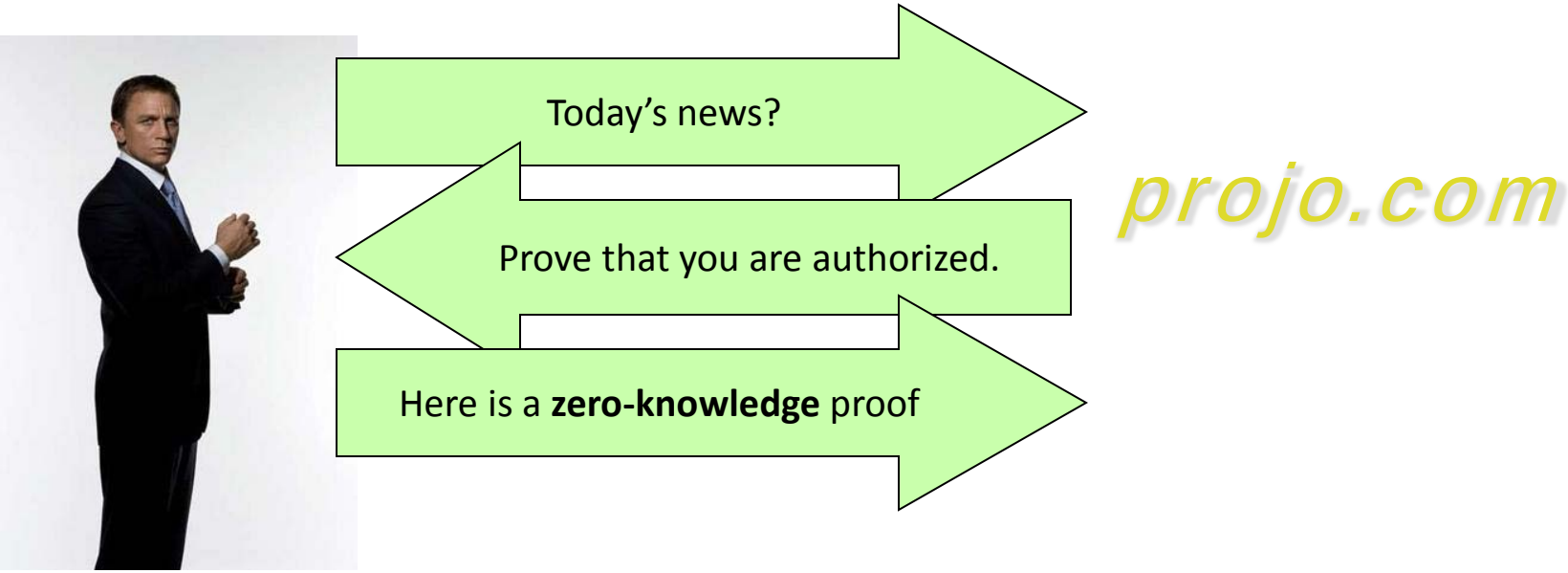


Subscription # is still personally identifiable information, because it allows projo.com to link all of James Bond's transactions together:

- 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

87% of US population is uniquely identifiable this way! [Sweeney]

Anonymous Credentials



Zero-knowledge proof: a proof that a statement is true that does not contain any information as to *why* [GMR85]

It's counter-intuitive that it can exist, but it does, for any provable assertion [GMW86]!

Anonymous Credentials

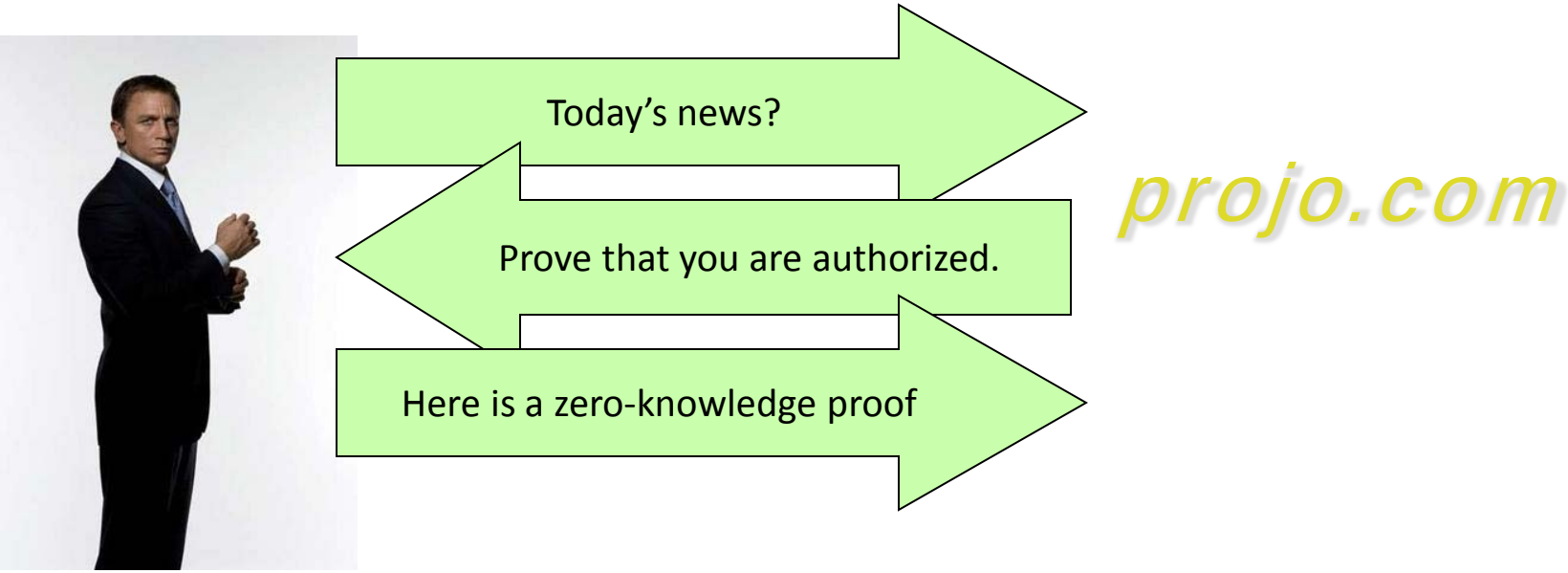
Today's news?

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

Here is a zero-knowledge proof

projo.com

Anonymous Credentials



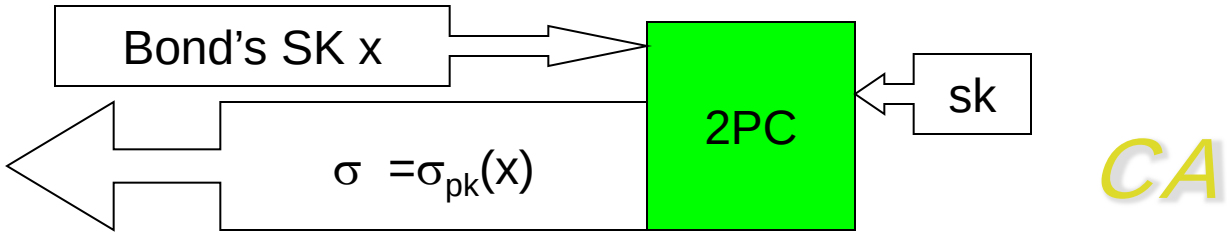
[Chaum85,…,LRSW99,Brands99, CL01,L02,…,BCCKLS09,CKLM13]

How Does It Work? [LRSW99,CL01,L02]

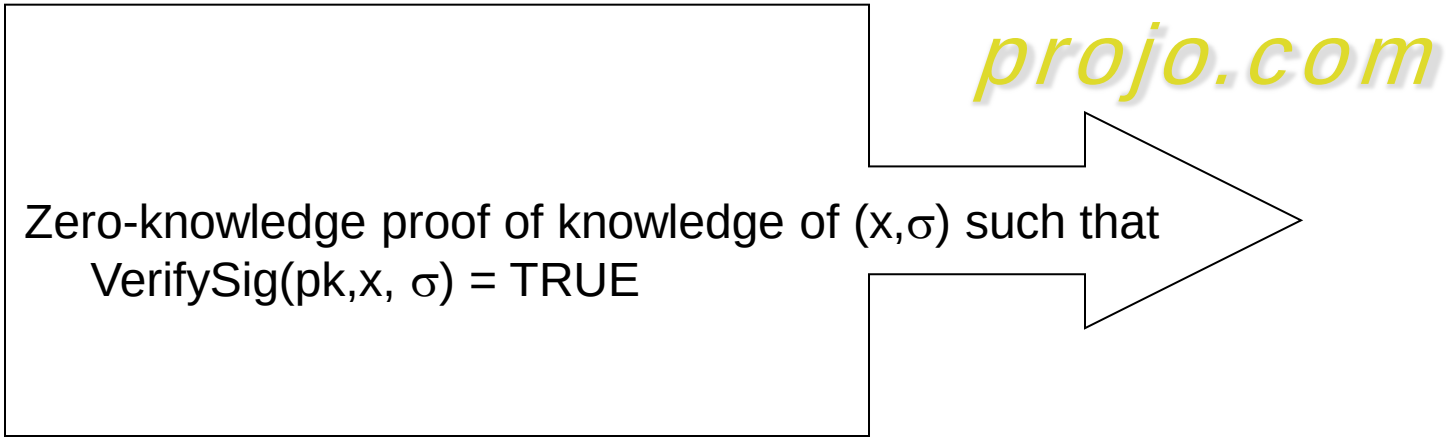
Building blocks: digital signatures, secure two-party protocols, ZK proofs

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

SUBSCRIBE:



LOGIN:



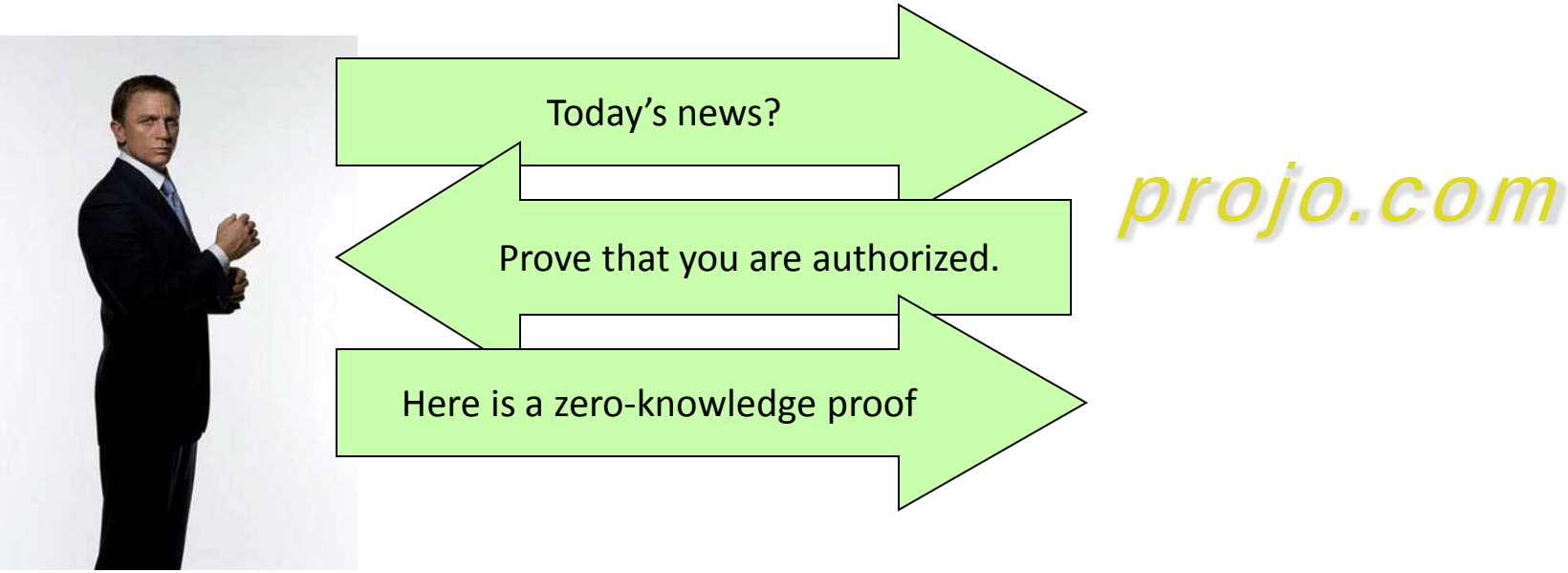
Is It Practical?

- Yes!
  - IBM's Idemix: works just as I described, crypto based on [CL01,L02,CL02]
  - Microsoft's UProve: slightly different (need a new σ for each login), still very practical [Brands99]

projo.com

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

Anonymous Credentials

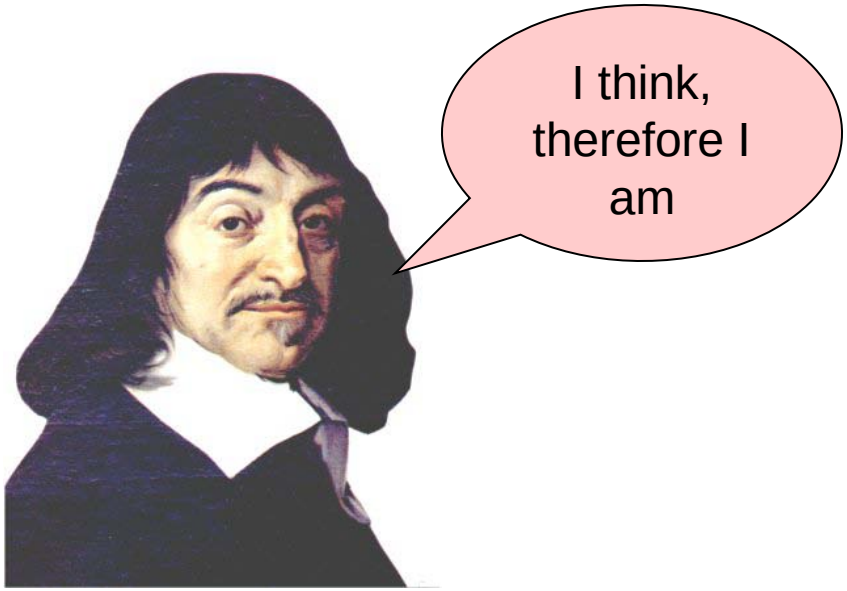


But how can we hold James Bond accountable if something goes wrong?

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>



René Descartes

Your Identity Online

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

Disclaimer: provided no one else can log in as me

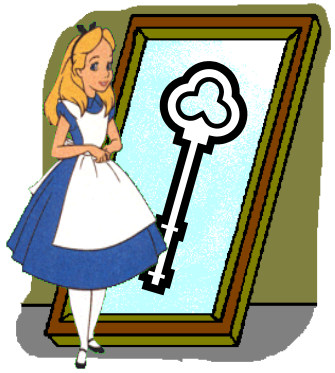
Anna Lysyanskaya

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

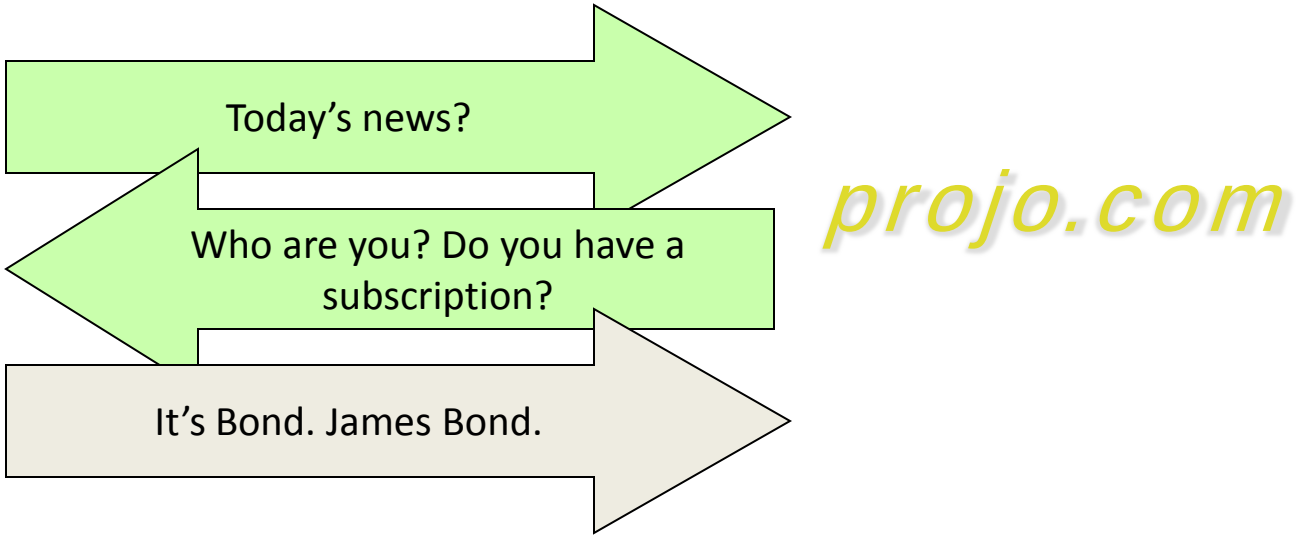
Your SECRET KEY is YOU.



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 know that your identity was stolen?

Identity Fraud/Theft



Projo.com won't know it's not James Bond. They may get suspicious at the frequency with which this subscriber checks the news, and if the subscriber is anonymous they won't know any better.

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

[CHL05,CHKLM06]

How Do Single-Use Credentials Work? [ChaumFiatNaor,Brands

- Recall: digital signatures, secure 2-party computation, ZK proofs of knowledge
- SETUP: Signature key pair for CA (pk,sk).
  Large prime Q
- SUBSCRIBE:

Bond's SK x

Random A,B < Q

$\sigma = \sigma_{pk}(x,A,B)$

2PC

sk

CA

- LOGIN:

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)

How Do Limited-Use Credentials Work? [CHL05,CHKLM06]

- SUBSCRIBE to read paper N times per day

Bond's SK x →

← Random s,t
$\sigma = \sigma_{pk}(x,s,t,N)$

2PC

sk →

CA

- LOGIN for the ith time on Day j: s, t are used as seeds to a pseudorandom function $F_{()}()$

← 0 < "new" R < Q

$A=F_s(i,j)$ (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. $1 \le i \le N$
2. $A = F_s(i,j)$
3. $T = x+RF_t(i,j)$
4. VerifySig(pk,(x,s,t,N), σ) = TRUE

projo.com

Store
(A,R,T,proof)

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

Identity Escrow

Today's news?

Prove that you are authorized. If we are subpoenaed, a judge and an FBI officer will need to know your identity

Here is a zero-knowledge proof, and an escrow of my identity that a judge and and FBI officer can decrypt together

[CvH,…,ACJT00,L02,CS03,…]

How Does Identity Escrow Work?

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

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

SUBSCRIBE:

Bond's SK x

2PC

sk

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

CA

LOGIN:

$C = \text{Enc}_{\text{FBI+Judge}}(\text{Bond})$

ZK proof of knowledge of (x,id,σ) such that

VerifySig(pk,(x,id),σ) = TRUE

and C encrypts id

projo.com

How to Revoke Anonymous Credentials?

Revocation of Credentials

- Non-anonymous
  - Approach 1: Refresh creds every day; revoked ones don’t get refreshed
  - Approach 2: Maintain revocation lists
- Anonymous
  - Approach 1: Refreshing works the same way
  - Approach 2: A user must prove that (s)he is not on the revocation list

Revocation Lists for Anonymous Credentials

- Dynamic accumulators [CL02b]
  - Think of it as a “hash” of membership certificates
  - A user can efficiently prove he is in the accumulator
  - Revocation means “removing” a user from the accumulator (can be done efficiently); non-revoked users can still prove that they are in the new accumulator
- Subset cover techniques [LibertPetersYung12]
  - A user can efficiently prove he is not in the revocation list just as efficiently as it would take in the non-anonymous case!

Bibliography (1)

- Anonymous credentials
  - Cryptographic algorithms [Chaum85 ,…, Brands99, CamenischLysyanskaya01,02,04,…]
  - Two deployable implementations:
    - Microsoft's UProve
    - IBM's Idemix
  - Pilots in progress on university campuses in Sweden and Greece (EU project ABC4Trust)
  - Pilot planned for 2013-2014 on major US campuses (collaboration with Internet2)

- Anonymous e-tokens, conditional anonymity, identity escrow
  - Cryptographic algorithms for e-cash [Chaum82, …, Brands93,…] and compact e-cash and e-tokens [CamenischHohenbergerLysyanskaya05,CHKLM05], group signatures [CvH,…,ACJT00,BLS04]
  - Proof-of-concept implementation: Brown's "Brownie points" project

Bibliography (2)

- Revocation of anonymous credentials
  - Dynamic accumulators [CL02b]
  - Subset-cover techniques [LPY12]

Conclusions

- No contradiction between privacy and accountability!
  - There are technologies for it that have been extensively looked at by cryptographers and computer security researchers, in fact a diversity of algorithms to choose from.
  - Some of these ideas are counter-intuitive.
- Good policy is key