Anonymous Credentials

Anna Lysyanskaya
Brown University

The Year 1984

- The world without much electronic data

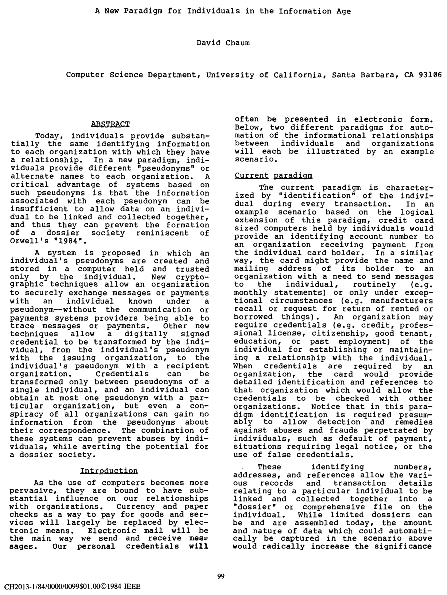
The Year 1984

- 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.”



A New Paradigm for Individuals in the Information Age

David Chaum

Computer Science Department, University of California, Santa Barbara, CA 93106

ABSTRACT

Today, individuals provide substantially the same identifying information to each organization with which they have a relationship. In a new paradigm, individuals provide different "pseudonyms" or alternate names to each organization. A critical advantage of systems based on such pseudonyms is that the information associated with each pseudonym can be insufficient to allow data on an individual to be linked and collected together, and thus they can prevent the formation of a dossier society reminiscent of Orwell's "1984".

A system is proposed in which an individual's pseudonyms are created and stored in a computer held and trusted only by the individual. New cryptographic techniques allow an organization to securely exchange messages or payments with an individual known under a pseudonym--without the communication or payments systems providers being able to trace messages or payments. Other new techniques allow a digitally signed credential to be transformed by the individual, from the individual's pseudonym with the issuing organization, to the individual's pseudonym with a recipient organization. Credentials can be transformed only between pseudonyms of a single individual, and an individual can obtain at most one pseudonym with a particular organization, but even a conspiracy of all organizations can gain no information from the pseudonyms about their correspondence. The combination of these systems can prevent abuses by individuals, while averting the potential for a dossier society.

Introduction

As the use of computers becomes more pervasive, they are bound to have substantial influence on our relationships with organizations. Currency and paper checks as a way to pay for goods and services will largely be replaced by electronic means. Electronic mail will be the main way we send and receive messages. Our personal credentials will often be presented in electronic form. Below, two different paradigms for automation of the informational relationships between individuals and organizations will each be illustrated by an example scenario.

Current paradigm

The current paradigm is characterized by "identification" of the individual during every transaction. In an example scenario based on the logical extension of this paradigm, credit card sized computers held by individuals would provide an identifying account number to an organization receiving payment from the individual card holder. In a similar way, the card might provide the name and mailing address of its holder to an organization with a need to send messages to the individual, routinely (e.g. monthly statements) or only under exceptional circumstances (e.g. manufacturers recall or request for return of rented or borrowed things). An organization may require credentials (e.g. credit, professional license, citizenship, good tenant, education, or past employment) of the individual for establishing or maintaining a relationship with the individual. When credentials are required by an organization, the card would provide detailed identification and references to that organization which would allow the credentials to be checked with other organizations. Notice that in this paradigm identification is required presumably to allow detection and remedies against abuses and frauds perpetrated by individuals, such as default of payment, situations requiring legal notice, or the use of false credentials.

These identifying numbers, addresses, and references allow the various records and transaction details relating to a particular individual to be linked and collected together into a "dossier" or comprehensive file on the individual. While limited dossiers can be and are assembled today, the amount and nature of data which could automatically be captured in the scenario above would radically increase the significance

99

CH2013-1/84/0000/0099$01.00©1984 IEEE

The Year 1984

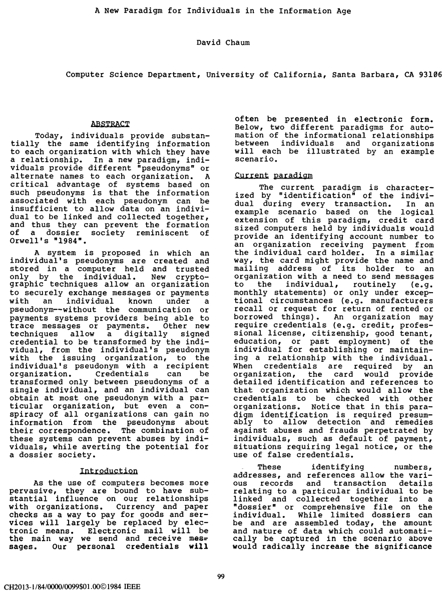
- David Chaum, “A New Paradigm for Individuals in the Information Age” IEEE S&P Oakland

“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.”



A New Paradigm for Individuals in the Information Age

David Chaum

Computer Science Department, University of California, Santa Barbara, CA 93106

ABSTRACT

Today, individuals provide substantially the same identifying information to each organization with which they have a relationship. In a new paradigm, individuals provide different "pseudonyms" or alternate names to each organization. A critical advantage of systems based on such pseudonyms is that the information associated with each pseudonym can be insufficient to allow data on an individual to be linked and collected together, and thus they can prevent the formation of a dossier society reminiscent of Orwell's "1984".

A system is proposed in which an individual's pseudonyms are created and stored in a computer held and trusted only by the individual. New cryptographic techniques allow an organization to securely exchange messages or payments with an individual known under a pseudonym--without the communication or payments systems providers being able to trace messages or payments. Other new techniques allow a digitally signed credential to be transformed by the individual, from the individual's pseudonym with the issuing organization, to the individual's pseudonym with a recipient organization. Credentials can be transformed only between pseudonyms of a single individual, and an individual can obtain at most one pseudonym with a particular organization, but even a conspiracy of all organizations can gain no information from the pseudonyms about their correspondence. The combination of these systems can prevent abuses by individuals, while averting the potential for a dossier society.

Introduction

As the use of computers becomes more pervasive, they are bound to have substantial influence on our relationships with organizations. Currency and paper checks as a way to pay for goods and services will largely be replaced by electronic means. Electronic mail will be the main way we send and receive messages. Our personal credentials will often be presented in electronic form. Below, two different paradigms for automation of the informational relationships between individuals and organizations will each be illustrated by an example scenario.

Current paradigm

The current paradigm is characterized by "identification" of the individual during every transaction. In an example scenario based on the logical extension of this paradigm, credit card sized computers held by individuals would provide an identifying account number to an organization receiving payment from the individual card holder. In a similar way, the card might provide the name and mailing address of its holder to an organization with a need to send messages to the individual, routinely (e.g. monthly statements) or only under exceptional circumstances (e.g. manufacturers recall or request for return of rented or borrowed things). An organization may require credentials (e.g. credit, professional license, citizenship, good tenant, education, or past employment) of the individual for establishing or maintaining a relationship with the individual. When credentials are required by an organization, the card would provide detailed identification and references to that organization which would allow the credentials to be checked with other organizations. Notice that in this paradigm identification is required presumably to allow detection and remedies against abuses and frauds perpetrated by individuals, such as default of payment, situations requiring legal notice, or the use of false credentials.

These identifying numbers, addresses, and references allow the various records and transaction details relating to a particular individual to be linked and collected together into a "dossier" or comprehensive file on the individual. While limited dossiers can be and are assembled today, the amount and nature of data which could automatically be captured in the scenario above would radically increase the significance

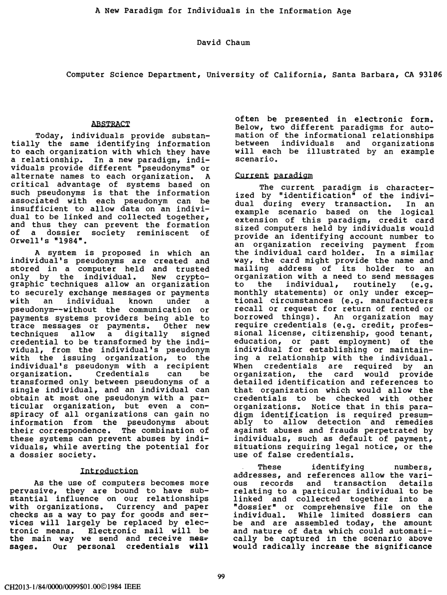
CH2013-1/84/0000/0099$01.00©1984 IEEE

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



A New Paradigm for Individuals in the Information Age

David Chaum

Computer Science Department, University of California, Santa Barbara, CA 93106

ABSTRACT

Today, individuals provide substantially the same identifying information to each organization with which they have a relationship. In a new paradigm, individuals provide different "pseudonyms" or alternate names to each organization. A critical advantage of systems based on such pseudonyms is that the information associated with each pseudonym can be insufficient to allow data on an individual to be linked and collected together, and thus they can prevent the formation of a dossier society reminiscent of Orwell's "1984".

A system is proposed in which an individual's pseudonyms are created and stored in a computer held and trusted only by the individual. New cryptographic techniques allow an organization to securely exchange messages or payments with an individual known under a pseudonym--without the communication or payments systems providers being able to trace messages or payments. Other new techniques allow a digitally signed credential to be transformed by the individual, from the individual's pseudonym with the issuing organization, to the individual's pseudonym with a recipient organization. Credentials can be transformed only between pseudonyms of a single individual, and an individual can obtain at most one pseudonym with a particular organization, but even a conspiracy of all organizations can gain no information from the pseudonyms about their correspondence. The combination of these systems can prevent abuses by individuals, while averting the potential for a dossier society.

Introduction

As the use of computers becomes more pervasive, they are bound to have substantial influence on our relationships with organizations. Currency and paper checks as a way to pay for goods and services will largely be replaced by electronic means. Electronic mail will be the main way we send and receive messages. Our personal credentials will often be presented in electronic form. Below, two different paradigms for automation of the informational relationships between individuals and organizations will each be illustrated by an example scenario.

Current paradigm

The current paradigm is characterized by "identification" of the individual during every transaction. In an example scenario based on the logical extension of this paradigm, credit card sized computers held by individuals would provide an identifying account number to an organization receiving payment from the individual card holder. In a similar way, the card might provide the name and mailing address of its holder to an organization with a need to send messages to the individual, routinely (e.g. monthly statements) or only under exceptional circumstances (e.g. manufacturers recall or request for return of rented or borrowed things). An organization may require credentials (e.g. credit, professional license, citizenship, good tenant, education, or past employment) of the individual for establishing or maintaining a relationship with the individual. When credentials are required by an organization, the card would provide detailed identification and references to that organization which would allow the credentials to be checked with other organizations. Notice that in this paradigm identification is required presumably to allow detection and remedies against abuses and frauds perpetrated by individuals, such as default of payment, situations requiring legal notice, or the use of false credentials.

These identifying numbers, addresses, and references allow the various records and transaction details relating to a particular individual to be linked and collected together into a "dossier" or comprehensive file on the individual. While limited dossiers can be and are assembled today, the amount and nature of data which could automatically be captured in the scenario above would radically increase the significance

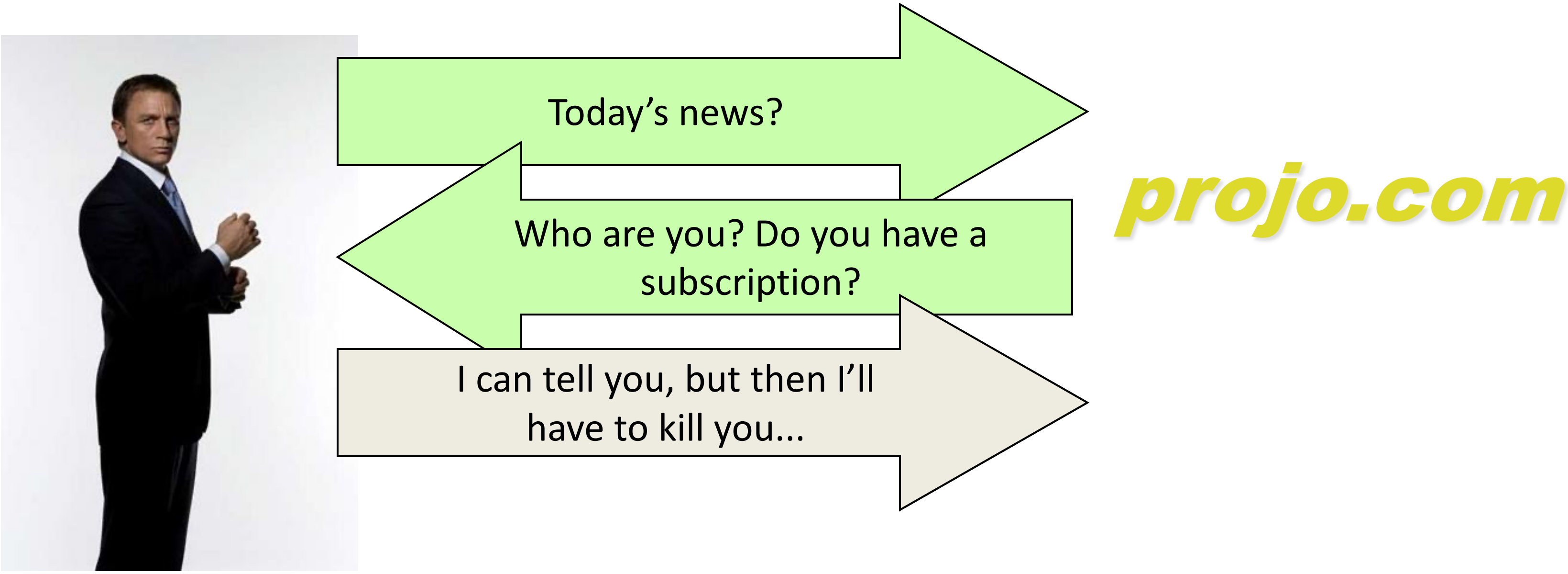
CH2013-1/84/0000/0099$01.00©1984 IEEE

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

50-Year Research Agenda

- How can you make sure a user is authorized if this user is anonymous?
  - Use anonymous credentials [Chaum85,…,CL01,…]
- What if an anonymous authorized user does something that's not allowed?
  - Use conditional anonymity (anonymous ecash [CFN88], etokens [CHL05,CHKLM06,BCKL09]): identifying misbehaving users under well-defined conditions
- What if there is an emergency?
  - Use revocable anonymity (group signatures [CvH91] and variants)
- Can we secretly trace specific users/users that match a specific secret blueprint?
  - Use privacy-preserving blueprints [KLN22]
- Can anonymous credentials be anonymously delegated?
  - Yes [CL06,BCKLS08,CKLM14]
  - Mercurial signatures [CL19,CL21,CLP22,MSBN22]

James Bond Reads the News

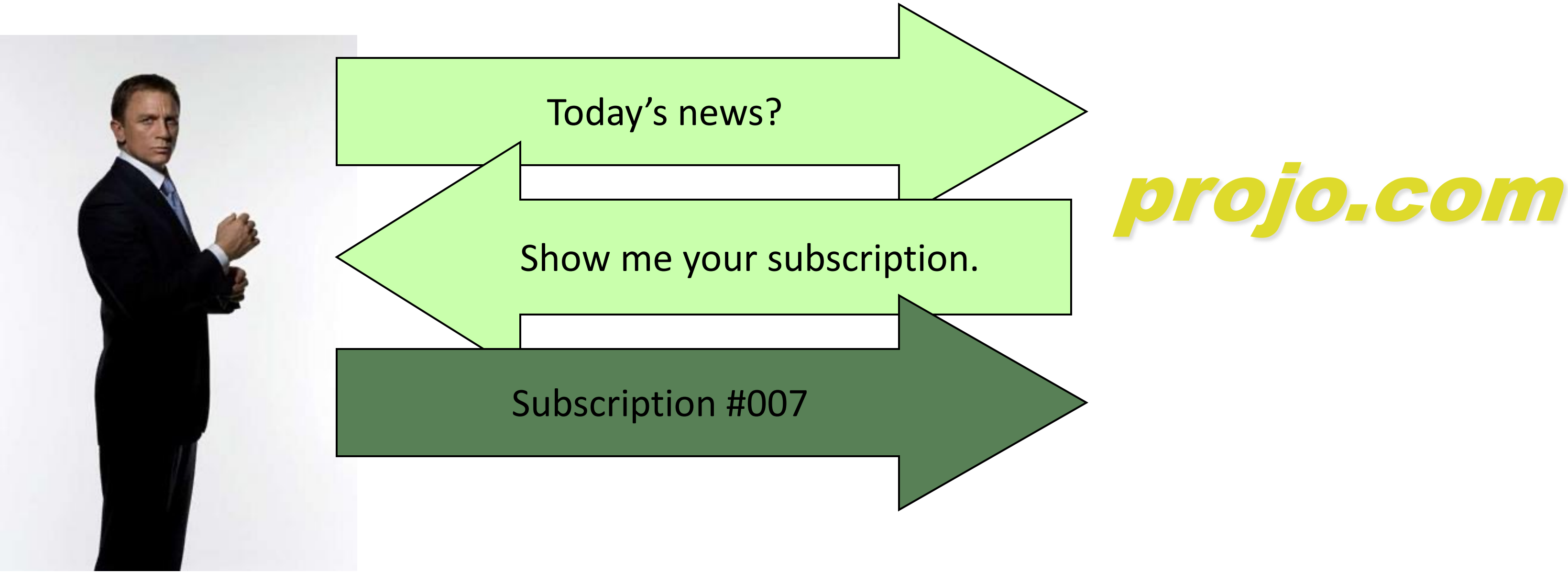


Today's news?

Who are you? Do you have a subscription?

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

James Bond Reads the News



Today's news?

Show me your subscription.

Subscription #007

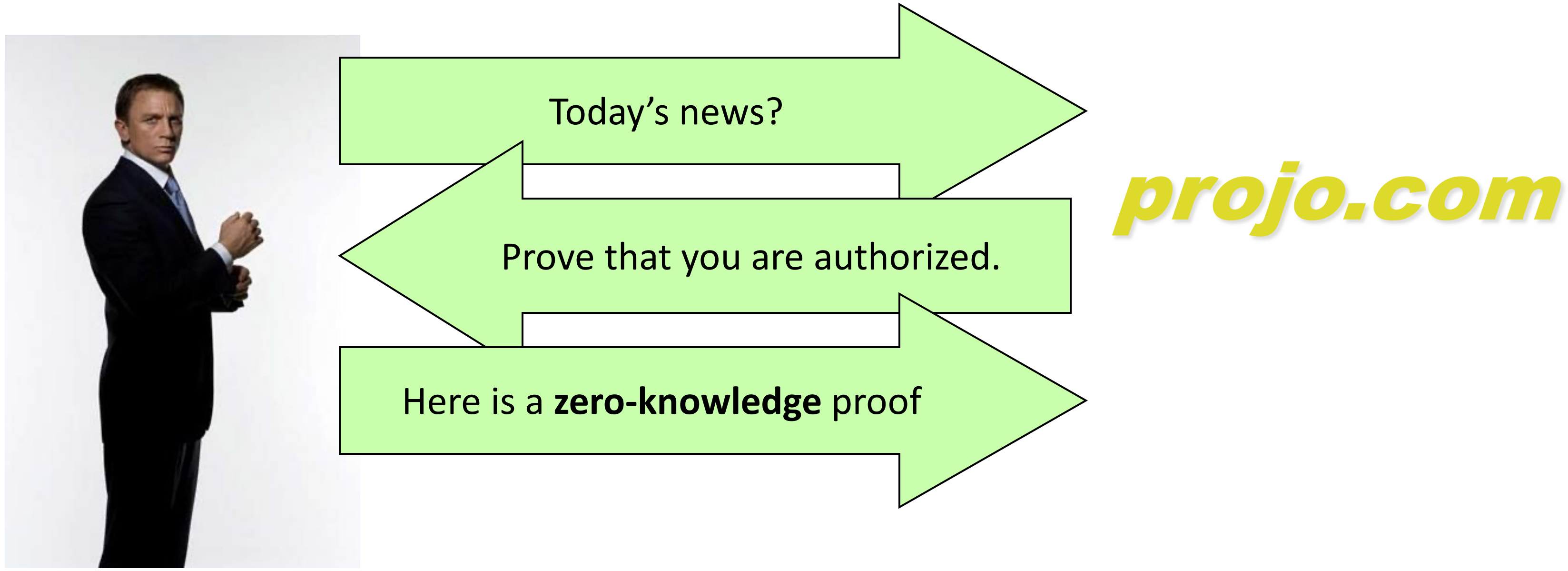
projo.com

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?

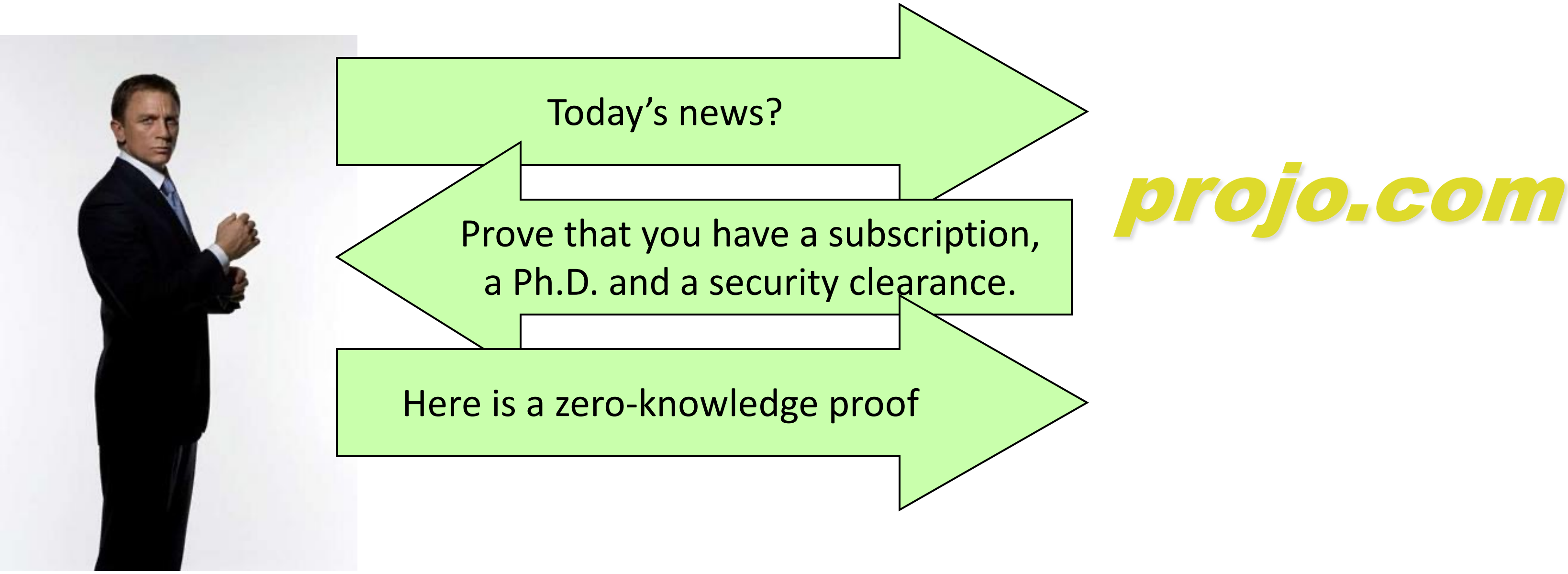
Prove that you are authorized.

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



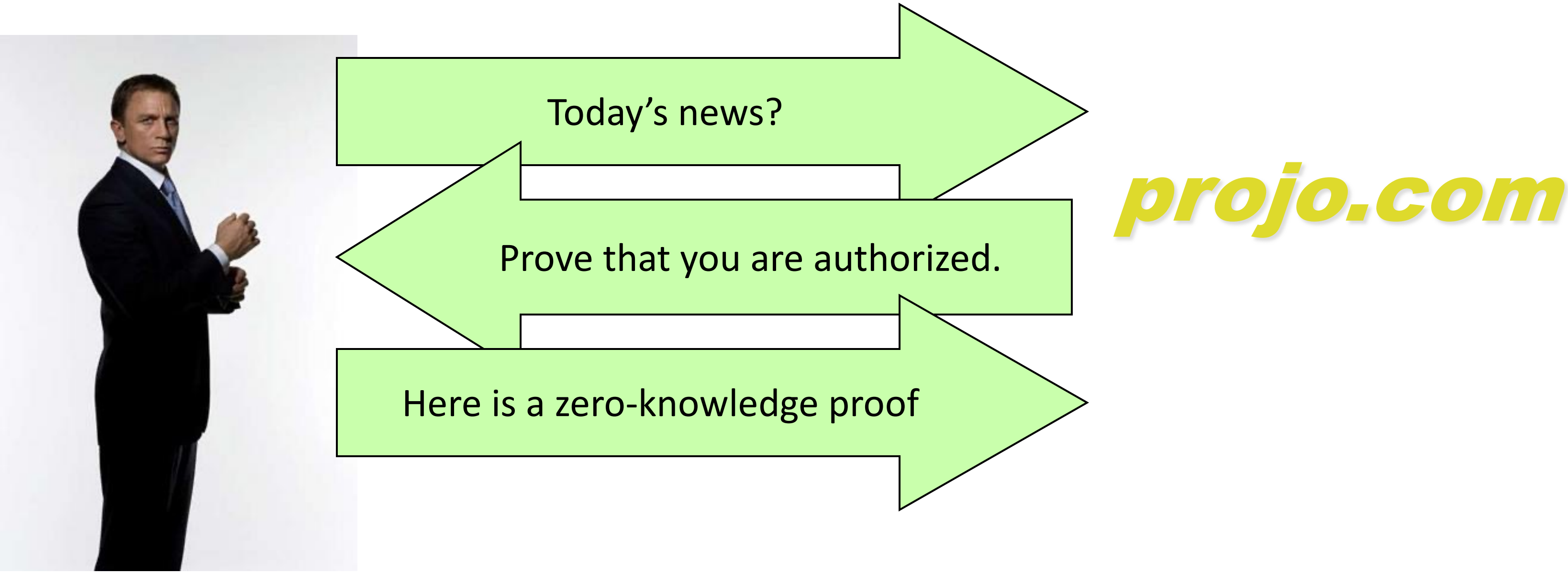
Today's news?

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

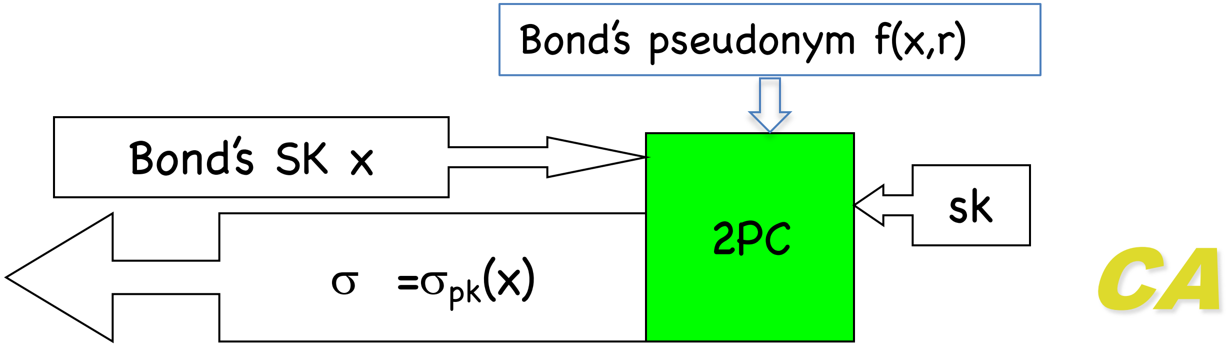
[Chaum84,85,…,LRSW99,CL01,L02,CL04,CL06,…,BCCKLS09,…,BL13,…,CL19,CL21,LR22,KLN22]

How Does It Work?

Building blocks: digital signatures, protocols, ZK proofs

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

SUBSCRIBE:



Bond’s pseudonym f(x,r)

Bond’s SK x

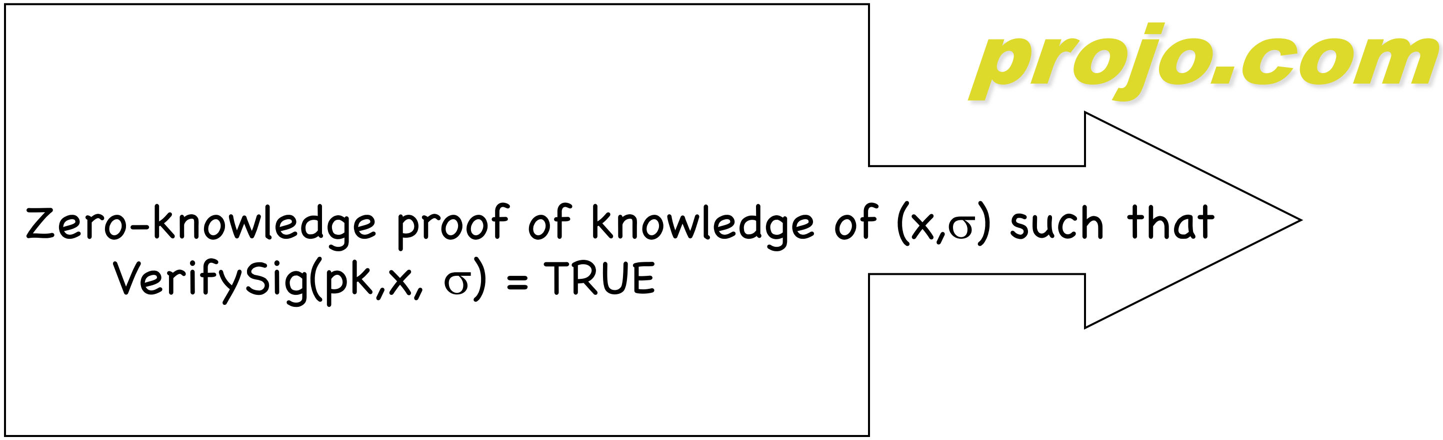
2PC

sk

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

CA

LOGIN:



projo.com

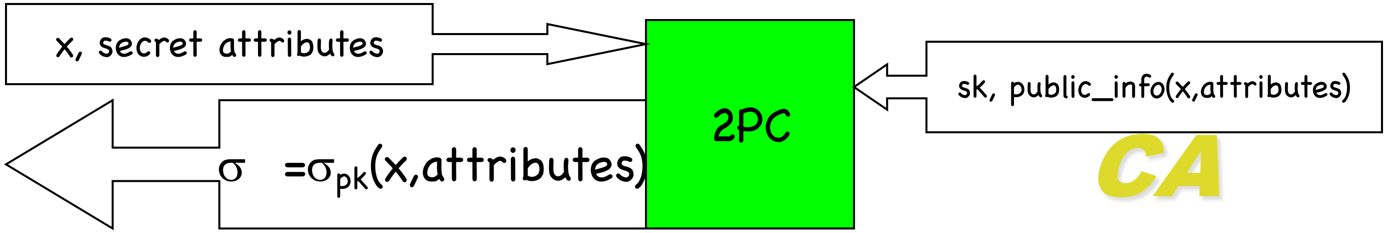
Zero-knowledge proof of knowledge of (x,σ) such that VerifySig(pk,x, σ) = TRUE

Also, identity attributes

Building blocks: digital signatures, protocols, ZK proofs

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

SUBSCRIBE:



x, secret attributes

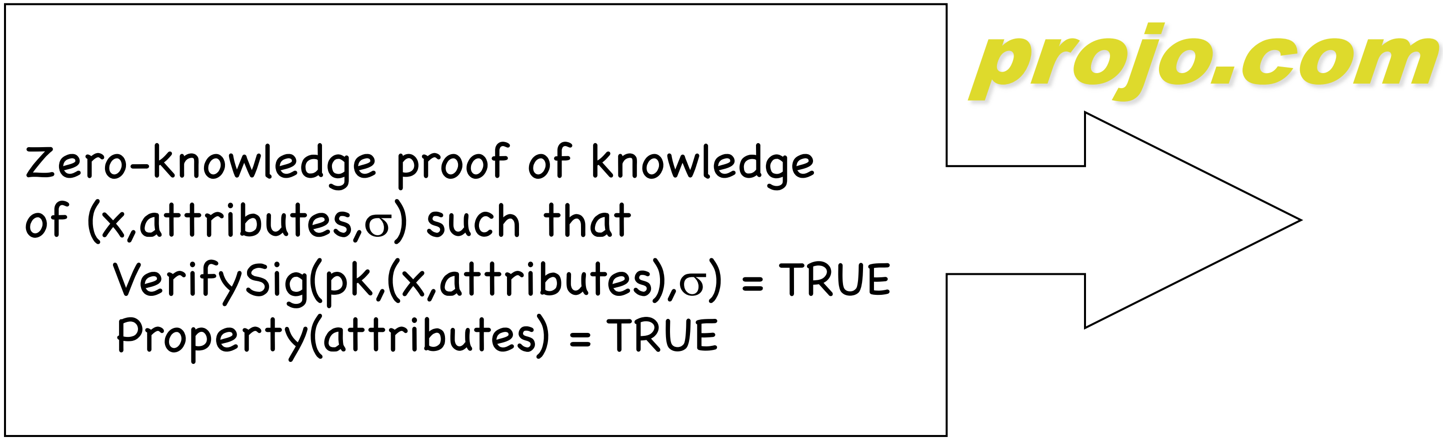
2PC

sk, public_info(x,attributes)

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

CA

LOGIN:



projo.com

Zero-knowledge proof of knowledge of (x,attributes,σ) such that

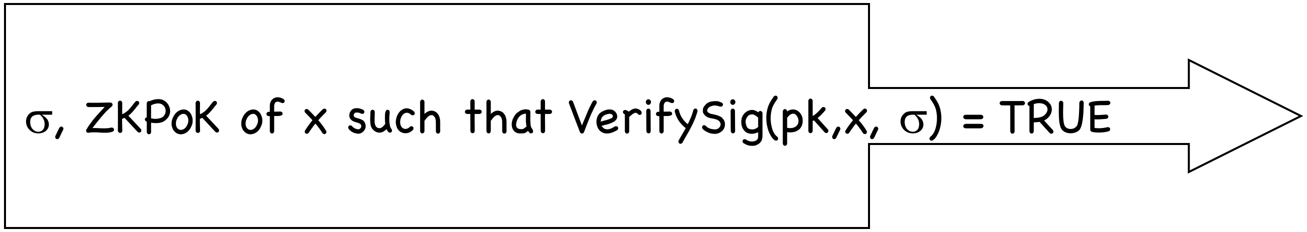
VerifySig(pk,(x,attributes),σ) = TRUE

Property(attributes) = 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
  - Protego [CDLP22, based on CL19]: another practical implementation, based on mercurial signatures

projo.com



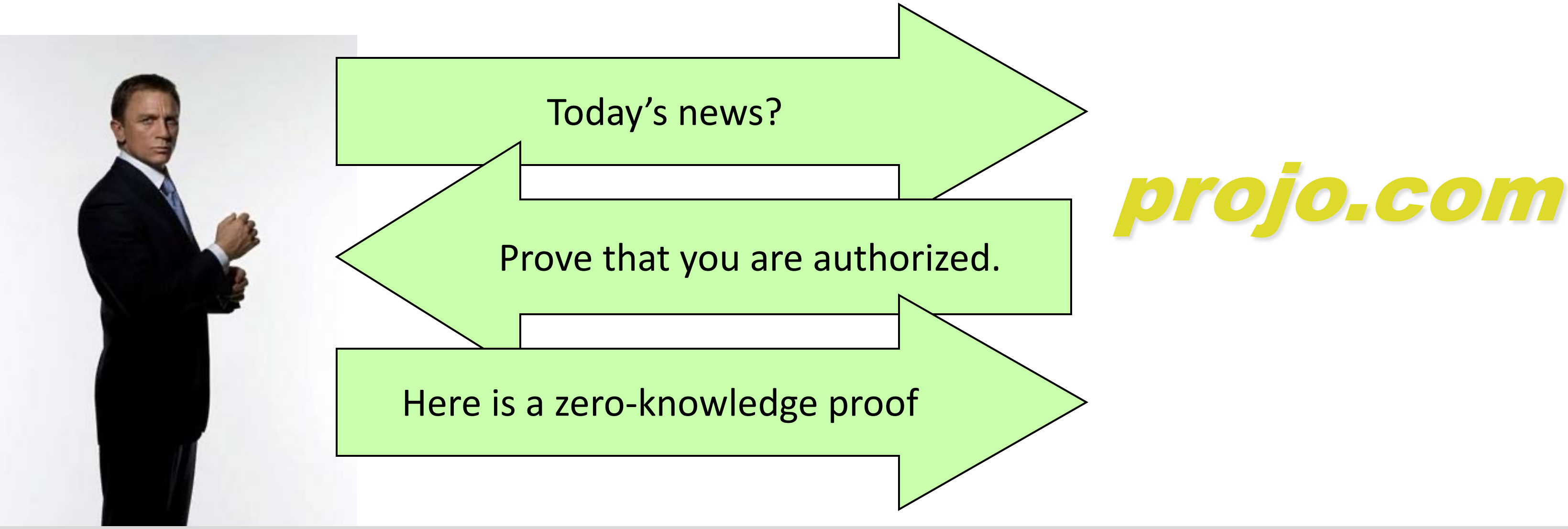
σ, ZKPoK of x such that VerifySig(pk,x, σ) = TRUE

Is It Ready for Practical Use?

- Still a lot of work to do:
  - Devil is in the details!
  - Subtleties in definitions, trust assumptions, complexity assumptions, issues with composition
  - So take everything I say as a proof-of-concept, not necessarily as ready for billions of people to start using this
    - Especially because this talk is a high-level overview, not a deep dive

Do we actually want privacy-preserving authentication?

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?

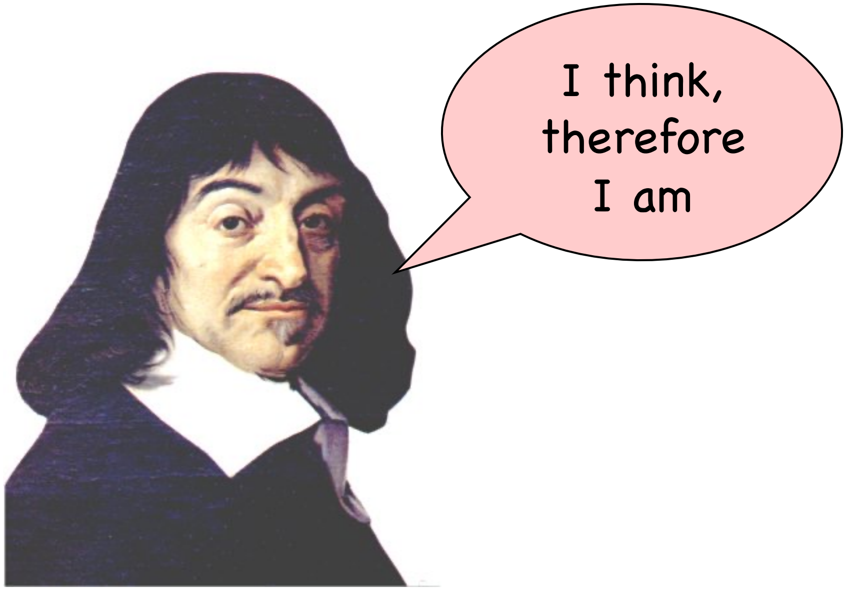
Digression: What is identity in this context?

(Never mind privacy!)

How can projo.com know it is talking to James Bond?

Your Identity Online

- When you are online, what makes you you?



René Descartes

Your Identity Online

- When you are online, what makes you you?

I log in,
therefore
I am

Disclaimer: provided no one else can log in as me

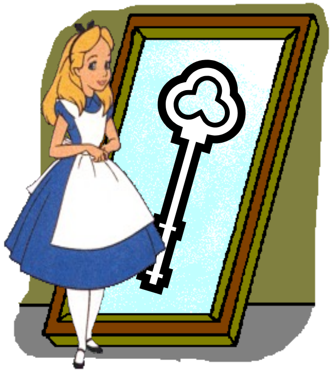
Anna Lysyanskaya

Conclusion: my password is what makes me me

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

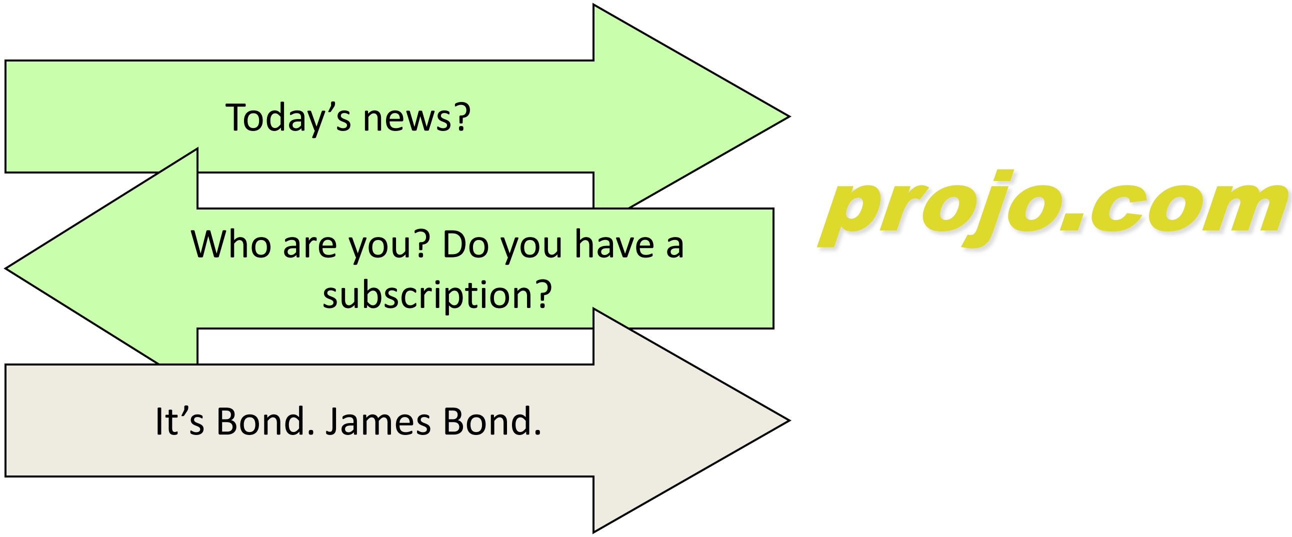
Your SECRET KEY is YOU.



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?

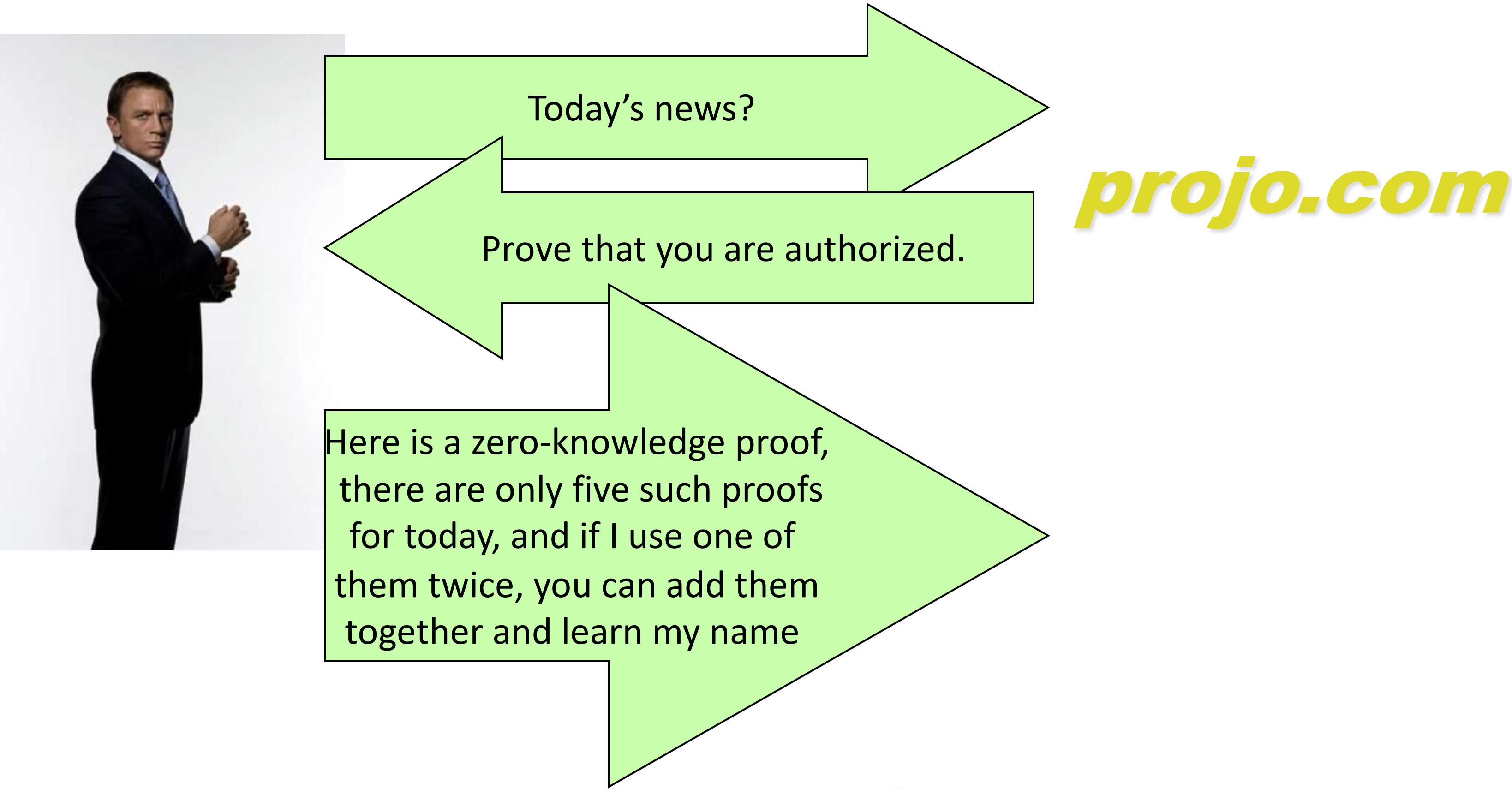
It’s Bond. James Bond.

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

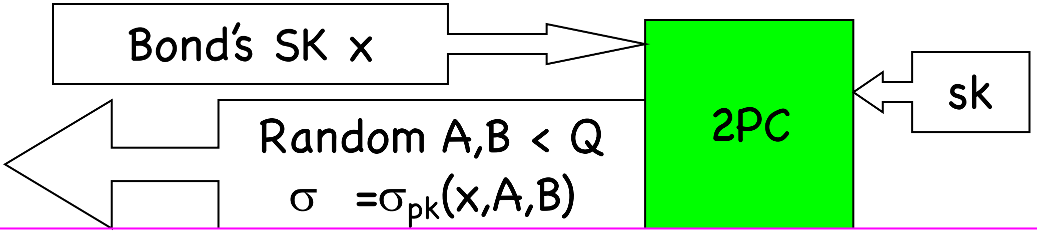
[CFN88,…,CHL05,CHKLM06]

How Do Single-Use Credentials Work? [ChaumFiatNaor]

- Recall: digital signatures, secure 2-party computation, ZK proofs of knowledge

- SETUP: Signature key pair for CA (pk,sk).
  Large prime Q

- SUBSCRIBE:



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

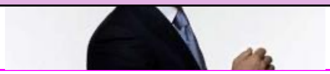
projo.com

Store
(A,R,T,proof)

How Do Single-Use Credentials Work? [ChaumFiatNaor]

- Recall: digital … n, ZK proofs of
-
- SI

Suppose a cred is spent twice.
Same cred => same A
Spent twice: two R's,
with high prob, $R \neq R'$
$T = x+RB \bmod Q$, $T' = x+R'B \bmod Q$
solve for x, id and punish Bond



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

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)

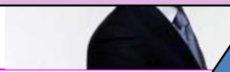
How Do Single-Use Credentials Work? [ChaumFiatNaor]

- Recall: digital … n, ZK proofs of

Suppose a cred is spent twice.
Same

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

- SI



CA

- LOGIN:

0 < "new" R < Q

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

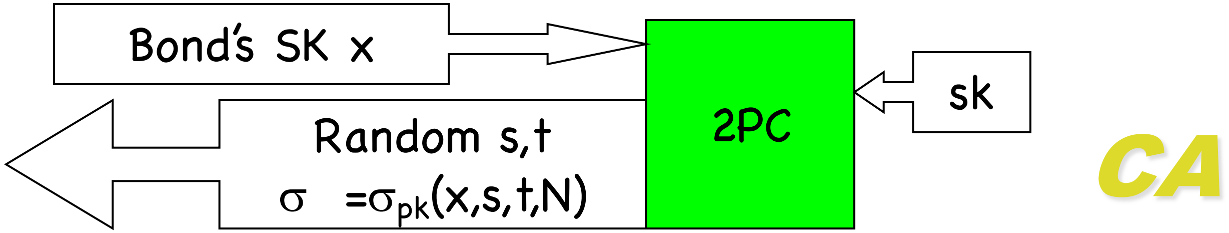
ZKPOK of (x,B,σ) such that
1. T = x+RB
2. VerifySig(pk,(x,A,B), σ) = TRUE

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

2PC

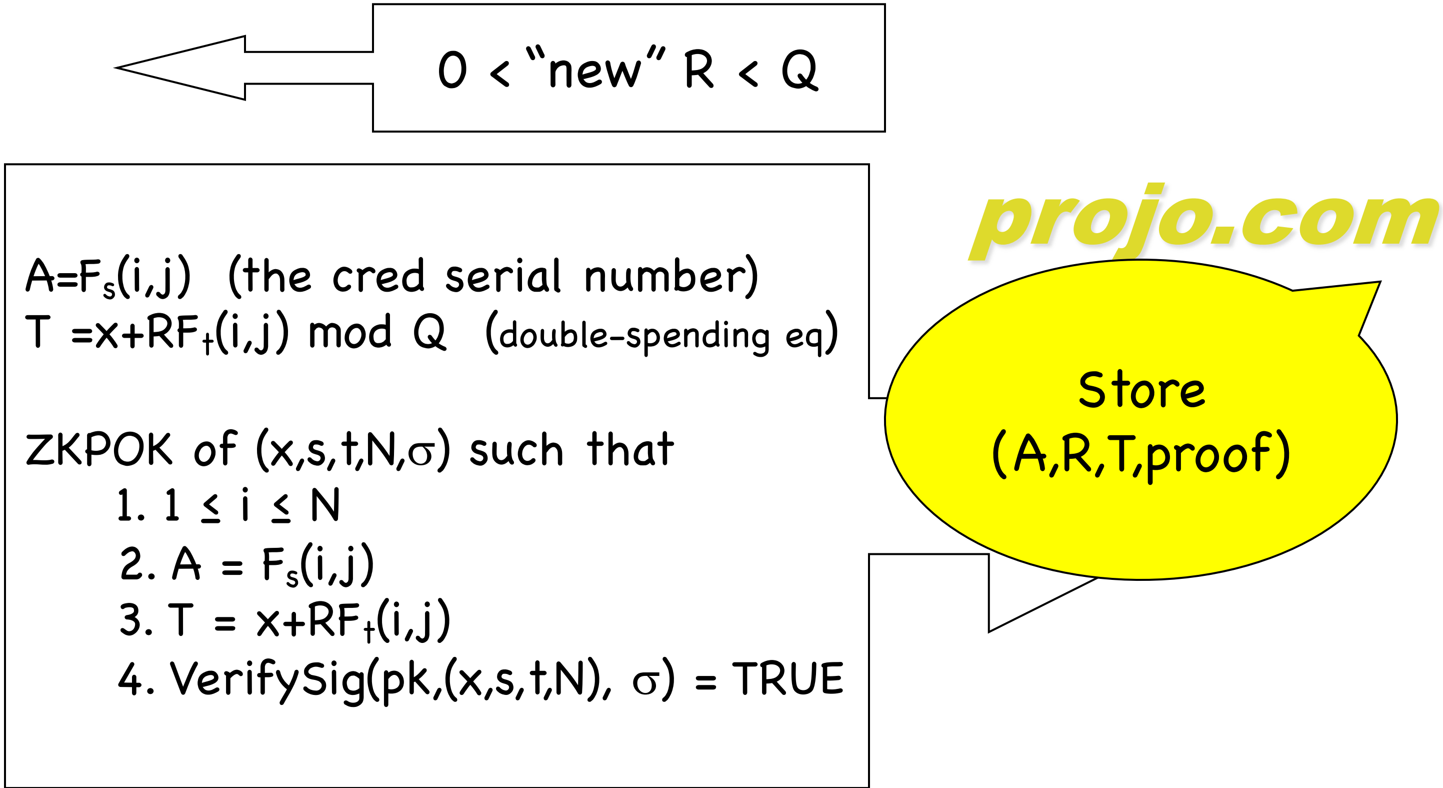
sk

Random s,t

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

CA

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



0 < "new" R < Q

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)

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

- SUBSCRIBE to

Suppose used >N times some day

=> repeating A = $F_s(i,j)$ for some i

A spent twice: two random R's,

with high prob, R ≠ R'

$T = x+RF_t(i,j)$, $T' = x+R'F_t(i,j)$

solve for x, id and punish user

- I

Q

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

rojo.com

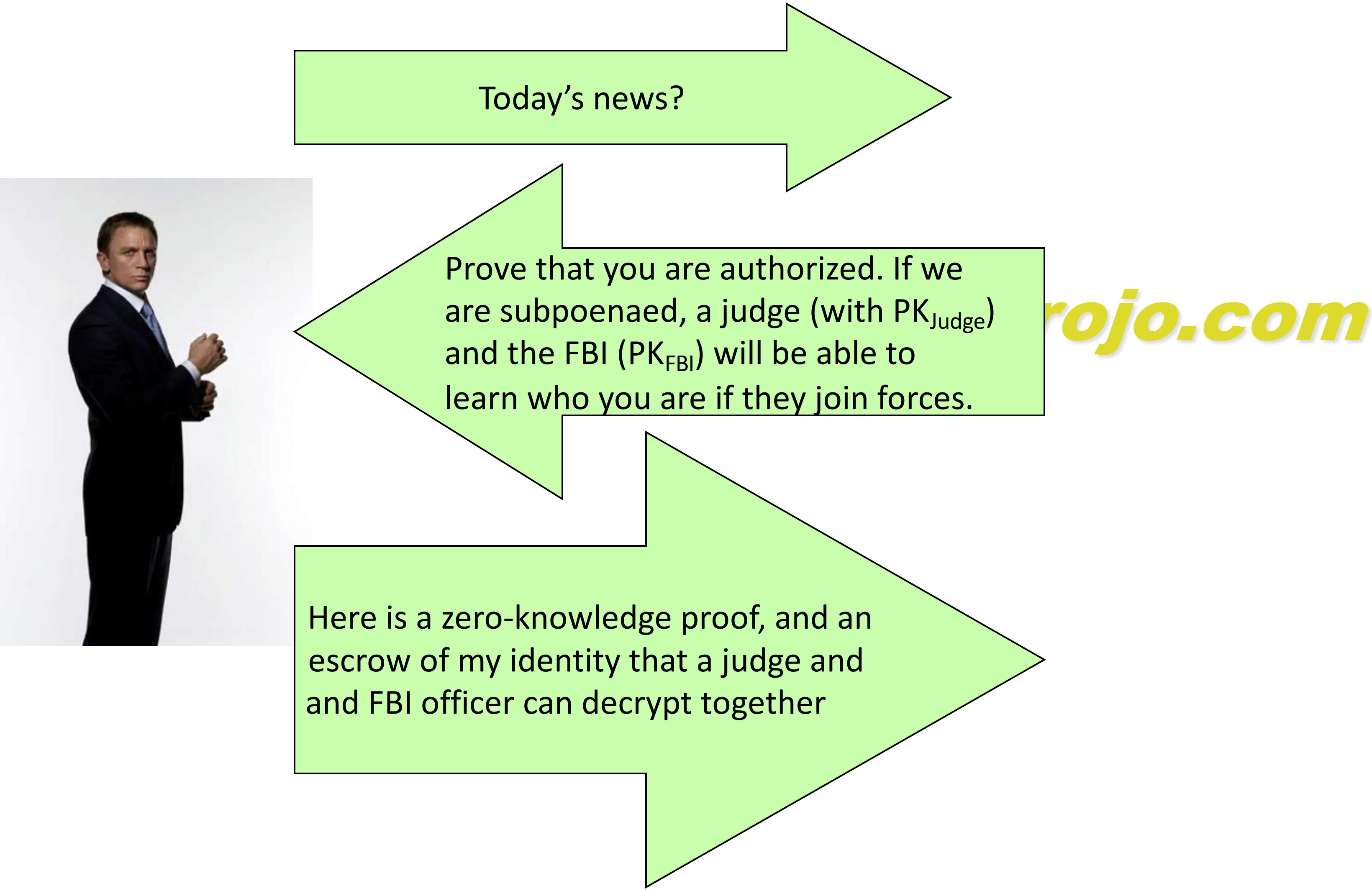
Store
A,R,T,proof)

$F_s(i,j)$

3. $T = x+RF_t(i,j)$
4. VerifySig(pk,(x,s,t,N), σ) = TRUE

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

Revocable Anonymity



Today's news?

Prove that you are authorized. If we are subpoenaed, a judge (with PK_{Judge}) and the FBI (PK_{FBI}) will be able to learn who you are if they join forces.

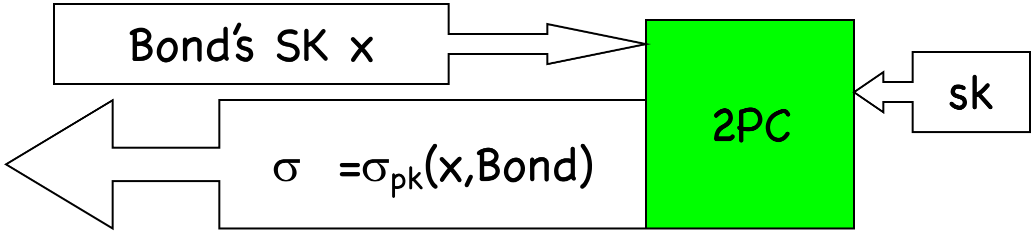
Here is a zero-knowledge proof, and an escrow of my identity that a judge and and FBI officer can decrypt together

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

2PC

sk

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

CA

LOGIN:

projo.com

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

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

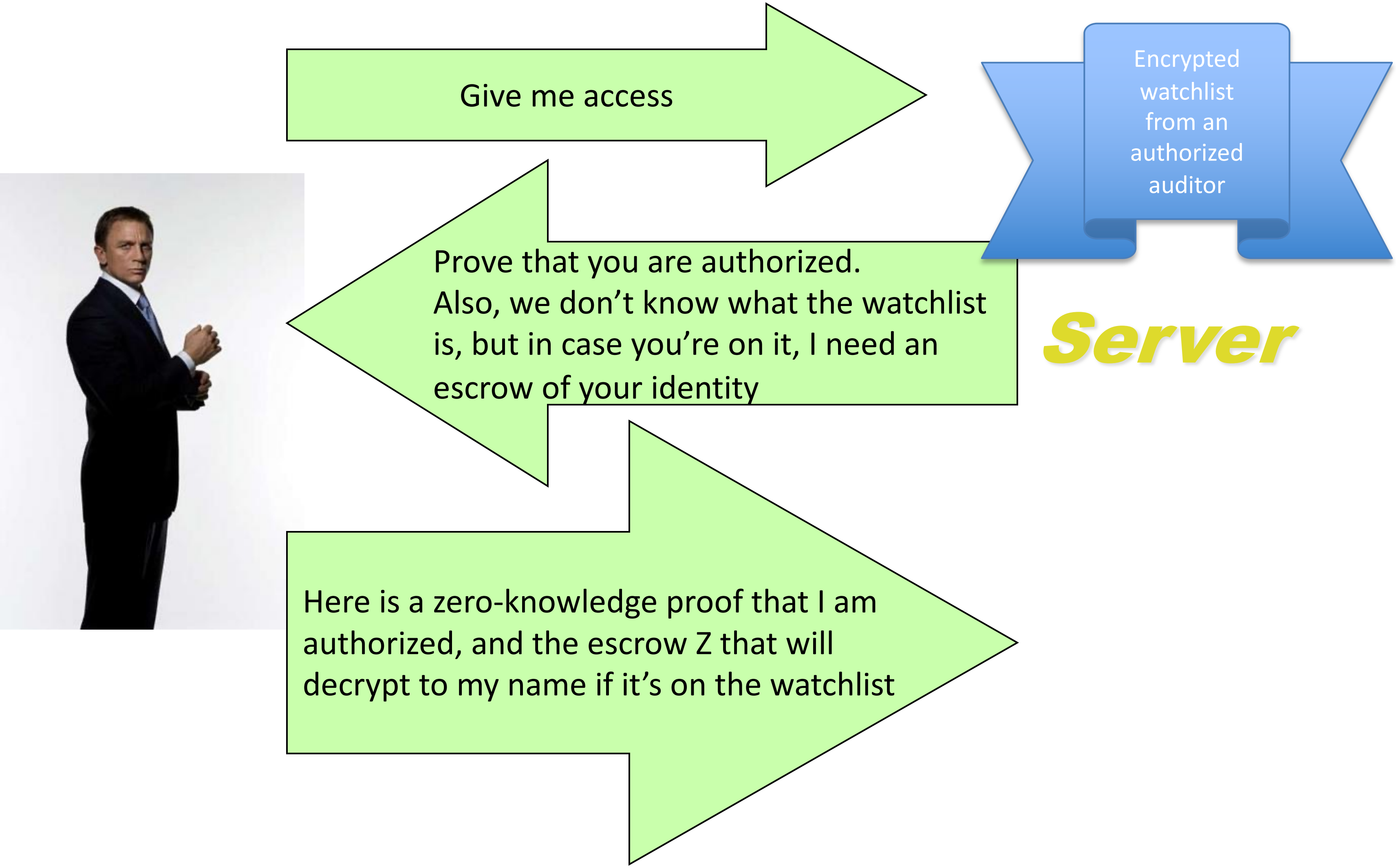
VerifySig$(pk,(x,id),\sigma)$ = TRUE

and C encrypts id

50-Year Research Agenda

- How can you make sure a user is authorized if this user is anonymous?
  - Use anonymous credentials [Chaum85,…,CL01,…]
- What if an anonymous authorized user does something that's not allowed?
  - Use conditional anonymity (anonymous ecash [CFN88], etokens [CHL05,CHKLM06,BCKL09]): identifying misbehaving users under well-defined conditions
- What if there is an emergency?
  - Use revocable anonymity (group signatures [CvH91] and variants)
- Can we secretly trace specific users/users that match a specific secret blueprint?
  - Use privacy-preserving blueprints [KLN22]
- Can anonymous credentials be anonymously delegated?
  - Yes [CL06,BCKLS08,CKLM14]
  - Mercurial signatures [CL19,CL21,CLP22,MSBN22]

Privacy-Preserving Blueprint [KLN22]



Give me access

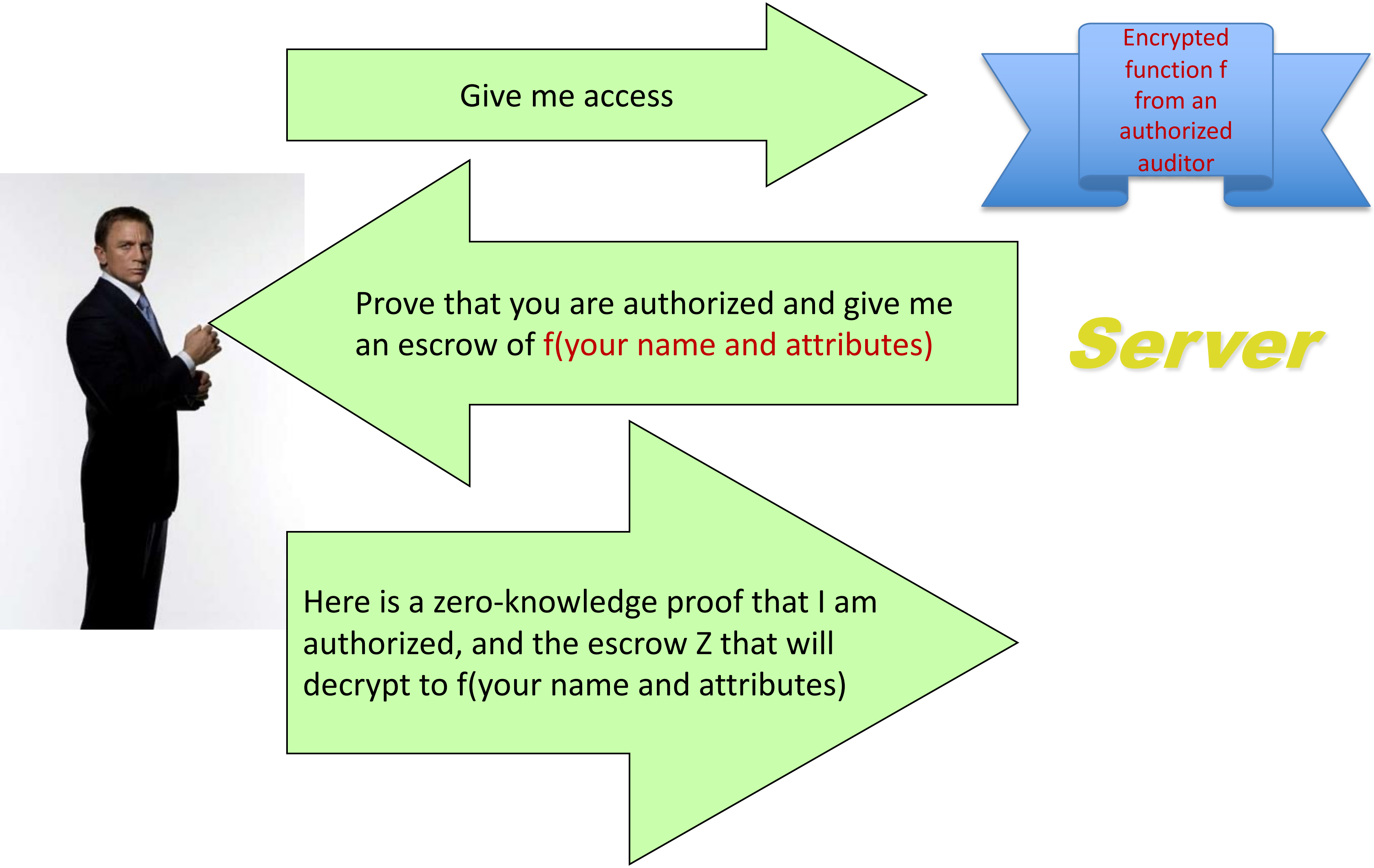
Encrypted watchlist from an authorized auditor

Prove that you are authorized.
Also, we don’t know what the watchlist is, but in case you’re on it, I need an escrow of your identity

Server

Here is a zero-knowledge proof that I am authorized, and the escrow Z that will decrypt to my name if it’s on the watchlist

Privacy-Preserving Blueprint [KLN22]



Give me access

Encrypted function f from an authorized auditor

Prove that you are authorized and give me an escrow of f(your name and attributes)

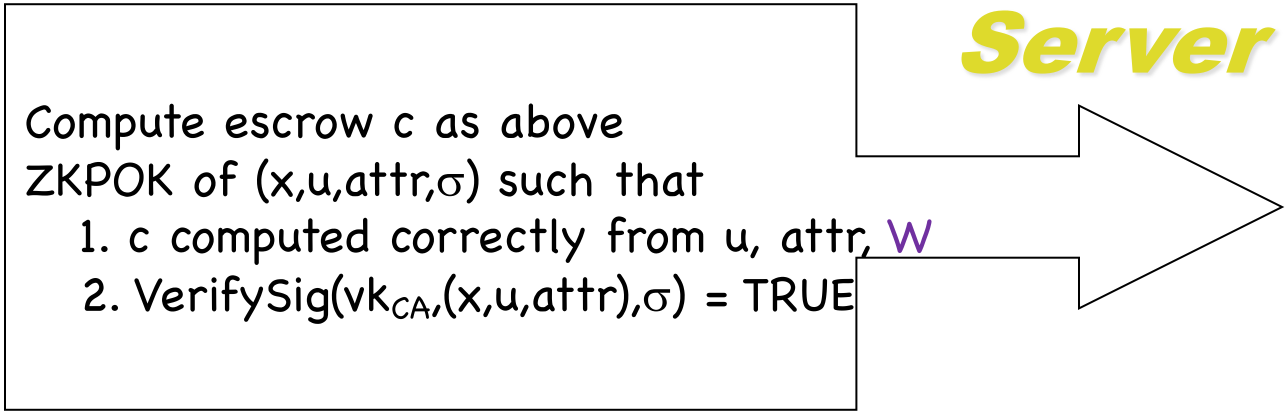
Server

Here is a zero-knowledge proof that I am authorized, and the escrow Z that will decrypt to f(your name and attributes)

Special case: watchlists [KLN22]

- Setup: same as anonymous credentials
- Auditor's setup:
  - Input: secret watchlist consisting of individuals (u_1, …, u_n) (think of as elements of Z_q)
  - Let $p(x)$ be a polynomial such that $p(u_i) = 0$, $a_0,\ldots,a_n$ are its coefficients
  - Compute an ElGamal encryption key pair (pk,sk) (in G of order q)
  - Publish: $W = (pk, Enc(pk,g^{a0}), \ldots, Enc(pk,g^{an}))$, encrypted coefficients of $p(x)$

- Escrowing user's attributes: if u on the watchlist, auditor wants attr
  - Recall: ElGamal is multiplicatively homomorphic:
    from $c_a = Enc(pk,a)$ and $c_b = Enc(pk,b)$ can compute $Enc(pk,ab) = c_a \boxtimes c_b$
  - From W, u can compute $c_{Eval} = Enc(pk,g^{p(u)})$
  - Next, compute a mask ciphertext $c_{Mask} = (c_{Eval})^r$
  - Next, compute the escrow $c = c_{Mask} \boxtimes Enc(pk,attr)$

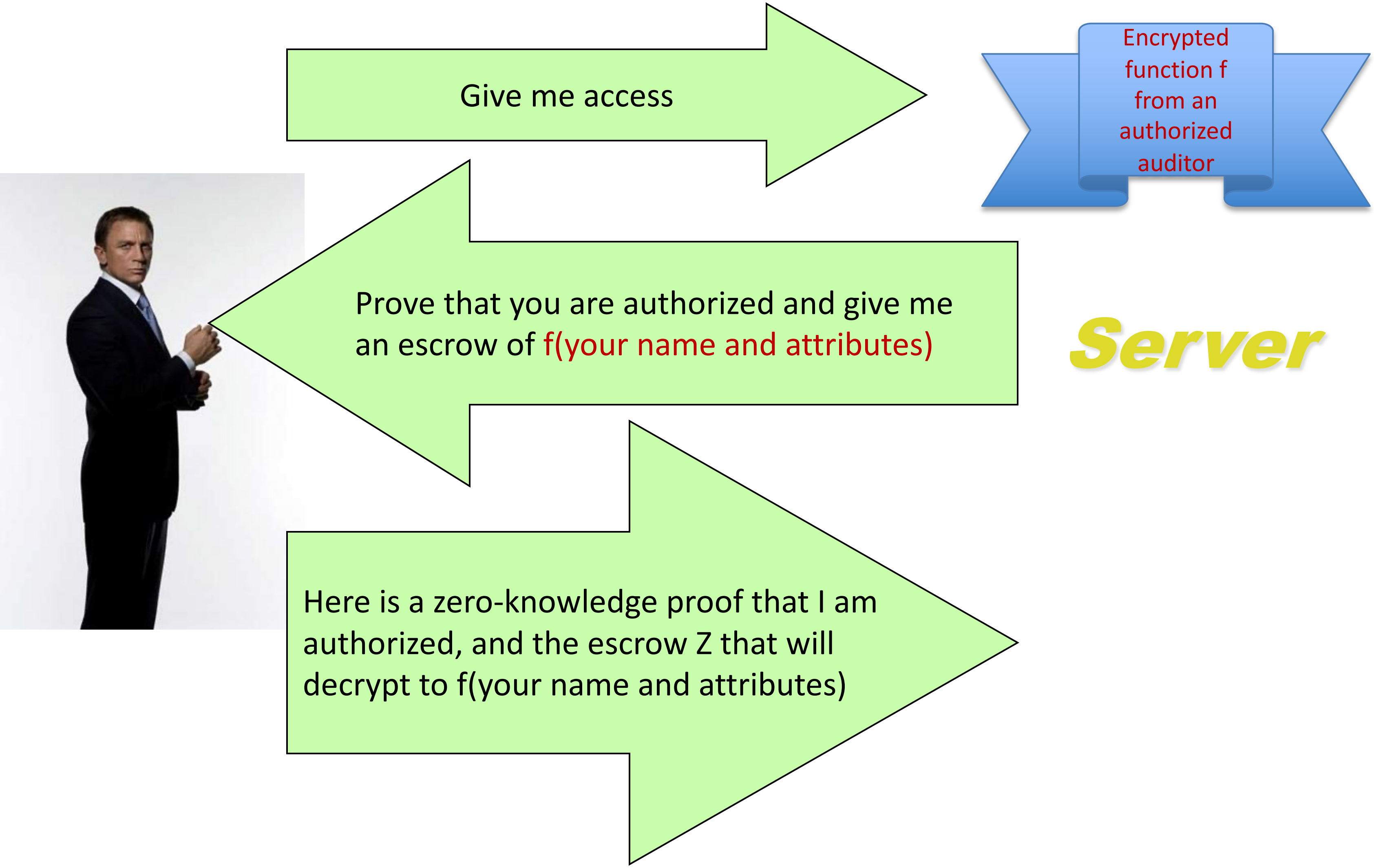


Compute escrow c as above

ZKPOK of $(x,u,attr,\sigma)$ such that

1. c computed correctly from u, attr, W
2. $VerifySig(vk_{CA},(x,u,attr),\sigma) = TRUE$

Privacy-Preserving Blueprint [KLN22]



Give me access

Encrypted function f from an authorized auditor

Prove that you are authorized and give me an escrow of f(your name and attributes)

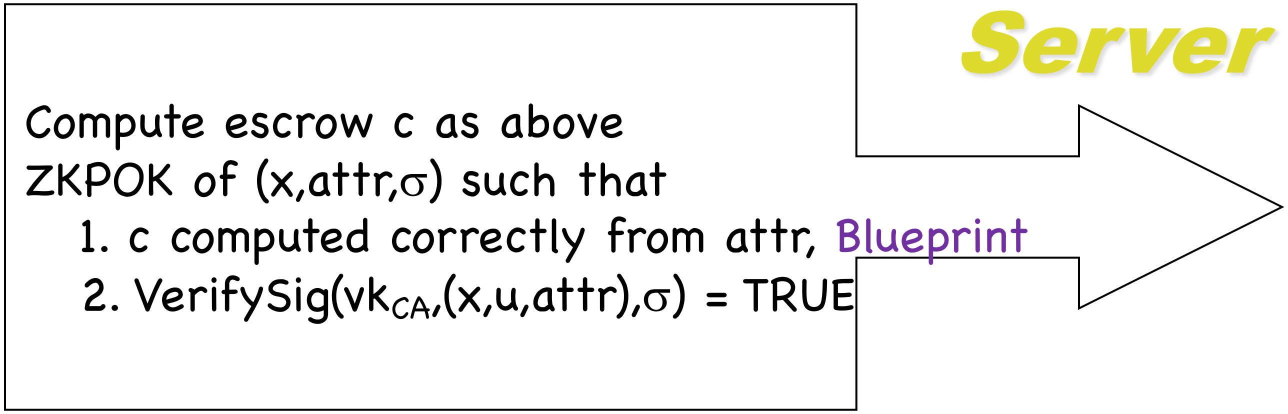
Server

Here is a zero-knowledge proof that I am authorized, and the escrow Z that will decrypt to f(your name and attributes)

The General Case [KLN22]

- Setup: same as anonymous credentials
- Auditor's setup:
  - Input: function f
  - Compute (pk,sk) for a homomorphic cryptosystem (needs to be homomorphic enough)
  - Publish Blueprint = (pk,Enc(pk,f))

- Escrowing user's attributes y: auditor wants f(attr)
  - From Blueprint and attr, compute c = Enc(pk,f(attr))
  - Important that the cryptosystem guarantee that c hides everything else about attr



Server

Compute escrow c as above
ZKPOK of $(x,attr,\sigma)$ such that
1. c computed correctly from attr, Blueprint
2. $VerifySig(vk_{CA},(x,u,attr),\sigma)$ = TRUE

50-Year Research Agenda

- How can you make sure a user is authorized if this user is anonymous?
  - Use anonymous credentials [Chaum85,…,CL01,…]
- What if an anonymous authorized user does something that's not allowed?
  - Use conditional anonymity (anonymous ecash [CFN88], etokens [CHL05,CHKLM06,BCKL09]): identifying misbehaving users under well-defined conditions
- What if there is an emergency?
  - Use revocable anonymity (group signatures [CvH91] and variants)
- Can we secretly trace specific users/users that match a specific secret blueprint?
  - Use privacy-preserving blueprints [KLN22]
- Can anonymous credentials be anonymously delegated?
  - Yes [CL06,BCKLS08,CKLM14]
  - Mercurial signatures [CL19,CL21,CLP22,MSBN22]

Summary

- No contradiction between anonymity and accountability! 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,...]
  - privacy-preserving blueprints [KLN22]
  - delegatable anonymous credentials [BCCKLS09,...,CL20]
- Policy and tech communities pursuing this
  - Gov't: GDPR, NSTIC
  - Tech giants: TCG, IBM, Microsoft, Google, Apple
  - Tech community – self-sovereign identity push