IRMA: I Reveal My Attributes

Privacy and Attribute-Based Identity Management

Gergely Alpár
Institute for Computing and Information Sciences
Radboud University
2016. augusztus 3.

Currently we are here...

Privacy and IRMA

Idemix Crypto

Three wars affecting privacy

Timeline of privacy regulation

1948 Universal Declaration of Human Rights (UDHR)

1953 European Convention on Human Rights (ECHR)

1959 European Court of Human Rights (ECtHR)

1980 OECD's recommendations: Principles on privacy and personal data

1985 Convention 108 (Protection of Individuals with regard to Automatic Processing of Personal Data)

1995 Data Protection Directive (Directive 95/46/EC)

2000 Safe Harbour agreement (Privacy Principles)

2012– General Data Protection Regulation (under construction)

2013 Snowden revelations

2015 Safe Harbour invalidated by the European Court of Justice

2016 EU-U.S. Privacy Shield

Various aspects of privacy

Differences between EU and US →

- EU: Privacy is a fundamental right
- US: Privacy requires others to refrain from infringements
  - Legally based on reasonable expectation of privacy: *e.g.* it does not exist when you voluntarily give information to third parties, like banks, ISPs, *etc.* ("third party doctrine")
  - Hence the US government can claim such data without warrant

Privacy versus data protection (in EU) →

- Privacy: Right for citizens
- Data protection: Right for data controllers, *i.e.*, if they stick to certain rules, then they can process data

Clouds

But what is “cloud”?

Underlying problems

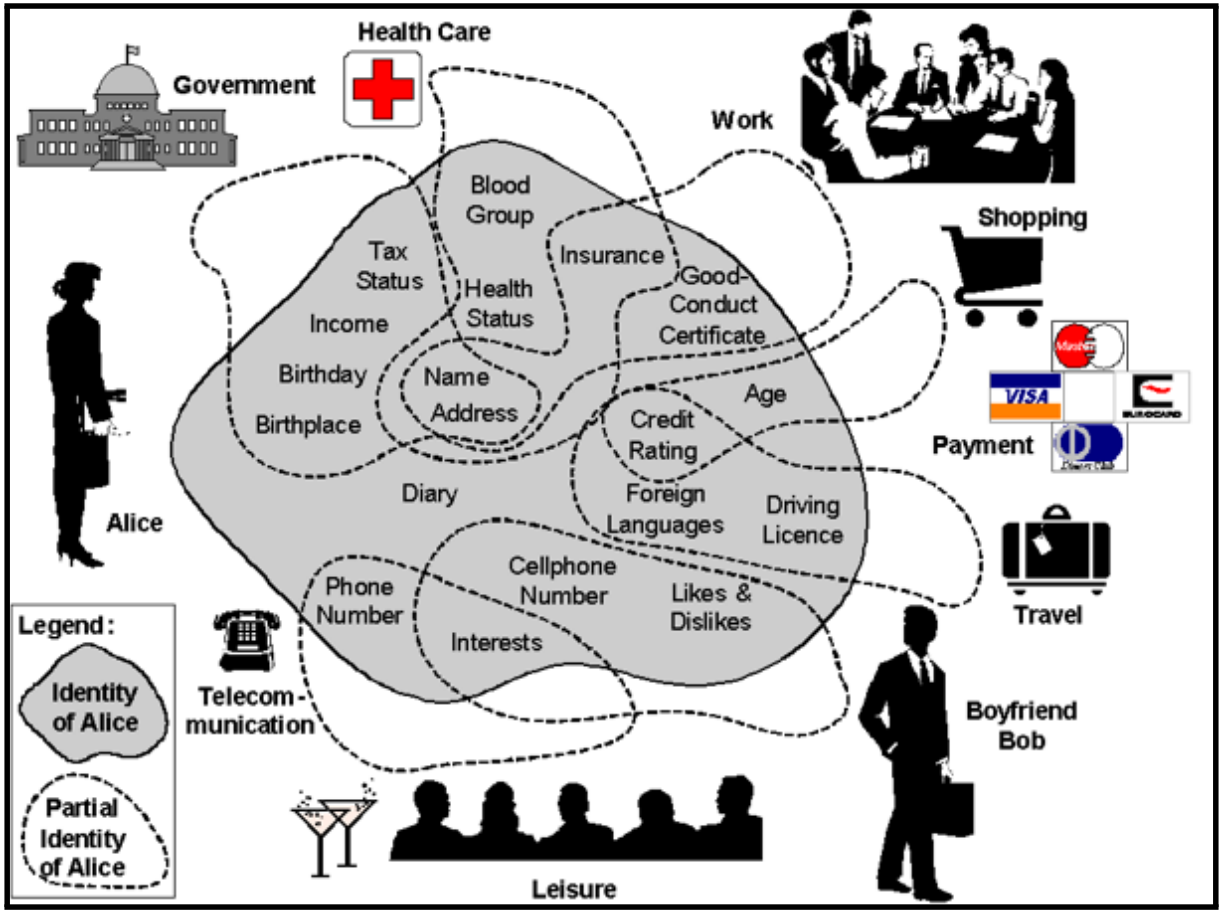
Centralisation

- Storage
- Processing
- Communication
- (Power)

Identification

- Unique in a scope
- Users often identifiable universally
- Secondary use, data aggreagation
- (At multiple layers)

Identity and Attributes



[Source: FIDIS]

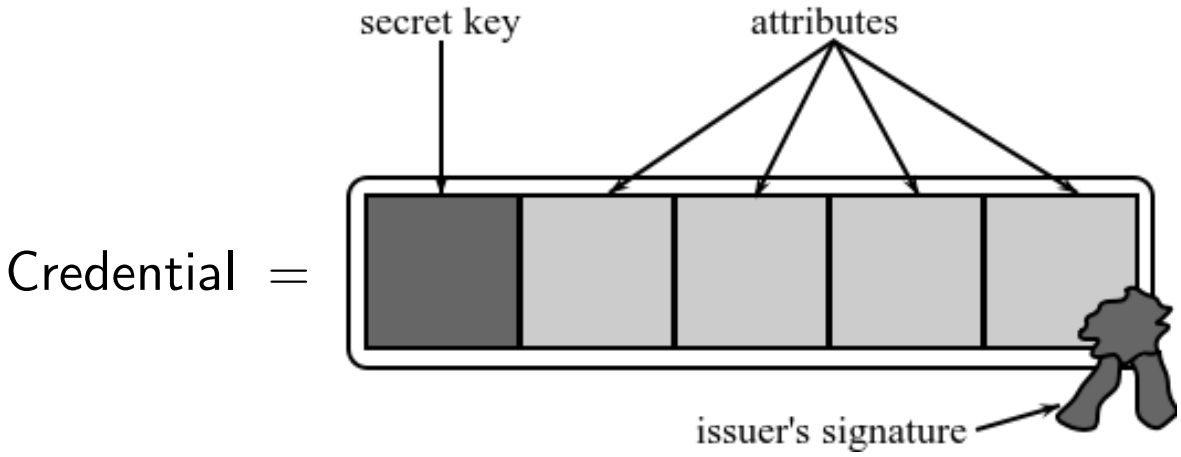
Possible Solution

- Problem: centralisation, identification
- Solution: User-managed attributes
  - Identifier
  - Personal data items (e.g. date of birth)
  - Characteristic (e.g. gender, brand)
  - Permission, role
  - Preference
- Attributes issued and revealed potentially independently
- Cryptographic technology: Attribute-based credentials
- Implementations possible on different carriers
  - Card
  - Phone
  - "Cloud(s)"

iCIS | Digital Security
Radboud University

Attribute-based credential

A user can have multiple credentials, each with multiple attributes:



- The secret key is securely stored, making credentials non-transferable
- The issuer's signature guarantees authenticity and integrity
- Any subset of the attributes can be shown in transactions.
  This is called selective disclosure.
  - The rest is hidden by zero-knowledge proofs

Smart-card implementation and IRMA

- First efficient smart-card implementation[1]
- IRMA project: privacy by design

Front

Back

- Card provision
- Issuing (authentic) attributes
- Authentication = Revealing attributes

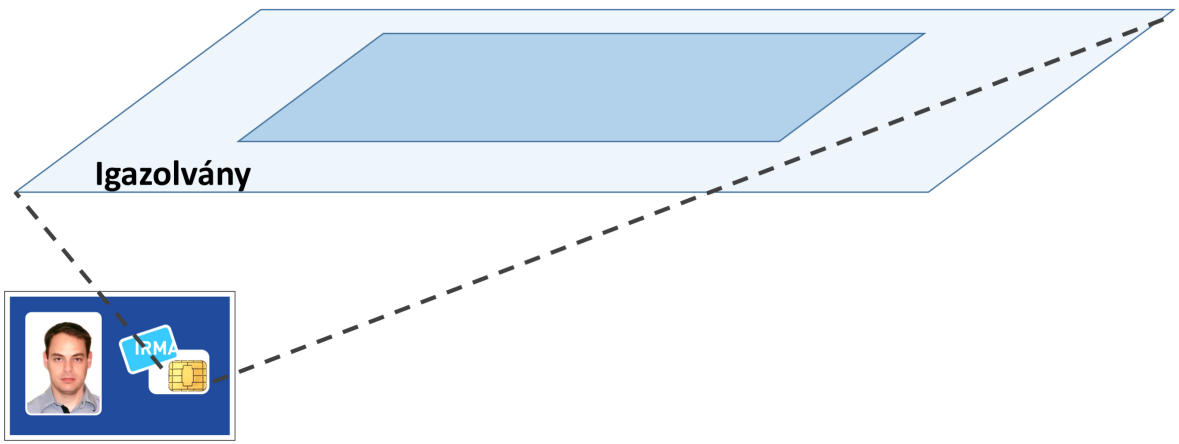
[1] P. Vullers and G. Alpár. "Efficient Selective Disclosure on Smart Cards Using Idemix". In: *IDMAN*. Springer, 2013, pp. 53–67.

IRMATube – demonstration

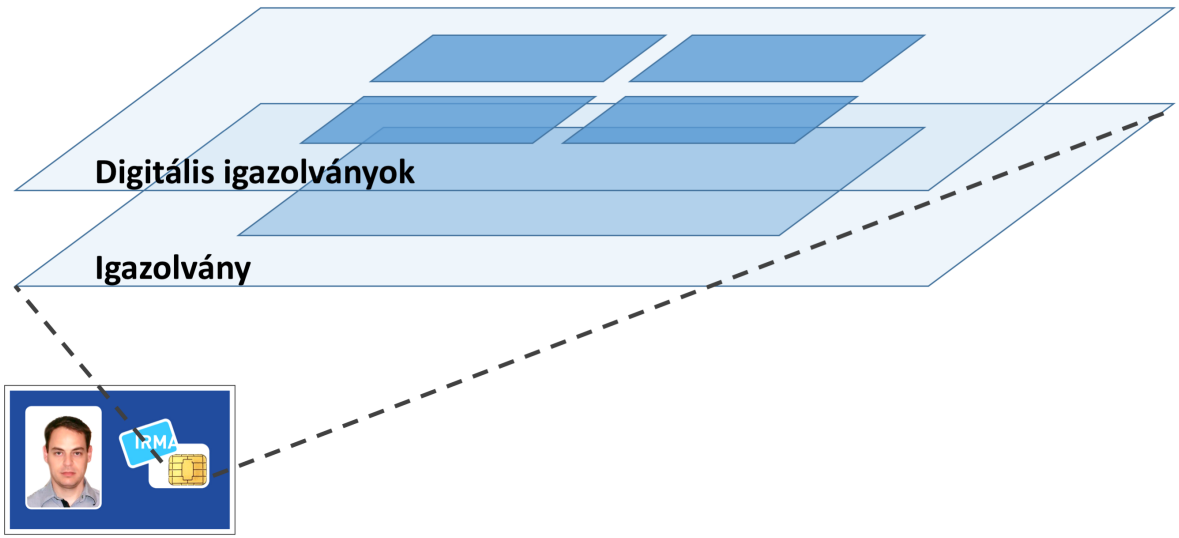
- To make IRMA even more user friendly, we created an Android app for attribute-based authentication: IRMA Phone.
- Privacy-friendly movie streaming
  - You reveal only the fact that you are a member of the service
  - . . . and possibly an over-age (*e.g.* ≥ 12) attribute

https://demo.irmacard.org

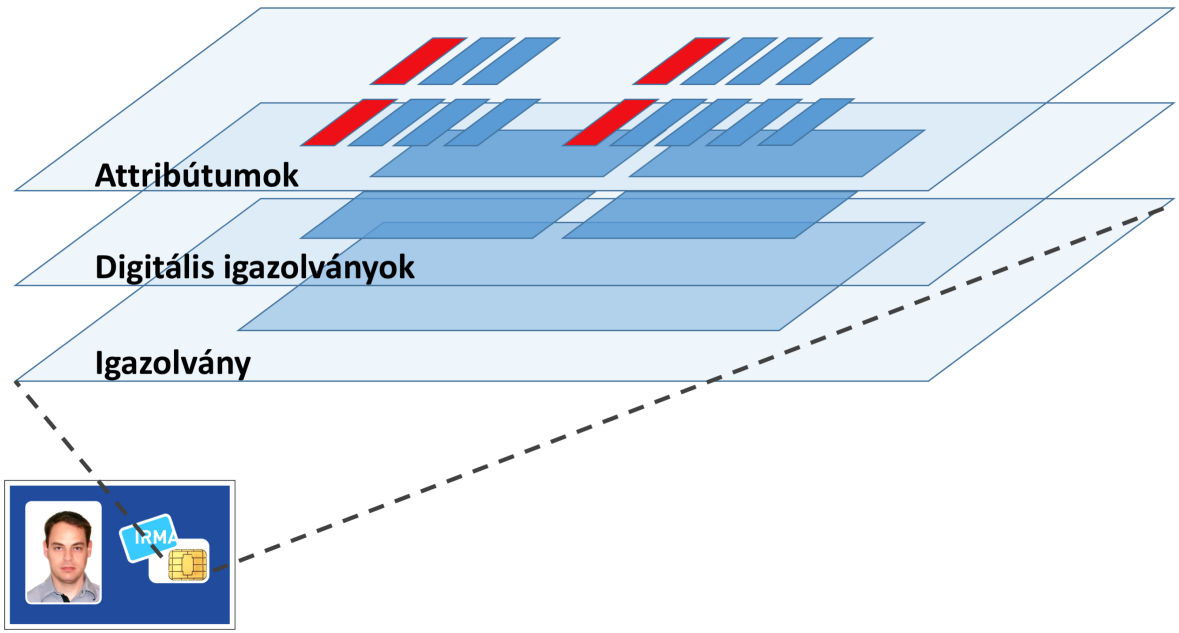
Carrier, Credentials and Attributes



Carrier, Credentials and Attributes

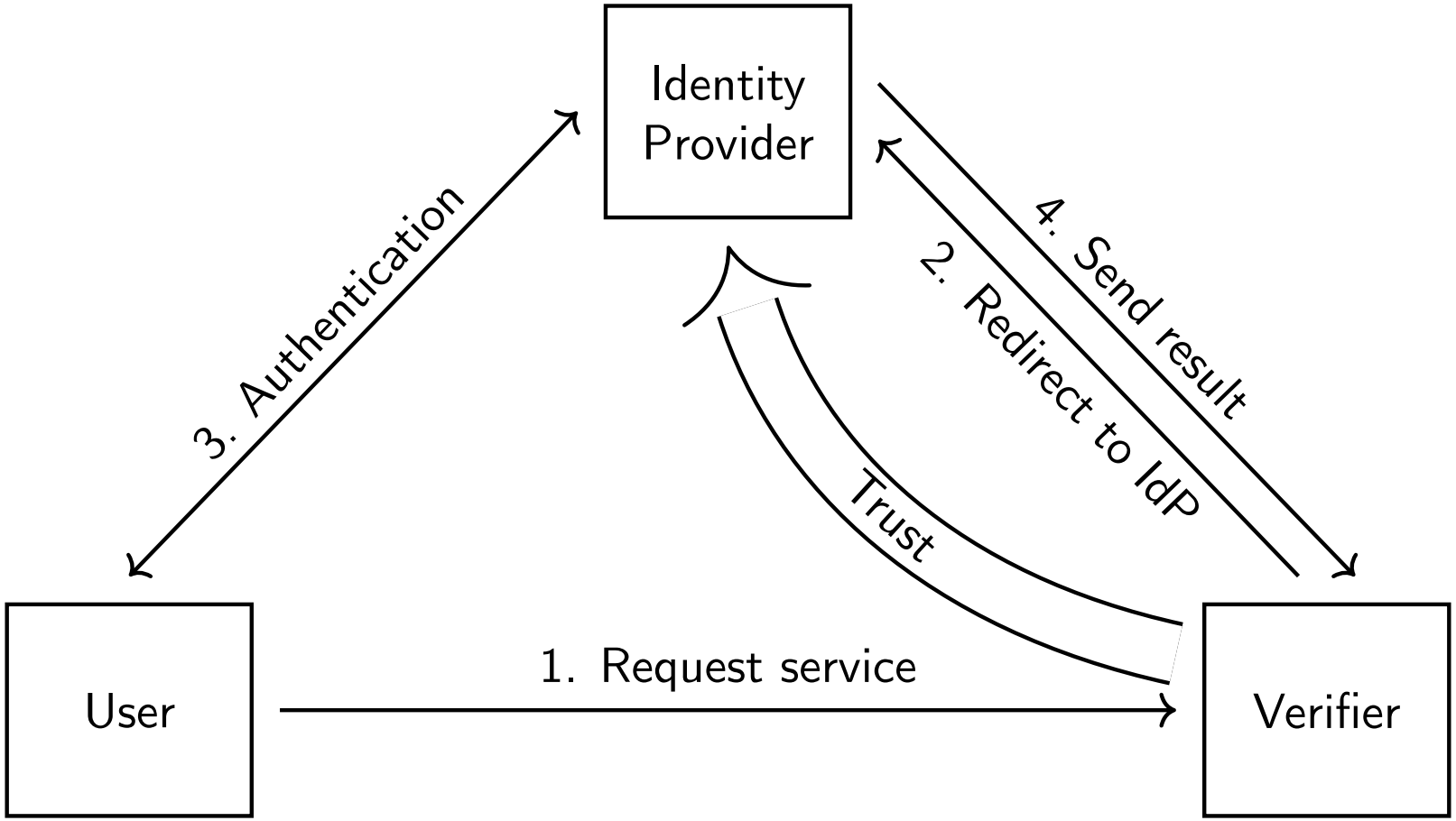


Carrier, Credentials and Attributes



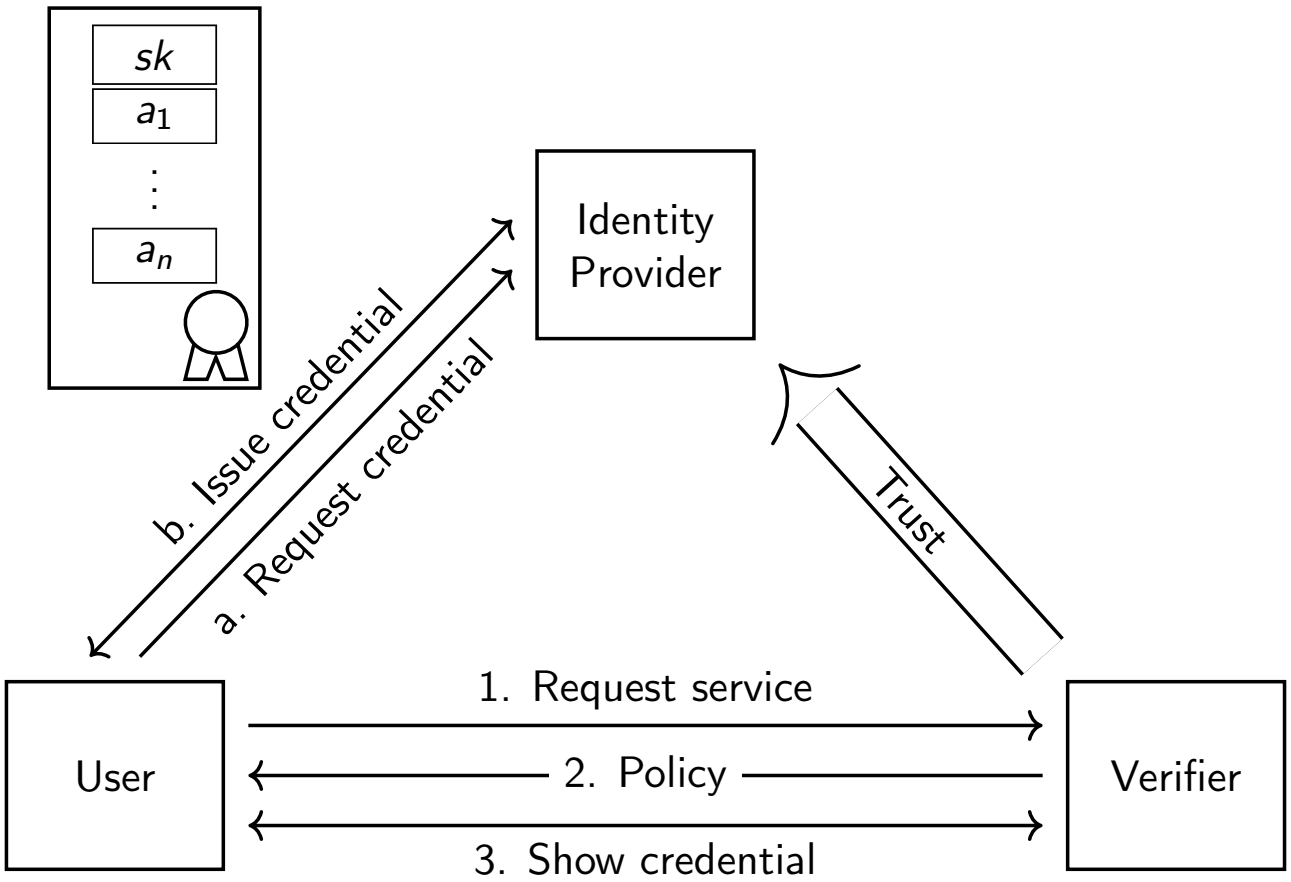
Traditional identity management

(by courtesy of W. Lueks)



Attribute-based credentials

(by courtesy of W. Lueks)



Strippenkaart vs OV-chipkaart

- The OV-chipkaart uses a unique identifier (even if it is anonymous), while a strippenkaart does not need this. Therefore, the usage of an OV-chipkaart is traceable.
- While there exists an anonymous OV-chipkaart, that is the 'unusual' or temporary solution. (Certain services mandate a non-anonymous, personal OV-chipkaart.) A strippenkaart is anonymous by default.
- Currently, the infrastructure is such that full anonymity is not an option. For instance, having an anonymous card as well as topping up with cash (that is, not with a personal bank card) is increasingly harder or impossible.

Currently we are here...

Privacy and IRMA

Idemix Crypto

A "Too Simple" Proof

- Let us work in $\mathbb{G}$ of order q
- Discrete logarithm: "I know the discrete logarithm $x = \log_g h$."

Prover Secret: x	$\mathbb{G}, g, q, h = g^x$	**Verifier**
	$\xrightarrow{x}$	$h \stackrel{?}{=} g^x$

- "Now you also know the discrete logarithm $\log_g h$." ☹

Schnorr's Proof of Knowledge [Schnorr 91]

- Let us work in $\mathbb{G}$ of order q
- Discrete logarithm: "I know the discrete logarithm $x = \log_g h$."
- $\mathrm{PK}\{\chi | h = g^{\chi}\}$—**P***roof of* **K***nowledge*
- Interactive

	Prover Secret: x	$\mathbb{G}, g, q, h = g^x$	**Verifier**
(1)	$w \in_R \mathbb{Z}_q$ $a := g^w$	$\xrightarrow{a}$	
(2)		$\xleftarrow{c}$	$c \in_R \{0,1\}$
(3)	$r := c \cdot x + w \pmod q$	$\xrightarrow{r}$	$a \stackrel{?}{=} g^r \cdot h^{-c}$

(1) Commitment
(2) Challenge
(3) Response

Simulated Communication

- Let us work in $\mathbb{G}$ of order q
- "I *seem to* know the discrete logarithm $\log_g h$." ☺
- Simulated conversation: transcript
- Choose $c \in_R \{0,1\}$, $r \in_R \mathbb{Z}_q^*$

$$a := g^r \cdot h^{-c}$$

Transcript and verification:

$$(a, c, r) \qquad a \stackrel{?}{=} g^r \cdot h^{-c}$$

iCIS | Digital Security
Radboud University

Schnorr's Proof of Knowledge [Schnorr 91]

- Let us work in $\mathbb{G}$ of order q
- Discrete logarithm: "I know the discrete logarithm $\log_g h$."
- $\mathrm{PK}\{\chi | h = g^{\chi}\}$—**P***roof of* **K***nowledge*
- Interactive

	Prover Secret: x	$\mathbb{G}, g, q, h = g^x$	**Verifier**
(1)	$w \in_R \mathbb{Z}_q$ $a := g^w$	$\xrightarrow{a}$	
(2)		$\xleftarrow{c}$	$c \in_R [0, 2^{128} - 1]$
(3)	$r := c \cdot x + w \pmod q$	$\xrightarrow{r}$	$a \stackrel{?}{=} g^r \cdot h^{-c}$

(1) Commitment
(2) Challenge
(3) Response

Schnorr Signature, *i.e.* Schnorr with Fiat–Shamir [FS 86]

- Discrete logarithm: "I know the discrete logarithm $\log_g h$."
- Non-interactive: $\mathrm{SPK}\{\chi | h = g^{\chi}\}(n)$
  - Challenge c is generated by a hash $\mathcal{H}$
  - $\mathcal{H} : \{0,1\}^* \to [0, 2^{128} - 1]$ (128-bit output)

Prover Secret: x	$\mathbb{G}, g, q, h = g^x, \mathcal{H}$	**Verifier**
	$\xleftarrow{n}$	$n \in_R \mathbb{Z}_q$
$w \in_R \mathbb{Z}_q$ $a := g^w$ $c := \mathcal{H}(a, n)$		
$r := c \cdot x + w \pmod q$	$\xrightarrow{a,r}$	$a \stackrel{?}{=} g^r \cdot h^{-\mathcal{H}(a,n)}$

How to Design ABCs? – In Three Simple Steps

Step 1 Take a commitment scheme

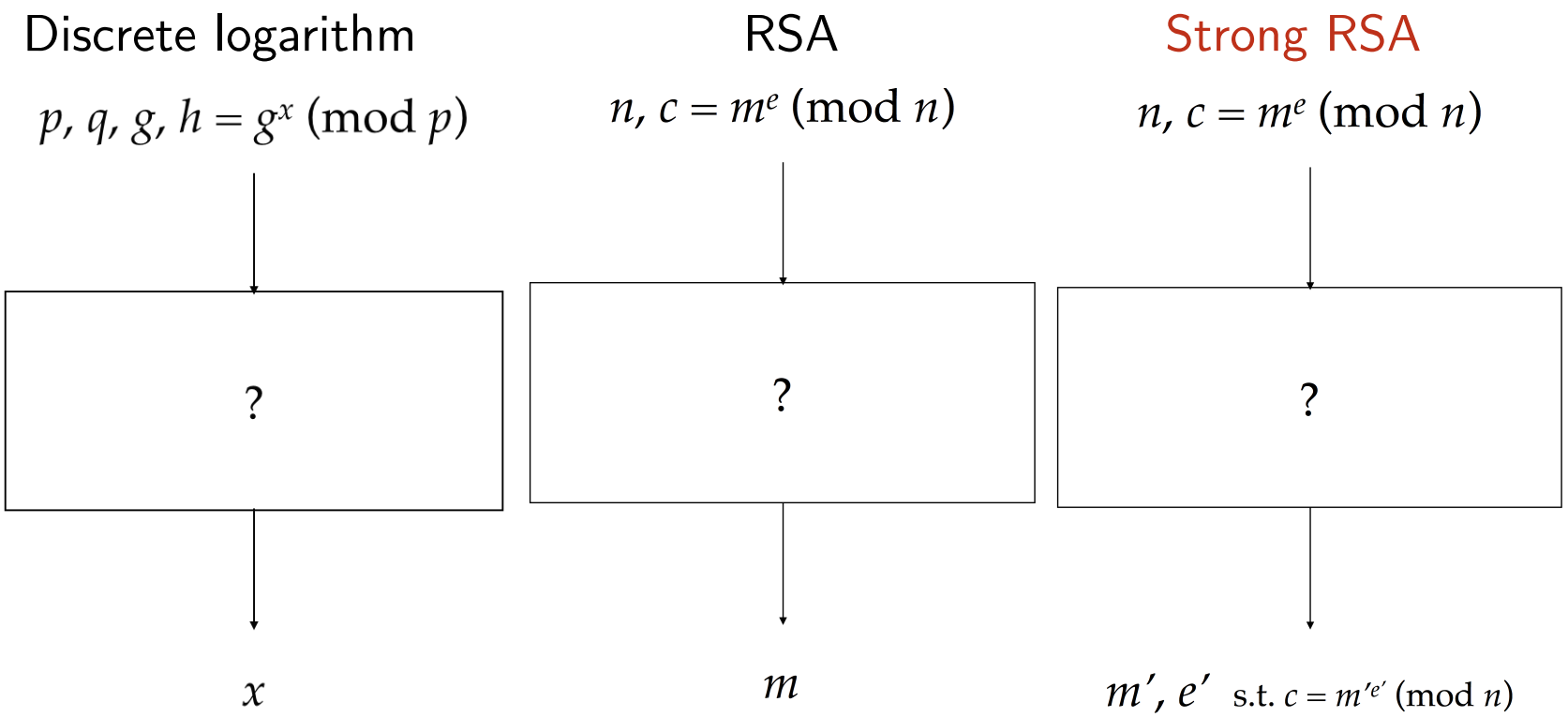
Step 2 Generalise it to multiple values

Step 3 Sign the extended commitment

Step +1 Apply here and there zero-knowledge proofs

Example: Idemix

Hard Problems



iCIS | Digital Security
Radboud University

Idemix ABC – Based on CL Signature

- Camenisch–Lysyanskaya (CL) signature [CL 01, CL 02]
- Strong RSA assumption [BP 97, FO 97]
  - **RSA** ($n = pq$) $\Longrightarrow$ Taking the eth root is hard
  - **Strong** $\Longrightarrow$ DL is hard
- Group QR_n:
  - p, q are safe primes ($p = 2p' + 1, q = 2q' + 1$ s.t. p', q' primes)
  - Quadratic residues in $\mathbb{Z}_n^*$
  - QR_n is a subgroup of order $\varphi(n)/4$
- Notation:
  - Some group elements that you'll see: $A, Z, S, R, R_1, R_2, R_3, \ldots$
  - Some further integers (exponents): $e, v, a, \ldots$

- Let's "design" Idemix's ABCs

iCIS | Digital Security
Radboud University

Step 1: Commitment

Take a commitment scheme – Pedersen on a_1

$$R^a \cdot R_1^{a_1} \text{ where } a \text{ is random.}$$

(mod n)

Step 2: Generalisation

Extend it to multiple values – generalise Pedersen on $(a_1, \ldots, a_L)$

$$R^a \cdot \underbrace{R_1^{a_1} \cdot \ldots \cdot R_L^{a_L}}_{\prod_{i=1}^{L} R_i^{a_i}}$$

where a is random.

iCIS | Digital Security
Radboud University

Step 3: Signature

Sign the extended commitment – CL on attributes: $a_1, \ldots, a_L$

$$A := \left(\qquad\qquad \right)^{1/e} \pmod{n}$$

Step 3: Signature

Sign the extended commitment – CL on attributes: $a_1, \ldots, a_L$

$$A := \left(\frac{Z}{S^v \cdot R^a \cdot \prod_{i=1}^{L} R_i^{a_i}} \right)^{1/e} \pmod{n}$$

where $(a), v, e$ are random.

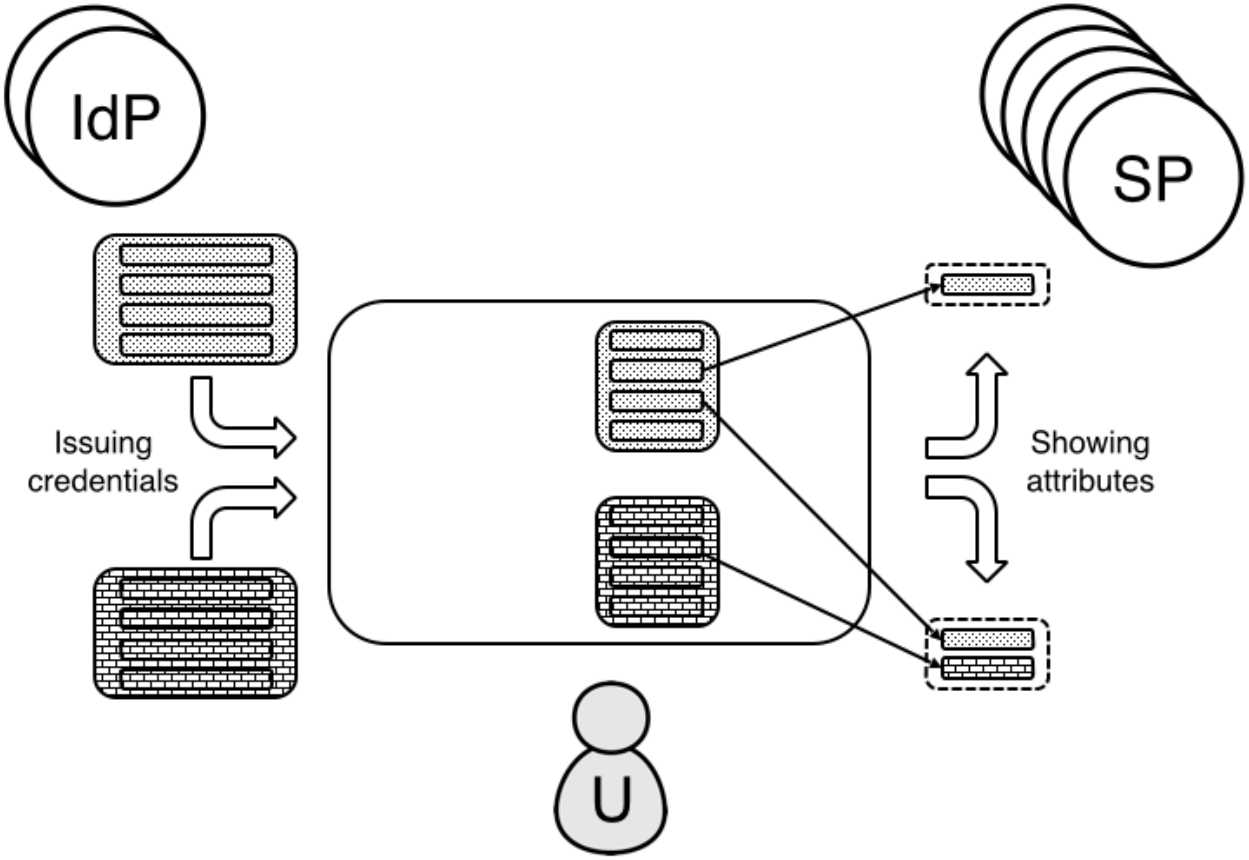
iCIS | Digital Security
Radboud University

CL Signature: Idemix ABCs

$$(A, e, v) \text{ where } A \equiv \left(\frac{Z}{S^v \cdot R^a \cdot \prod_{i=1}^{L} R_i^{a_i}} \right)^{1/e} \pmod{n}$$

- Commitment
  - Binding: computational (representation problem)
  - Hiding: perfect (randomised)
- CL Signature
  - Private key: p, q; Public key: $n = pq$, Z, S, "all Rs"
  - A bit like RSA: $(\cdot)^{1/e} \pmod{n}$
  - More complicated: advanced functions
- Issuing: blind signature (zero-knowledge proof)

Issuing and Showing



Idemix Showing: Authentication

Signature:

$$(A, e, v) \text{ where } A \equiv \left(\frac{Z}{S^v \cdot R^a \cdot \prod_{i=1}^{L} R_i^{a_i}} \right)^{1/e} \pmod{n}$$

- Public key: $n, Z, S, R, R_1, \ldots, R_L$
- Attributes (block of messages): $(a), a_1, \ldots, a_L$
- Verification:

$$Z \stackrel{?}{\equiv} A^e \cdot S^v \cdot \underbrace{R^a \cdot \prod_{i=1}^{L} R_i^{a_i}}_{R'} \pmod{n}$$

- IdP $\longrightarrow$ U; $\underline{\text{U} \longrightarrow \text{V}}$

iCIS | Digital Security
Radboud University

CL Signature Randomisation

Signature:

$$(A, e, v) \text{ where } A \equiv \left(\frac{Z}{S^v \cdot R'}\right)^{1/e} \pmod{n}$$

- Select random r
- $\overline{A} := A \cdot S^{-r} \pmod{n}$, $\overline{v} := v + er$

  (*Reminder:* The verification is $Z \stackrel{?}{\equiv} A^e \cdot S^v \cdot R' \pmod{n}$)
- Indeed, $(\overline{A}, e, \overline{v})$ is valid:

$$\overline{A}^e S^{\overline{v}} R' \equiv A^e S^{-er} S^v S^{er} R' \equiv A^e S^v R' \equiv Z \pmod{n}.$$

- Can we achieve untraceability with randomisation?

What about e?

How to hide e? – *i.e.* Multi-show Unlinkability

- Randomised signature: $(\overline{A}, e, \overline{v})$

$$\overline{A}^{e} S^{\overline{v}} \cdot R^{a} \cdot \prod_{i=1}^{L} R_i^{a_i} \equiv Z \pmod{n}.$$

- Representation problem is hard:

$$n;\ Z;\ (\overline{A}, S, R, R_1, \ldots, R_L) \xrightarrow{?} \text{“}(e, \overline{v}, a, a_1, \ldots, a_L)''$$

- So, to prove that she has a signature:
  - U gives $\overline{A}$ (*i.e.* a part of the randomised signature) and
  - U proves that she knows the exponents (*i.e.* a representation)

$$\mathrm{PK}\{(\varepsilon, \overline{\nu}, \alpha, \alpha_1, \ldots, \alpha_L) : Z \equiv \overline{A}^{\varepsilon} S^{\overline{\nu}} R^{\alpha} \prod_{i=1}^{L} R_i^{\alpha_i} \pmod{n}\}.$$

But then selective disclosure is easy!

Selective disclosure

- Zero-knowledge proof about all exponents:

$$\mathrm{PK}\{(\varepsilon, \overline{\nu}, \alpha, \alpha_1, \ldots, \alpha_L) : Z \equiv \overline{A}^{\varepsilon} S^{\overline{\nu}} R^{\alpha} \prod_{i=1}^{L} R_i^{\alpha_i} \pmod{n}\}.$$

- Disclose some and prove the rest; *e.g.*:
  U $\longrightarrow$ V disclose a_1, a_2 and prove:

$$\mathrm{PK}\{(\varepsilon, \overline{\nu}, \alpha, \alpha_3, \ldots, \alpha_L) : Z \cdot R_1^{-a_1} \cdot R_2^{-a_2} \equiv \overline{A}^{\varepsilon} S^{\overline{\nu}} R^{\alpha} \prod_{i=3}^{L} R_i^{\alpha_i} \pmod{n}\}.$$

iCIS | Digital Security
Radboud University

In Sum: ABCs are Powerful!

- Security
  - Authenticity
  - Integrity
  - Non-transferability
- Privacy
  - Issuer unlinkability
  - Multi-show unlinkability
  - Selective disclosure (data minimisation)
- Techniques and their smart-card implementations
  - IBM's Idemix [CL 01, CL 02] $\rightarrow$ [VA 13]
  - Microsoft's U-Prove [Brands 99] $\rightarrow$ [MV 12]
  - Anonymous Credentials Light [BL 13] $\rightarrow$ [HRP 15]

Conclusions

- Privacy is deeply embedded in culture and society
  - Governments and intelligence services
  - Business interests
  - War and terrorism
  - Globalisation
- Currently, identity management is *privacy-unfriendly* and diverse
  - Centralised and identifying
  - Not interoperable
  - Traceable (mostly for many parties)
- Attribute-based credentials (and IRMA) provide a new approach
  - User centred
  - Privacy and flexibility in authentication
  - Many open questions (good carriers, interoperability, business models, etc.)

THANK YOU!