The Alphabet of ABCs

OUrsi

Greg Alpár

greg.alpar@ou.nl

Open Universiteit & Radboud University

April 4, 2017

Open Universiteit
www.ou.nl

Outline

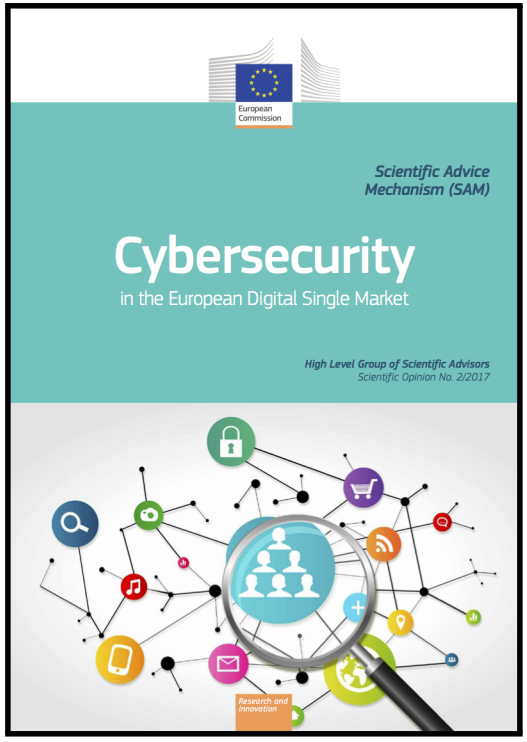
Motivation: Identity in the digital world

Attribute-based credentials and tricks

Ongoing and future work

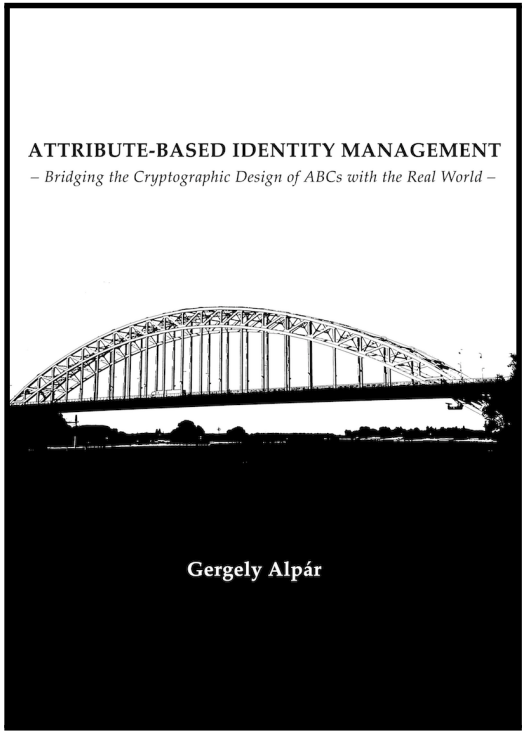
Open Universiteit
www.ou.nl

Attribute-based identity management



CONTEXTUAL IDENTITY

To respect privacy, promote the development and context-tailored use of attribute-based digital identity management.

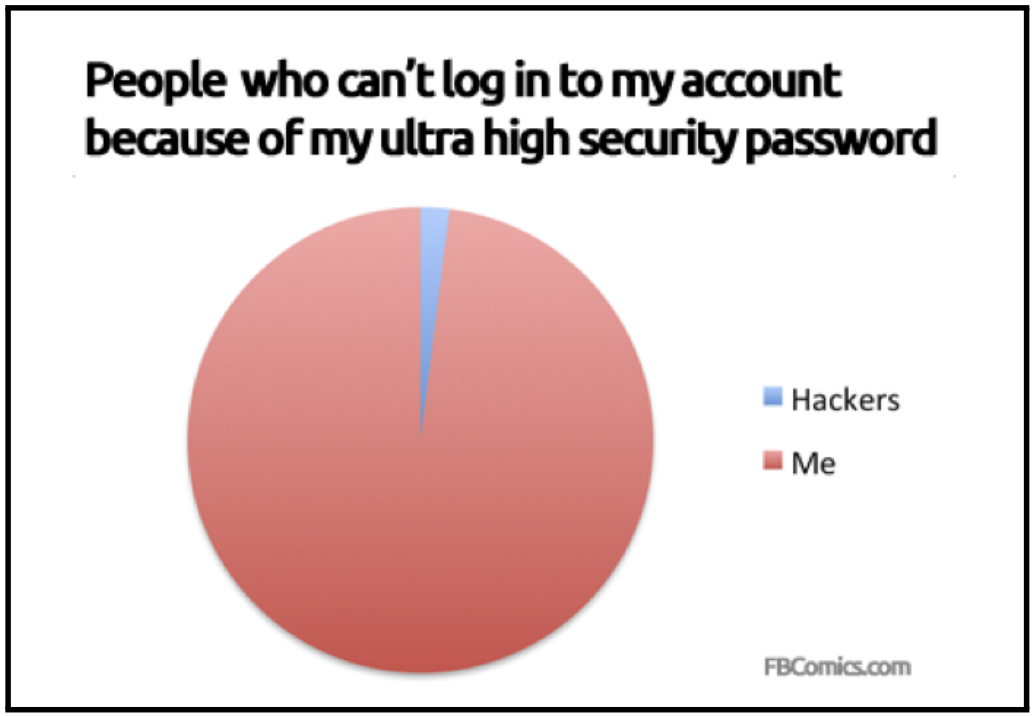


Open Universiteit
www.ou.nl

Motivation: Identity in the digital world

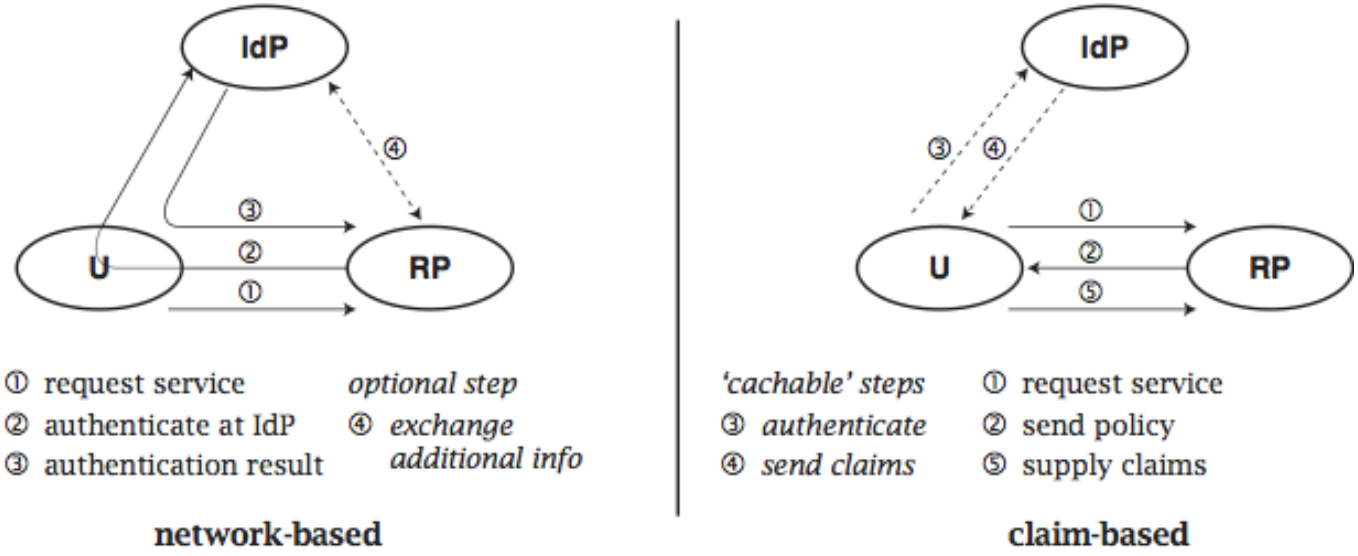
Users: security, privacy, usability

- Password is often not secure
- Authentication: always identifying
- Many types of authentication
- Mobile devices



Open Universiteit
www.ou.nl

Network-based and claim-based identity management



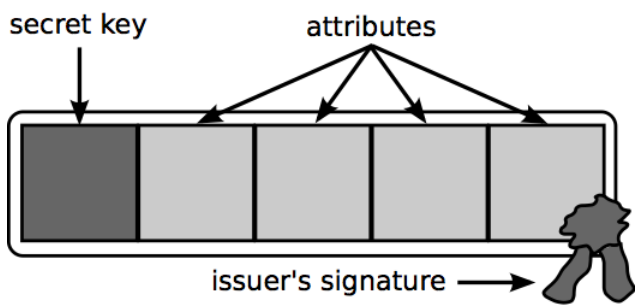
IRMA Demo (demo.irmacard.org):

- IRMATube
- ≥ 18
- name

Open Universiteit
www.ou.nl

Goals

- Independence between issuing and showing: time and protocol
- Privacy
- Credential: security for the system
  - Authenticity
  - Integrity
  - Non-transferability
- Credential: privacy for the user
  - Issuer unlinkability (blind signature, randomisation)
  - Multi-show unlinkability (randomisation, zero-knowledge proofs)
- Attribute-based credentials



Open Universiteit
www.ou.nl

Attribute-based credentials and tricks

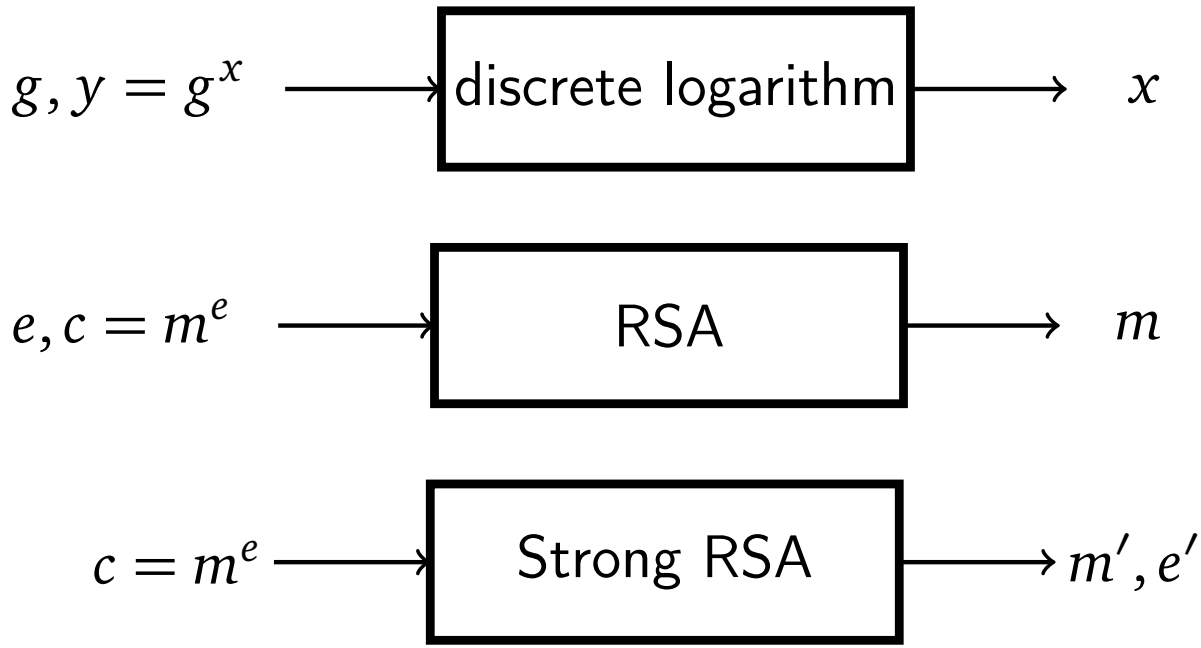
Recap: public-key cryptography

- Pair: public key, secret key
- Applications:
  - Encryption: message encryption to the recipient
    - *e.g.* RSA enc: $c = m^e \bmod n$, where $n = p \cdot q$
  - Signature: signature verification
    - *e.g.* RSA sig: $s = m^{1/e} \bmod n$
  - Authentication: proof of secret key
- Certificate on the public key (by CA/Issuer)
- Public-key infrastructure (PKI)
- Note: public key is an identifier
- Attribute certificate: $C_{\geq 18} = \text{Sign}(sk_{Auth}, \text{“Over 18”})$
- BUT, general privacy problems:
  - Issuer (authority) linkability
  - Multiple showing linkability

Open Universiteit
www.ou.nl

Hard problems, *i.e.* Assumptions

Typically, computational problems are defined in a large *finite* mathematical structure. (We omit the underlying structures here.)



Discrete logarithm – a toy example

The exponents of 23 modulo 29 (the order is $q = 7$):

0	1	2	3	4	5	6	7	...
1	23	7	16	20	25	24	1	...

$\mathrm{Dlog}_{23}\, 25 = 5$

Open Universiteit
www.ou.nl

A "too simple" proof of knowledge

How can public-key cryptography be used for authentication?

- Discrete logarithm: "I know the discrete logarithm $x = \mathrm{Dlog}_g h$."

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

- "Now you also know the discrete logarithm $\mathrm{Dlog}_g h$." ☹

A zero-knowledge proof [Schnorr 91]

- Discrete logarithm: "I know the discrete logarithm $x = \mathrm{Dlog}_g h$."
- $PK\{x|h = g^x\}$—**P***roof of* **K***nowledge*
- Interactive

	Prover Secret: x	$g, h = g^x$	**Verifier**
(1)	random w		
	$a := g^w$	$\xrightarrow{a}$	
(2)		$\xleftarrow{c}$	random c
(3)	$r := c \cdot x + w$	$\xrightarrow{r}$	$a \stackrel{?}{=} g^r \cdot h^{-c}$

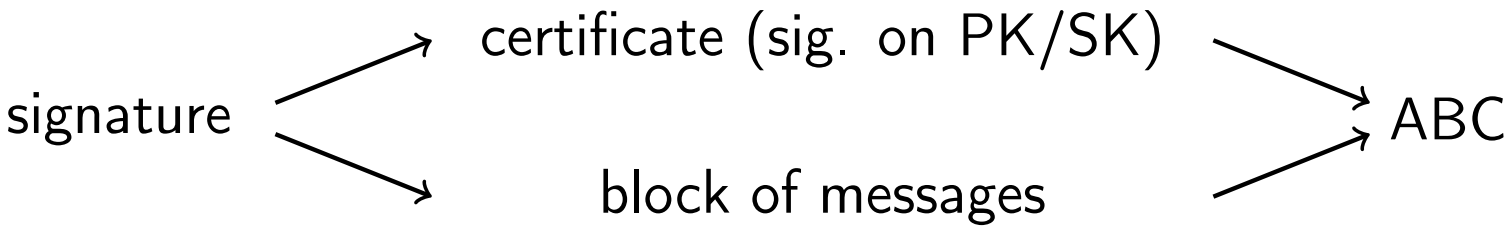
(1) Commitment

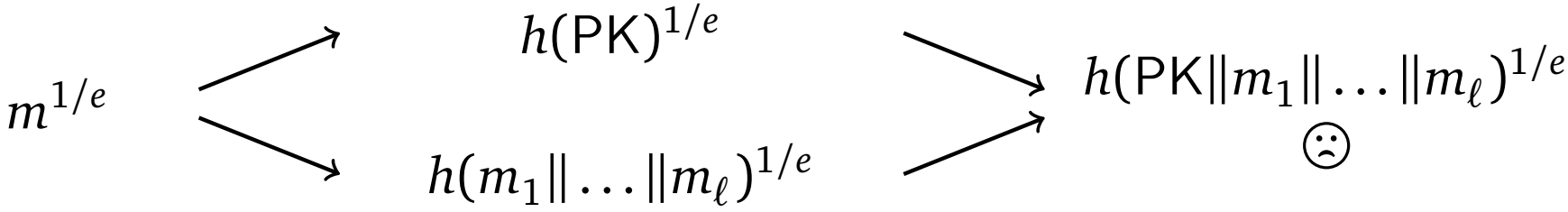
(2) Challenge

(3) Response

Open Universiteit
www.ou.nl

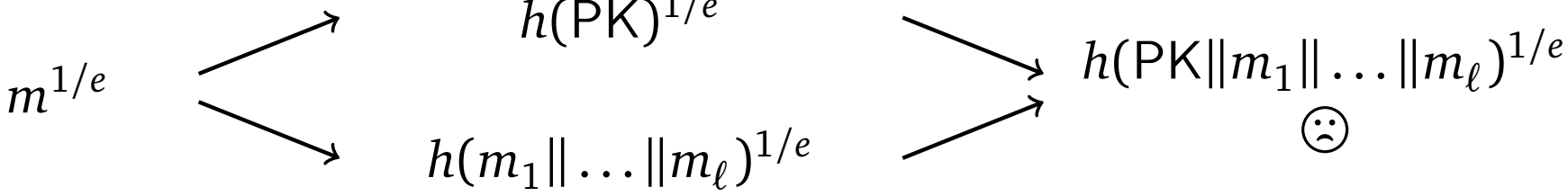
Attribute-based credential (ABC)



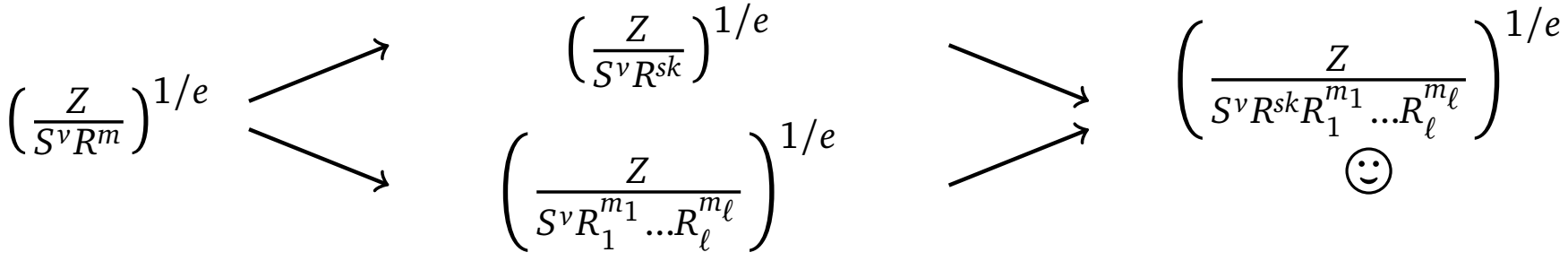


Problem: *e.g.* all message components have to be known to check the signature!

Attribute-based credential (ABC) – Attempt 2



Camenisch–Lysyanskaya signature: (A, e, v) on m : $A = \left(\frac{Z}{S^v R^m}\right)^{1/e}$
Assumptions: **Strong RSA**, **Representation**



Open Universiteit
www.ou.nl

CL Signature Randomisation

Signature (the public key is Z, S; "msg" is $R' = R^{sk} R_1^{m_1} \dots R_\ell^{m_\ell}$):

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

Verification: $Z \stackrel{?}{=} A^e \cdot S^v \cdot R'$

Randomisation:

- Select random r
- $\overline{A} := A \cdot S^{-r}$, $\overline{v} := v + er \Longrightarrow (\overline{A}, e, \overline{v})$ is a randomised signature.
- Indeed:
$$\overline{A}^e S^{\overline{v}} R' = A^e S^{-er} S^v S^{er} R' = A^e S^v R' = Z.$$
- Can we achieve untraceability with randomisation?

What about e?

Open Universiteit
www.ou.nl

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

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

$$\overline{A}^{e} S^{\overline{v}} R^{sk} R_1^{m_1} \ldots R_\ell^{m_\ell} = Z.$$

- Representation problem is hard:

$$Z;\ (\overline{A}, S, R, R_1, \ldots, R_\ell) \xrightarrow{?} \text{“}(e, \overline{v}, sk, m_1, \ldots, m_\ell)\text{”}$$

- 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)

$$PK\{(e, \overline{v}, sk, m_1, \ldots, m_\ell) : Z = \overline{A}^{e} S^{\overline{v}} R^{sk} R_1^{m_1} \ldots R_\ell^{m_\ell}\}.$$

But then selective disclosure is easy!

Selective disclosure

- Zero-knowledge proof about all exponents:

$$PK\{(e, \overline{v}, sk, m_1, m_2, m_3, \ldots, m_\ell) : Z = \overline{A}^e S^{\overline{v}} R^{sk} R_1^{m_1} R_2^{m_2} R_3^{m_3} \ldots R_\ell^{m_\ell}\}.$$

- Disclose some and prove the rest; *e.g.*:

U $\longrightarrow$ V disclose m_1, m_2 and prove:

Having m_1, m_2, V can compute $ZR_1^{-m_1} R_2^{-m_2}$. U proves:

$$PK\{(e, \overline{v}, sk, m_1, \ldots, m_\ell) : ZR_1^{-m_1} R_2^{-m_2} = \overline{A}^e S^{\overline{v}} R^{sk} R_3^{m_3} \ldots R_\ell^{m_\ell}\}.$$

Open Universiteit
www.ou.nl

Ongoing and future work

Recent research

1. Revocation: "How to revoke anonymous credentials?"
   - Epoch-based revocation (Lueks et al. *Fast Revocation of Attribute-Based Credentials for Both Users and Verifiers*, 2016): U's unique r value, $g_{ev} = \mathcal{H}(epoch||verifier)$
     - $g_0, h_0, xxxPK\{r, \ldots | h_0 = g_0^r \wedge ABC \ldots\}$
     - $g_1, h_1, PK\{r, \ldots | h_1 = g_1^r \wedge ABC \ldots\}$
2. Phone vs smart card: "a phone is convenient but not secure"
   - Secret sharing of the secret key between cloud and phone
   - Computation of proofs without recovering secret key
   - Implemented; however, yet to be written
3. RSA is old and big: "use elliptic-curve crypto (ECC)"
   - New scheme: Ringers et al. *An efficient self-blindable attribute-based credential scheme*, 2017
   - Implementation is on the way

Open Universiteit
www.ou.nl

Applications

1. Attribute-based signature (ABS): "An ABC proof as a signature" (Hampiholi et al. *Towards practical Attribute-Based Signatures*, 2015)
2. Airbnb: "A house also has an identity"
3. Internet of Things: "Control and minimise data collection wherever possible" (Alpár et al. *New Directions in IoT Privacy Using Attribute-Based Authentication*, 2016)
4. Webshop: "Why not minimise data at *every* transactions?"

Attribute-based identity management

$\longrightarrow$ **Attribute-based transactions**

Open Universiteit
www.ou.nl

Thank you

Open Universiteit
www.ou.nl