IRMA: Attribute-Based Identity Management Using Smart Cards

Summer School on Real-World Crypto and Privacy

Gergely Alpár
gergely@cs.ru.nl
June 4, 2015

iCIS | Digital Security
Radboud University

Currently we are here...

Security and Privacy Today

Attribute-based identity management

Crypto of ABCs

Smart-card implementation

IRMA: the best of ABCs

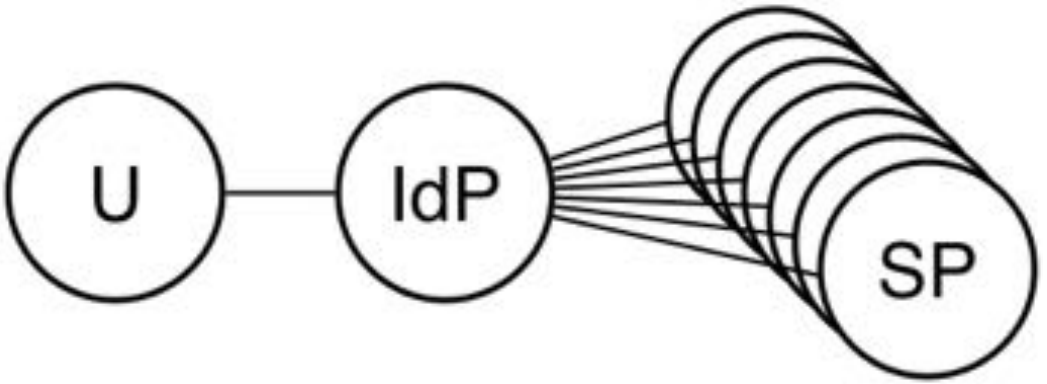
"[By 2025 f]ew individuals will have the energy, interest, or resources to protect themselves from *dataveillance*; privacy will become a *luxury*."

[Pew Research Center, December 2014]

Authentication

- Passwords
  - "38% of adults sometimes think it would be easier to solve world peace than attempt to remember all their passwords" [Harris Interactive, 2012]
- Many accounts at service providers
- Identity management
  - Users
  - Identity provider(s) = Issuer
  - Service providers = Relying party = Verifier

Problems with Identity Management



- Security
  - Single point of failure
  - Valuable target
- Privacy
  - Can log in (?)
  - Linking all user activities
  - Profiling

Authorisation is necessarily identifying

Outline

Security and Privacy Today

Attribute-based identity management

Crypto of ABCs

Smart-card implementation

IRMA: the best of ABCs

Currently we are here...

Security and Privacy Today

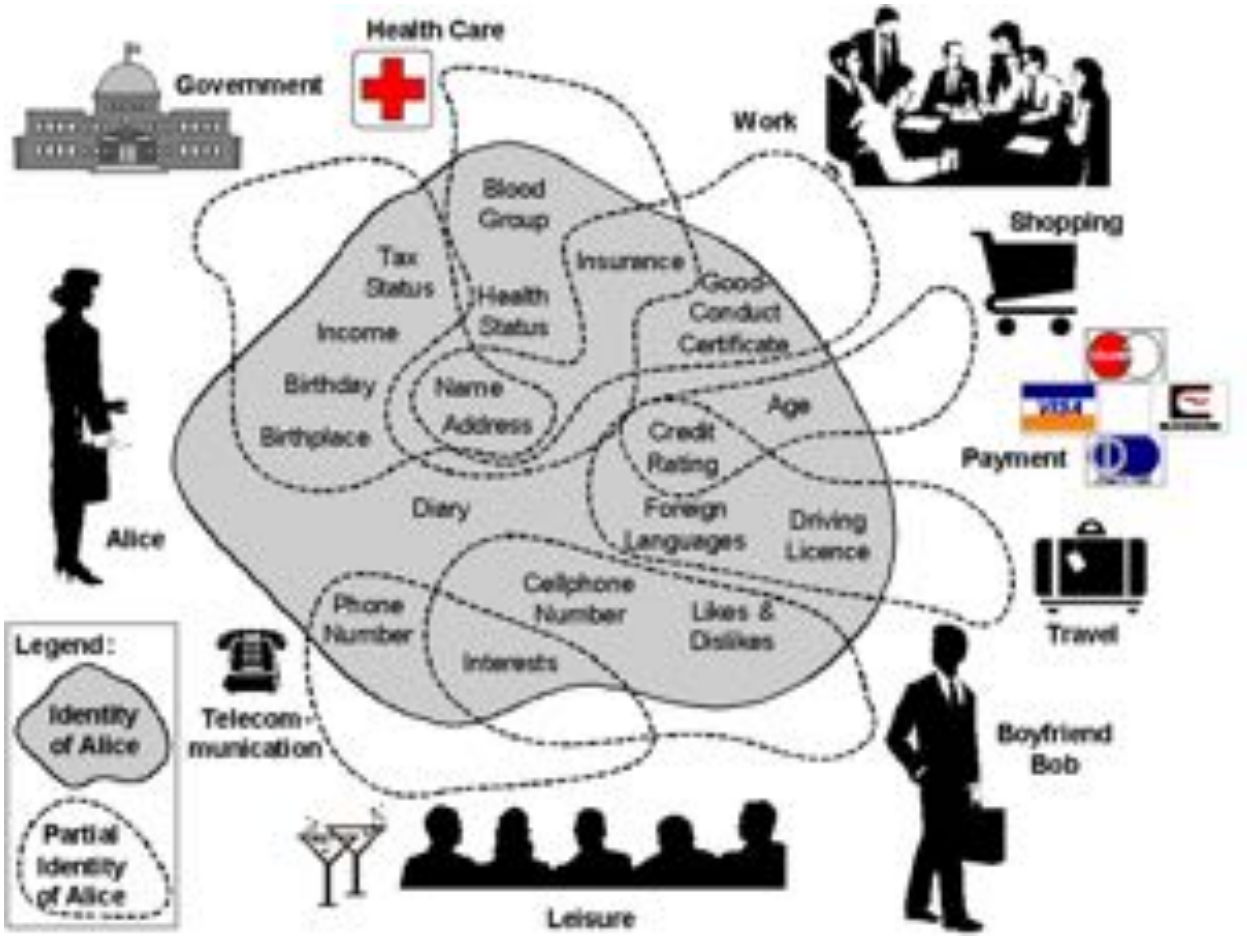
Attribute-based identity management

Crypto of ABCs

Smart-card implementation

IRMA: the best of ABCs

Identity and Attributes



[FIDIS 2005]

Digital Identity

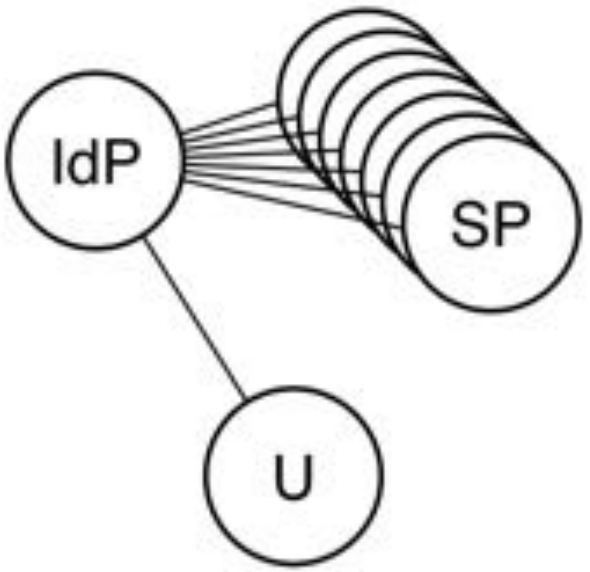
- Attributes
- Partial identities

- Identifying and non-identifying attributes

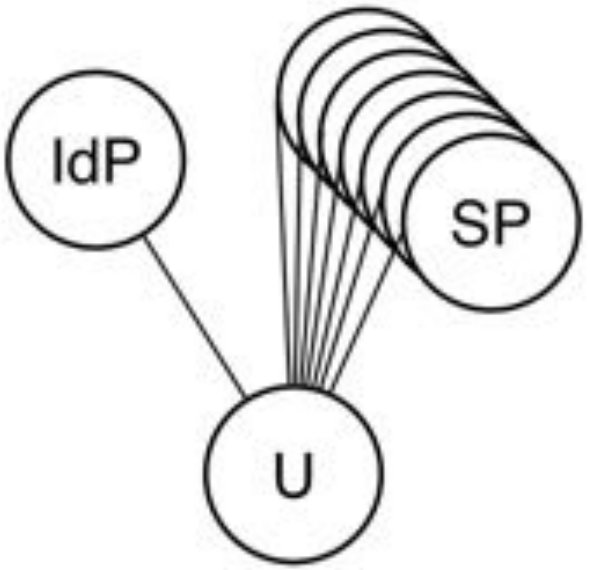
- Username + authentication + lookup

- Authorisation based on attributes
  - Directly looking up relevant attributes
  - Identifying and non-identifying authorisation (DEMO: ≥ 18)

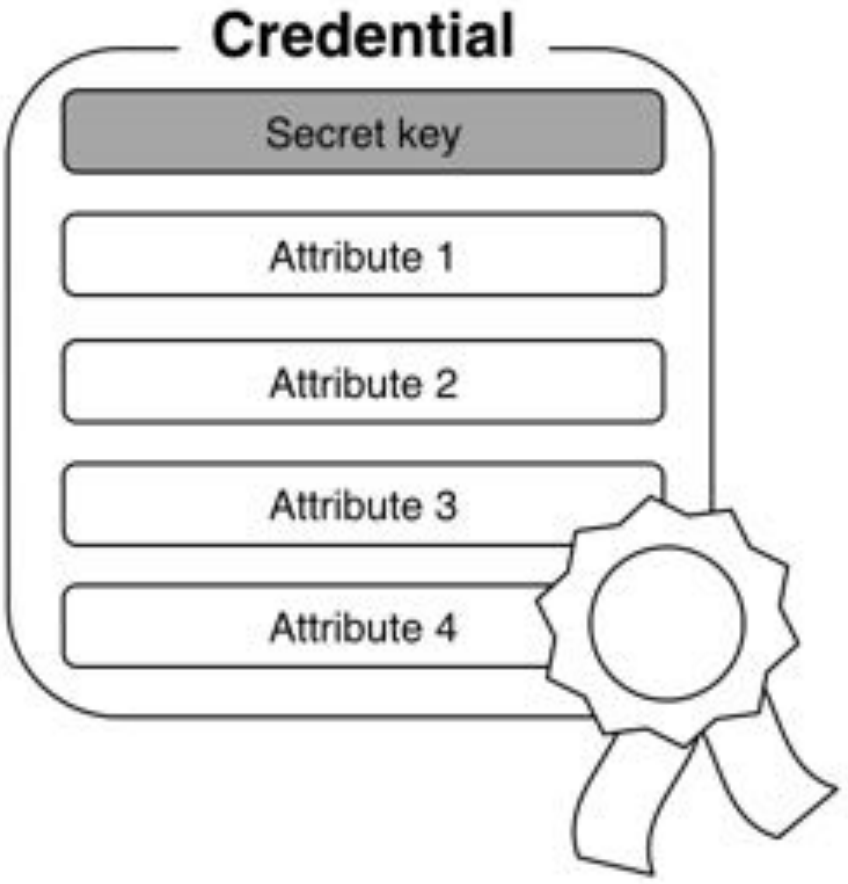
Identity Management



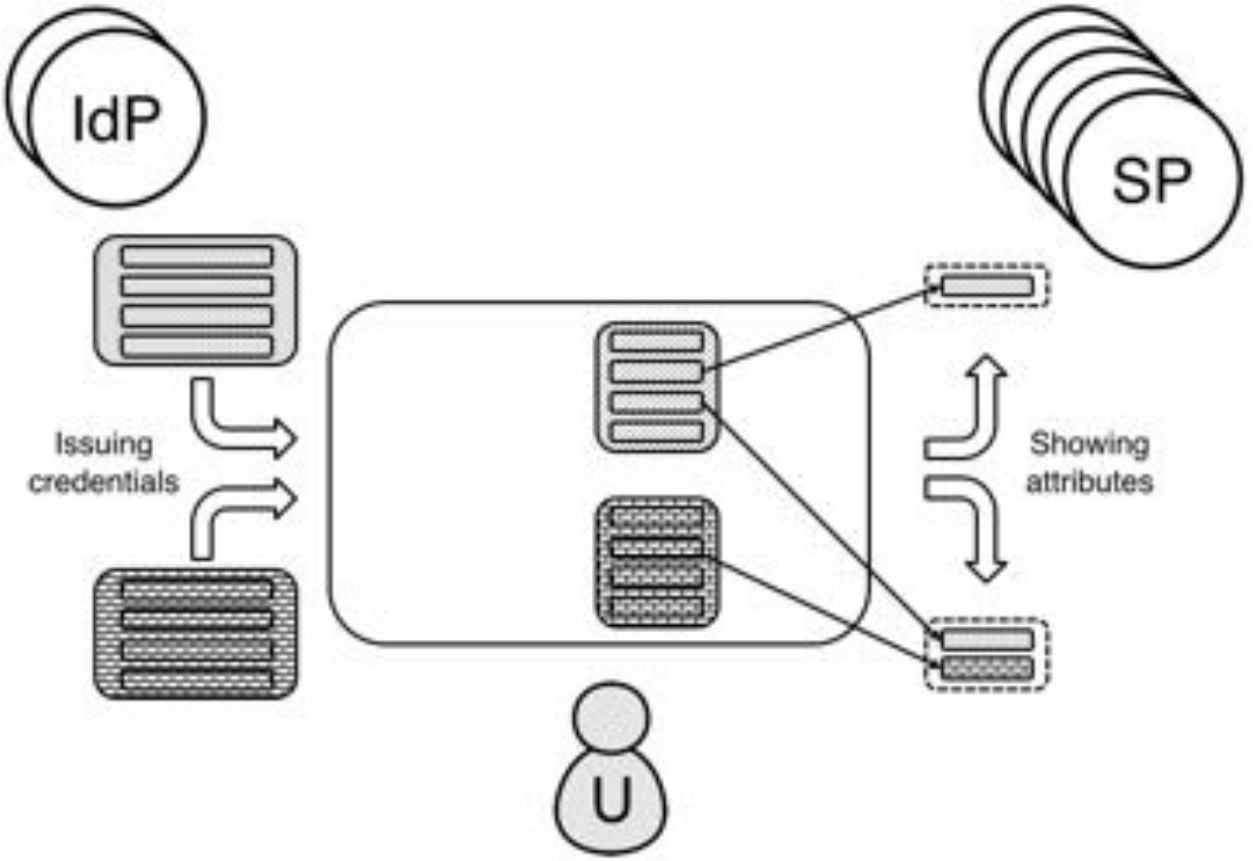
Attribute-Based Identity Management



Attribute-Based Credential



Issuing and Showing



Currently we are here...

Security and Privacy Today

Attribute-based identity management

Crypto of ABCs

Smart-card implementation

IRMA: the best of ABCs

Plan for Crypto

- Commitment
- Zero-knowledge proof
- Attribute-based credential (ABC)
- Selective disclosure

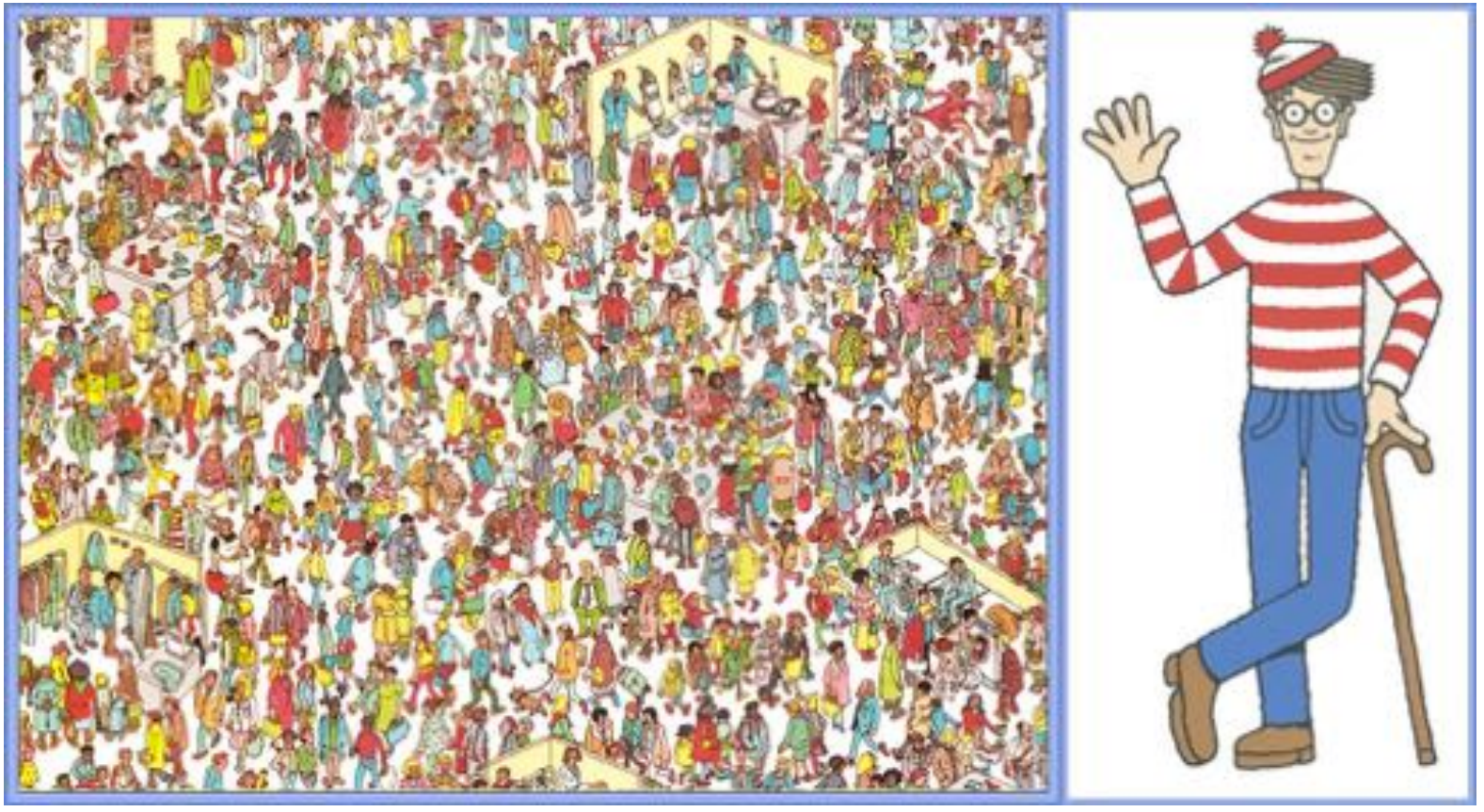
Commitment

- (Temporary) secret in a box with a padlock
- ... and a key.

- Phases:
  - Commit
  - Opening
- Examples (related to the DL problem):
  - $h = g^x \pmod{p}$. Commit: h, g, p; Opening: x.
  - $h = g^r \cdot g_1^x \pmod{p}$. Commit: h, g, g_1, p; Opening: r, x.

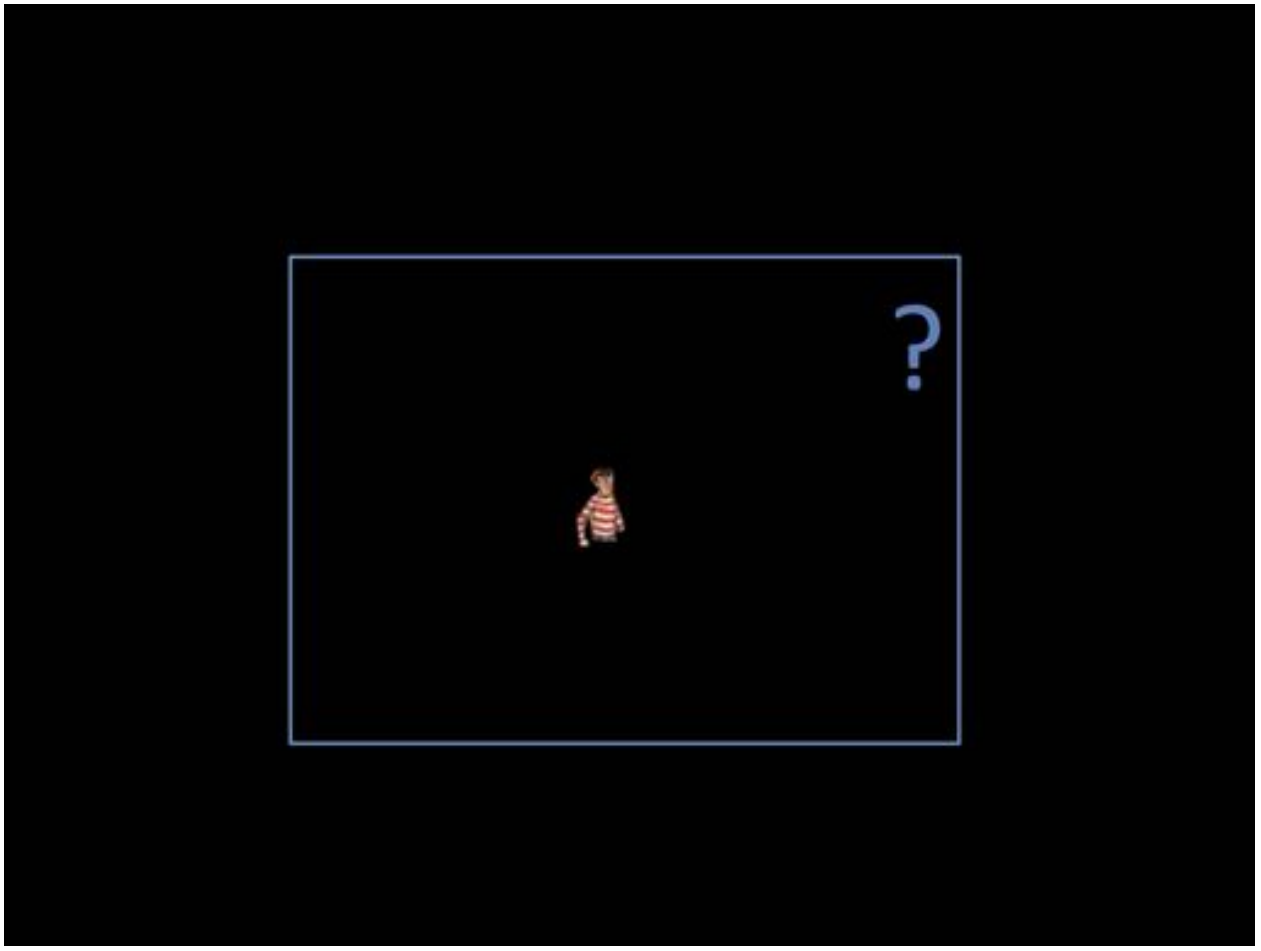
- Computational hiding and perfect binding.
  OR
- Perfect hiding and computational binding. [Damgård 99]

Where's Waldo?—Zero-Knowledge Proof



iCIS | Digital Security
Radboud University

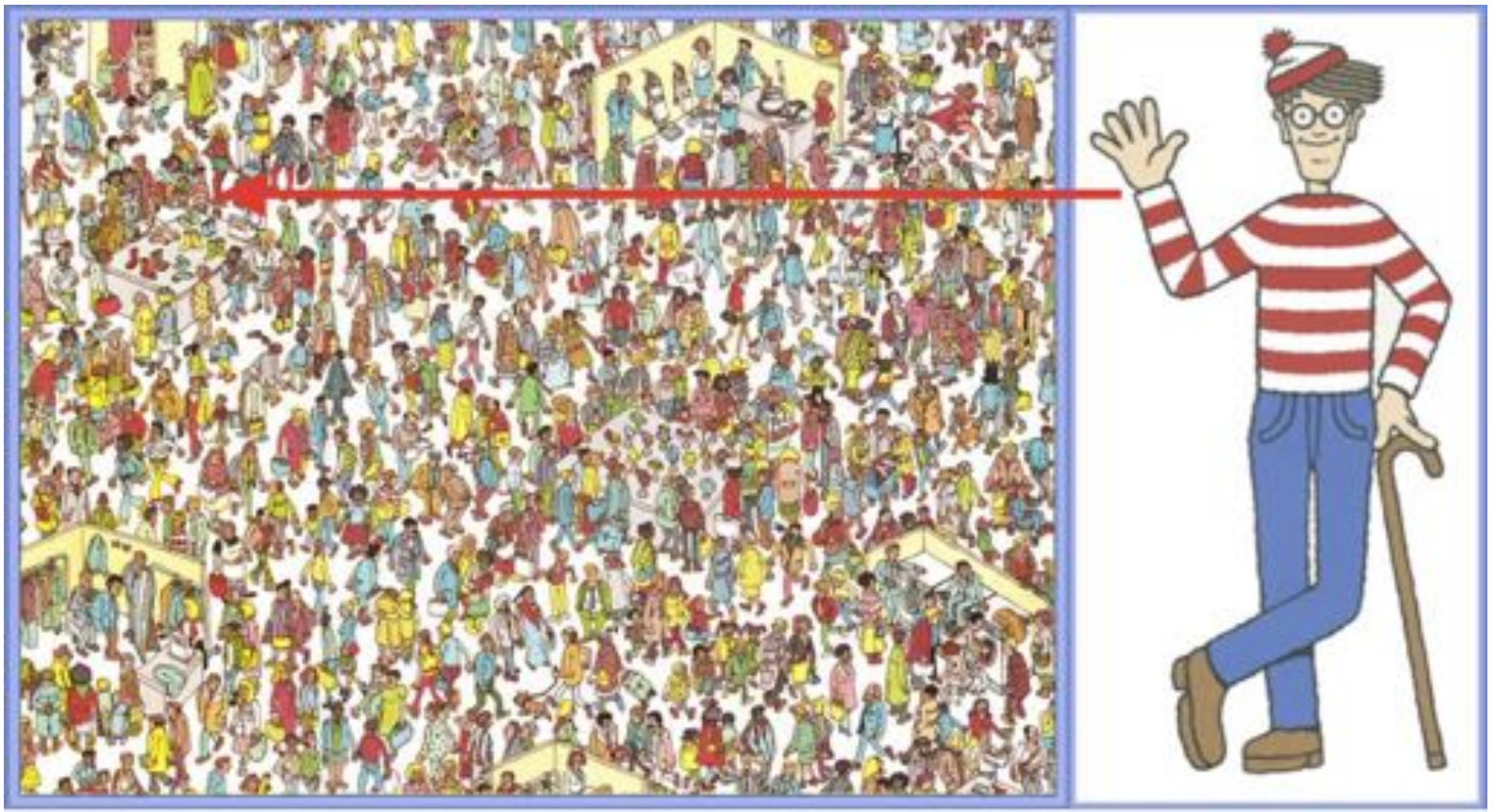
Where's Waldo?—Zero-Knowledge Proof



[Naor et al. 99]

iCIS | Digital Security
Radboud University

Where's Waldo?



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

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

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

IBM's Idemix Based on CL

- 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
    - Quadratic residues in $\mathbb{Z}_n^*$
    - QR_n is a subgroup of order $\varphi(n)/4$
  - 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

Step 1: Commitment

Take a commitment scheme – Pedersen on a_1

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

iCIS | Digital Security
Radboud University

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: $a_1, \ldots, a_L$

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

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.

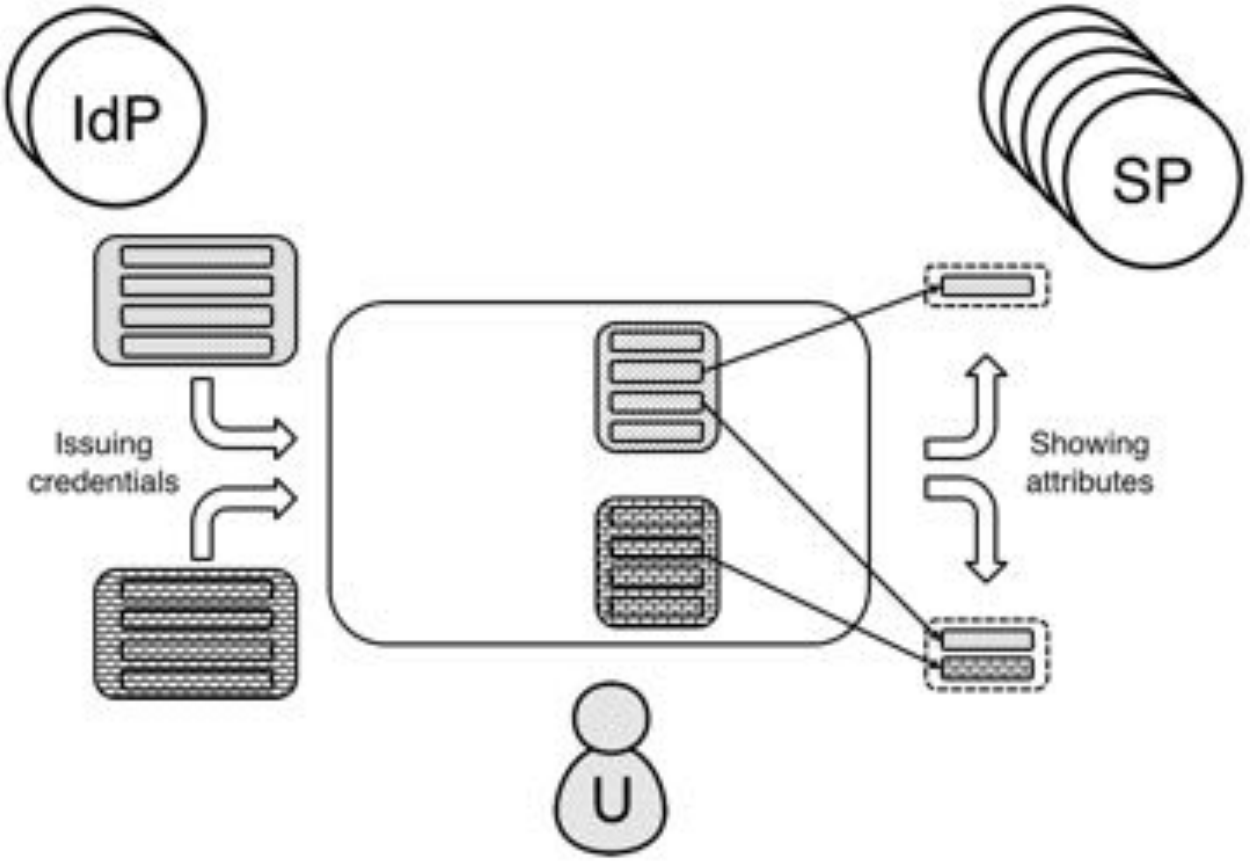
iCIS | Digital Security
Radboud University

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



CL Signature: Verification

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; U $\longrightarrow$ V

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

iCIS | Digital Security
Radboud University

What about e? – *i.e.* How to hide e?

- 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, U proves that she knows:

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

But then selective disclosure is easy!

iCIS | Digital Security
Radboud University

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:

U $\longrightarrow$ V disclose: a_1, a_2 and prove:

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

In Sum: ABCs are Powerful!

- Security
  - Authenticity
  - Integrity
  - Non-transferability
- Privacy
  - Issuer unlinkability
  - Multi-show unlinkability
  - Selective disclosure (data minimisation)
- Technics
  - IBM's idemix [CL 01, CL 02]
  - Microsoft's U-Prove [Brands 99]

Currently we are here...

Security and Privacy Today

Attribute-based identity management

Crypto of ABCs

Smart-card implementation

IRMA: the best of ABCs

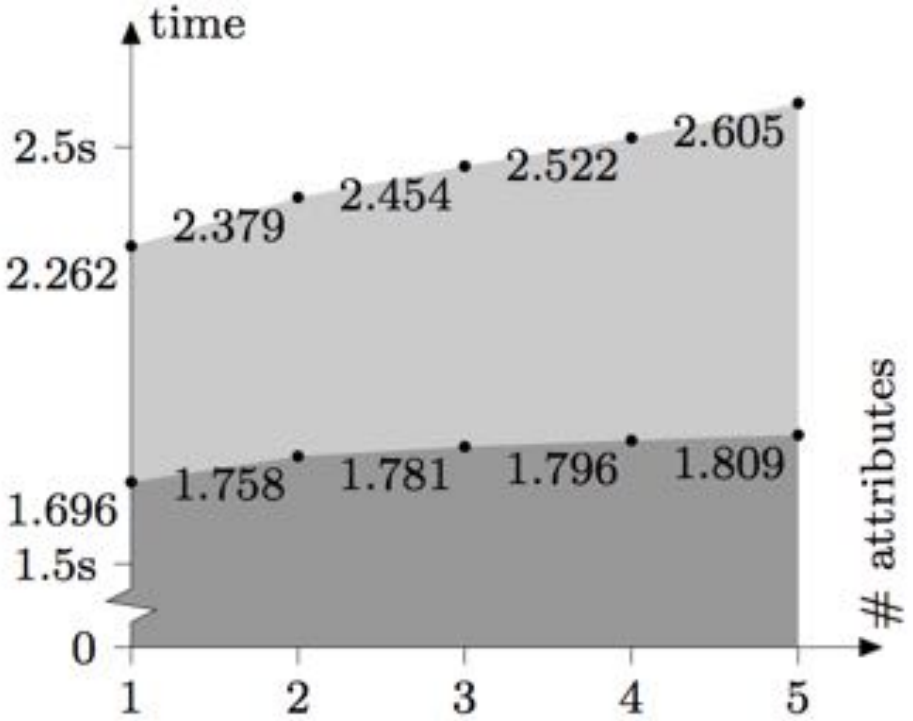
Why Smart Cards?

- Secure
- User-friendly

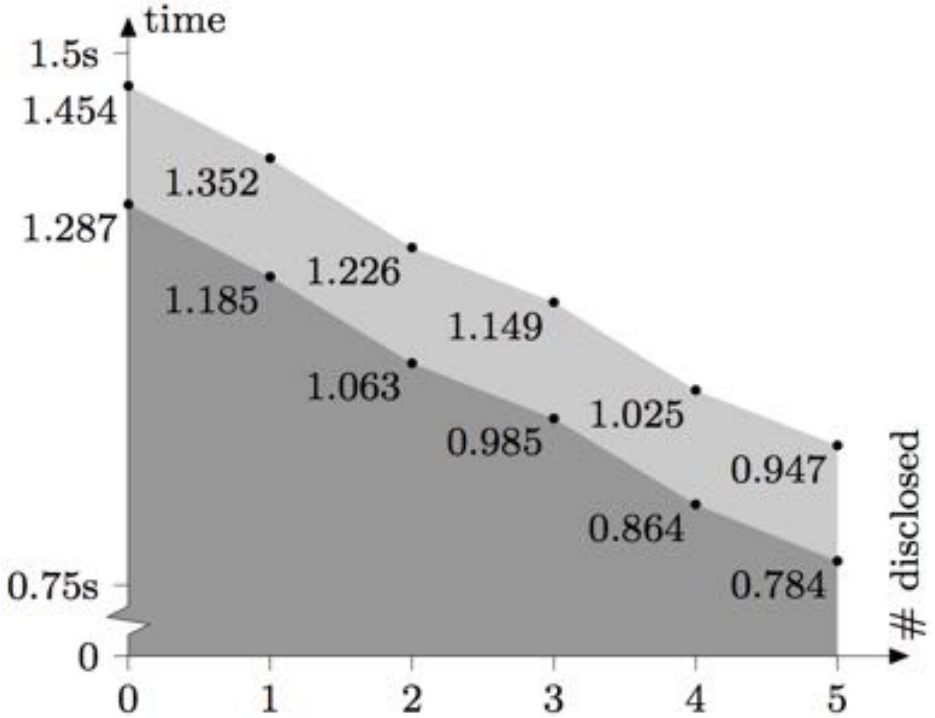
- Feels private
- Looks private

- Restrictions
  - No user interface (DEMO: Card management)
  - JavaCard? No (too restricted API)
  - MULTOS (Infineon SLE78 chip)
  - Small RAM
  - Slow EEPROM

Performance: Issuing [VA 13]



Performance: Showing [VA 13]



Currently we are here...

Security and Privacy Today

Attribute-based identity management

Crypto of ABCs

Smart-card implementation

IRMA: the best of ABCs

IRMA Team

"I Reveal My Attributes"

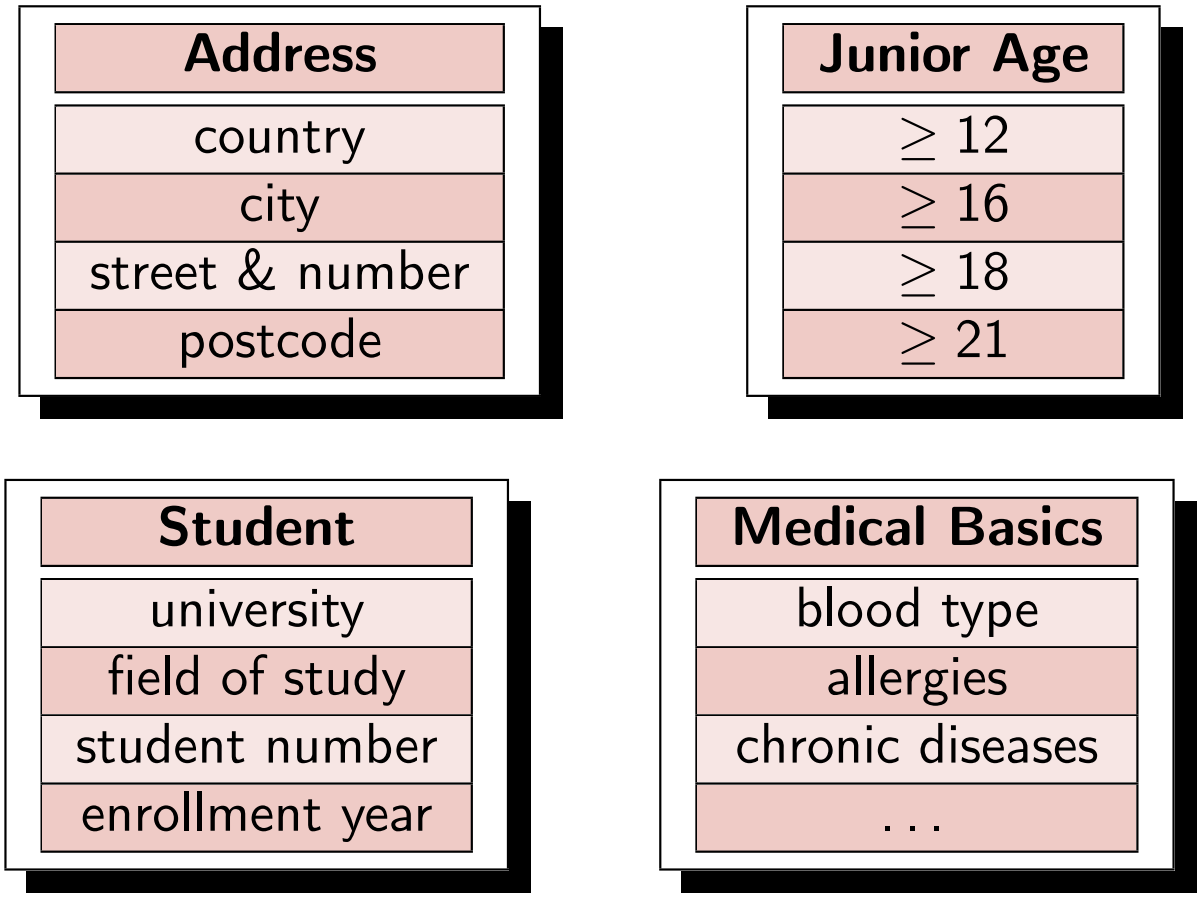
iCIS | Digital Security
Radboud University

The IRMA Card

Front

Back

ABC Examples



Challenges: ABCs on Smart Cards

- Card anonymity
- Card life cycle

- Credential design
- Online and offline use cases (DEMO: IRMA Tube)

- User authentication (PIN)
- Certification of issuers and verifiers
- Secure channel between card and verifier

- User interfaces (consent!)
- Card management

- Card revocation
- Preventing abuse of anonymity

Summary

- "Attributes rather than identifiers"
- Attribute-based identity management is becoming practical
- Privacy and user control (without losing functionality)
- Nice crypto

- Lots of further questions
  - Deployment
  - Socio-technical aspects
  - Combat suspicion against anonymity
  - To make other attribute-based technologies practical

Questions?

IRMA-related References 1

- https://www.irmacard.org
- Gergely Alpár, Lejla Batina, Roel Verdult. Using NFC Phones for Proving Credentials, PILATES 2012, LNCS 7201, Kaiserslautern, Germany, 2012.
- Gergely Alpár, Lejla Batina, Wouter Lueks. Designated Attribute-Based Proofs for RFID Applications, In Jaap-Henk Hoepman and Ingrid Verbauwhede, editors, RFID Security and Privacy (RFIDsec), LNCS 7739, Nijmegen, The Netherlands, pages 59–75. Springer, 2012.
- Pim Vullers and Gergely Alpár. Efficient Selective Disclosure on Smart Cards Using Idemix. In Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell editors, Policies and Research in Identity Management (IDMAN), 3rd IFIP WG 11.6 Working Conference, London, UK, IFIP AICT 396, pages 53–67. Springer, 2013.
- Gergely Alpár and Bart Jacobs. Credential Design in Attribute-Based Identity Management. In Ronald Leenes and Eleni Kosta, editors, Bridging distances in technology and regulation, pages 189–204, 3rd TILTing Perspectives Conference, Tilburg, NL, April 25-26, 2013.

IRMA-related References 2

- Gergely Alpár and Jaap-Henk Hoepman. A Secure Channel for Attribute-based Credentials [Short paper]. In Proceedings of the 2013 ACM Workshop on Digital Identity Management (DIM 2013), pages 13–18, Berlin, November 8, 2013.
- Merel Koning, Paulan Korenhof, Gergely Alpár and Jaap-Henk Hoepman. The ABC of ABC: an analysis of attribute-based credentials in the light of data protection, privacy and identity. In Proceedings of the 10th International Conference on Internet, Law & Politics (IDP 2014): A decade of transformations, pages 357–374, Barcelona, July 3-4, 2014.
- Antonio de la Piedra, Jaap-Henk Hoepman, and Pim Vullers, Towards a Full-Featured Implementation of Attribute Based Credentials on Smart Card. In A. Kiayias and D. Gritzali, editors, 13th Int. Conf. on Cryptology and Network Security (CANS 2014), Heraklion, Crete, Greece, October 22-24 2014.
- Wouter Lueks, Gergely Alpár, Jaap-Henk Hoepman, and Pim Vullers. Fast Revocation of Attribute-Based Credentials for Both Users and Verifiers. In Proceedings of the IFIP International Information Security and Privacy Conference (IFIP SEC 2015), Hamburg, May 26-28, 2015.

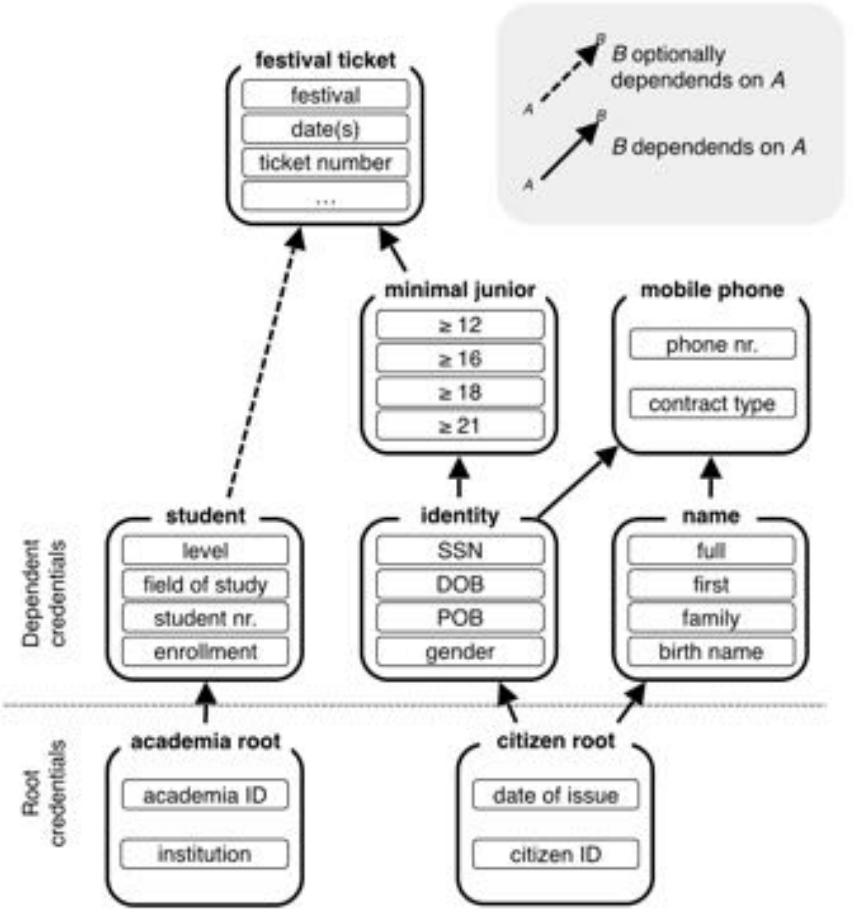
References 1

- [BP 97] N. Barić and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In Advances in Cryptology–EUROCRYPT'97, pages 480–494. Springer, 1997.
- [Brands 99] S. A. Brands. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, MA, USA, 2000.
- [CL 01] J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In B. Pfitzmann, editor, Advances in Cryptology–EUROCRYPT 2001, volume 2045 of LNCS, pages 93–118. Springer Berlin / Heidelberg, 2001.
- [CL 02] J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. In S. Cimato, G. Persiano, and C. Galdi, editors, Security in Communication Networks, volume 2576 of LNCS, pages 268–289. Springer Berlin / Heidelberg, 2002.
- [Damgård 99] I. Damgård. Commitment schemes and zero-knowledge protocols. In Lectures on Data Security, pages 63–86. Springer, 1999.
- [FIDIS 2005] J. Backhouse. D4. 1: Structured account of approaches on interoperability. FIDIS Deliverables, 2005.

References 2

- [FO 97] E. Fujisaki and T. Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In Advances in Cryptology–CRYPTO'97, pages 16–30. Springer, 1997.
- [FS 86] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, Advances in Cryptology–CRYPTO '86, volume 263 of LNCS, pages 186–194. Springer, 1987.
- [Naor et al. 99] M. Naor, Y. Naor, and O. Reingold. Applied Kid Cryptography or How to convince your children you are not cheating. Journal of Craptology, 0 (1) (1999).
- [Schnorr 91] C.-P. Schnorr. Efficient signature generation by smart cards. Journal of cryptology, 4(3):161–174, 1991.
- [VA 13] Pim Vullers and Gergely Alpár. Efficient Selective Disclosure on Smart Cards Using Idemix. In Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell editors, Policies and Research in Identity Management (IDMAN), 3rd IFIP WG 11.6 Working Conference, London, UK, IFIP AICT 396, pages 53–67. Springer, 2013.

Credential "Tree"



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

- Discrete logarithm: "I know the discrete logarithm $\log_g h$."
- Non-interactive: $\mathrm{SPK}\{\chi | h = g^{\chi}\}(n)$

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

iCIS | Digital Security
Radboud University