How Light is Lightweight Crypto

(and what has changed since RFIDSec cca 2005-06)

Lejla Batina

Digital Security Group
Institute for Computing and Information Sciences (ICIS)
Radboud University Nijmegen
The Netherlands

and KU Leuven, Belgium

RFIDSec13 – July 11, 2013

some slides credit: Gergely Alpar

Take-home messages

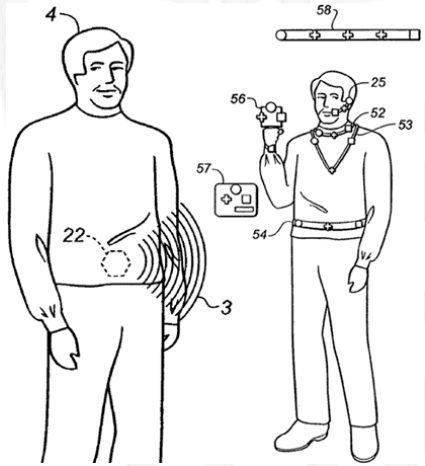
- We need PKC for privacy in RFID applications
- Zero-knowledge proofs can be used for revealing private data responsibly
- This puts a lot of constraints on hardware
- Technologies around **anonymous credentials** are feasible even in low-lost applications

Outline

- Some history
- Introduction
  - ABC – attribute-based credentials
  - Privacy-friendly authentication
  - Using NFC-enabled phones for authentication: open issues
- Part 1: Privacy in the bag or "the curious case of designated proofs"
- Part 2: ECC processor for RFID applications
- Part 3: IRMA project
- Conclusions, future work

RFID tags and alikes

- Supply chain management
- Product authentication
- Vehicles tracking
- Medical care
- RFID passports
- Mobile credit card payment systems
- Transportation payment systems
- Animal identification



RFIDSec cca 2005-06

- Sanjay Sarma: “we need security for 2k gates”
- Emerging new applications: medical/pharmaceutics, transportation, sensor networks, car immobilizers, key chains etc.
  - resource limited: area (< 1 mm^2), memory, bandwidth
  - low-cost, low-power (< 500µW or I < 10µA @ 1.5 V), low-energy
- Does ECC fit RFID:
  - Area – depends on the library used
  - Performance – poor ☹
  - Power – YES! ☺ => there is hope
- Privacy enhancement, counterfeit detection
- Side-channel security

RFIDSec cca 2013

- Many new lightweight block ciphers, hash functions
- Implementations optimized, power/energy revisited
- ECC does fit RFID
- Applications: transportation, medical applications, smart phones,…
- Privacy issues still open and coming:
  - Depends on application
  - **Attribute-based authentication**

Why attribute-based authentication

- Privacy-friendly
- Protection against identity fraud
- More flexible approach for authentication and identity management

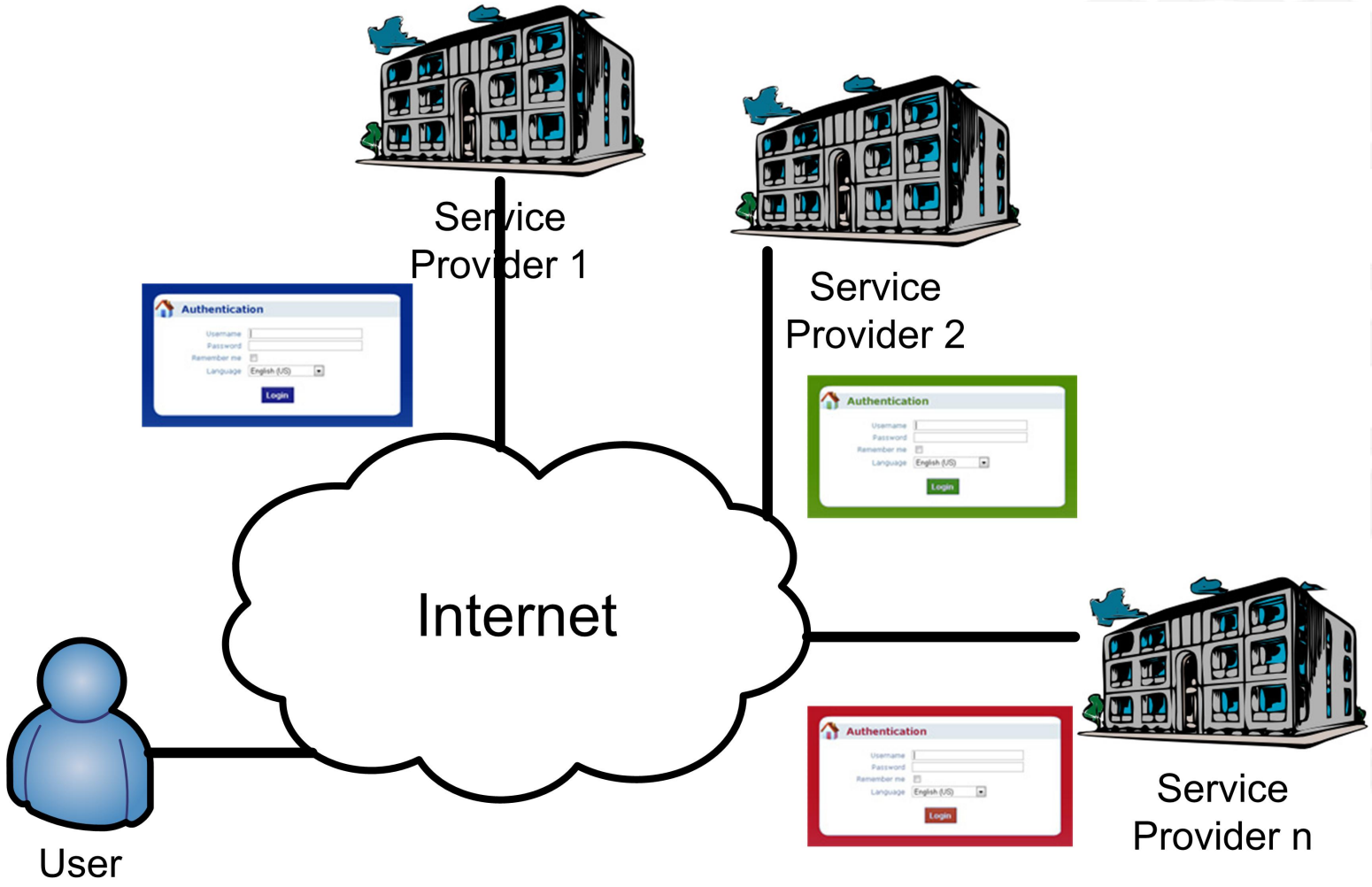
But why now?

- Proposed more than 25 years ago by David Chaum
- Stefan Brands: first practical realization of ABCs
- IBM's Idemix based on zero-knowledge proofs
- Recent generation of smartcard powerful enough to perform the crypto operations required

Credentials or attributes

- Credentials contain attributes
- Credentials are issued and attributes are shown
- Example - Identity credential can contain
  - Social security nr.
  - Date of birth (but also “under 18”)
  - Place of birth
  - Gender

Credentials all over…



Solutions

- 1st: credential and provide data to SP

Solutions

Current practice

- 1st: credential and provide data to SP

Solutions

- 1st: credential and provide data to SP
- 2nd: credential in the mobile phone (App)

Solutions

- 1st: credential and provide data to SP
- 2nd: credential in the mobile phone (App)

App

- Credential stored on mobile
- More trust in the phone
- One-factor authentication
- Restricted functionality

Solutions

- 1st: credential and provide data to SP
- 2nd: credential in the mobile phone (App)
- 3rd: card + reader (EMV-CAP)

Solutions

- 1st: credential and provide data to SP
- 2nd: credential in the mobile phone (App)
- 3rd: card + reader (EMV-CAP)

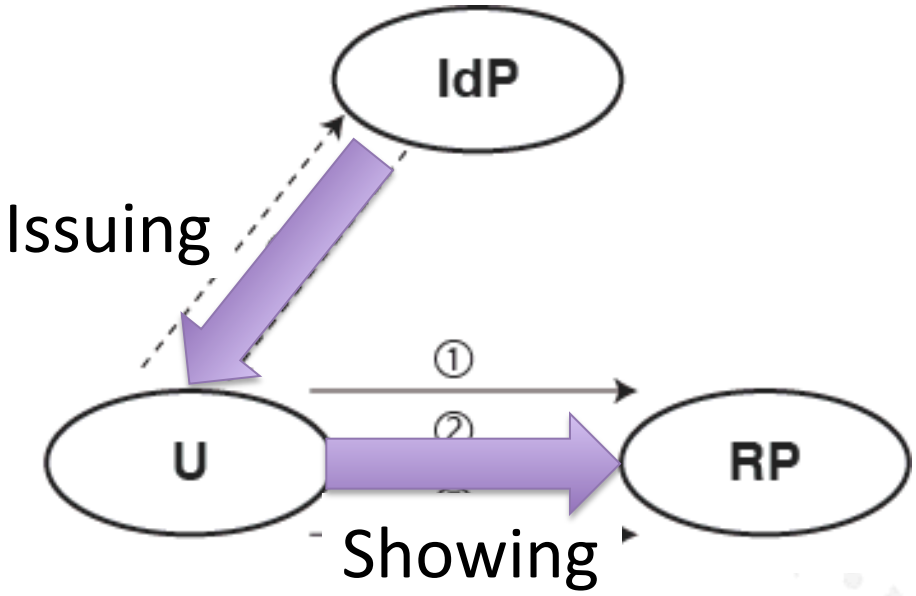
Card reader

- SP's device
- 1 reader/service
- Extra gadget to carry around

Solutions

- 1st: credential and provide data to SP
- 2nd: credential in the mobile phone (App)
- 3rd: card + reader (EMV-CAP)
- 4th: card + NFC- enabled mobile phone (personal card reader)

Credential flow



'cachable' steps

③ *authenticate*

④ *send claims*

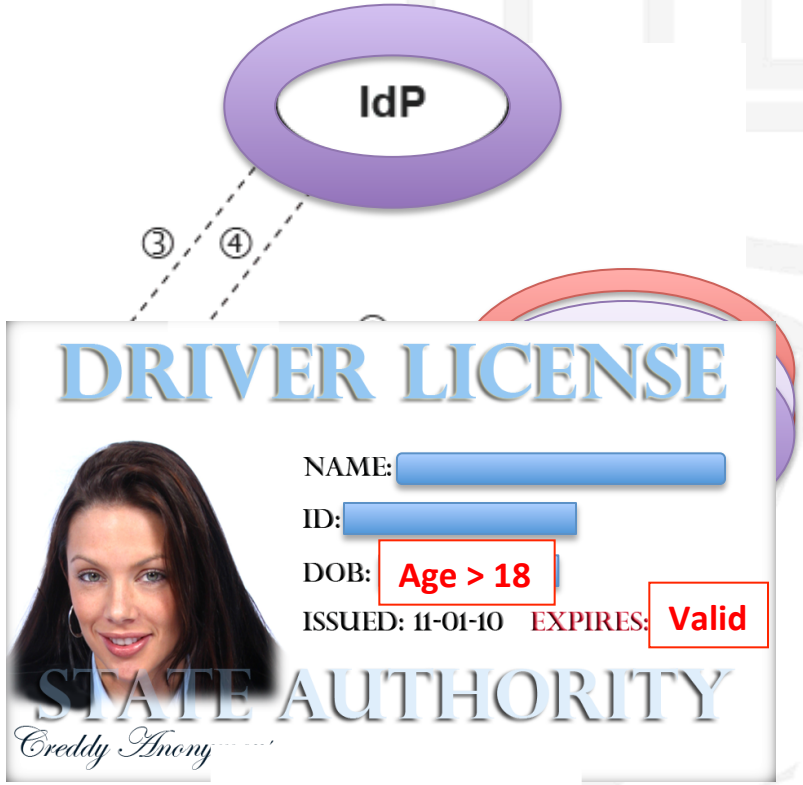
① request service

② send policy

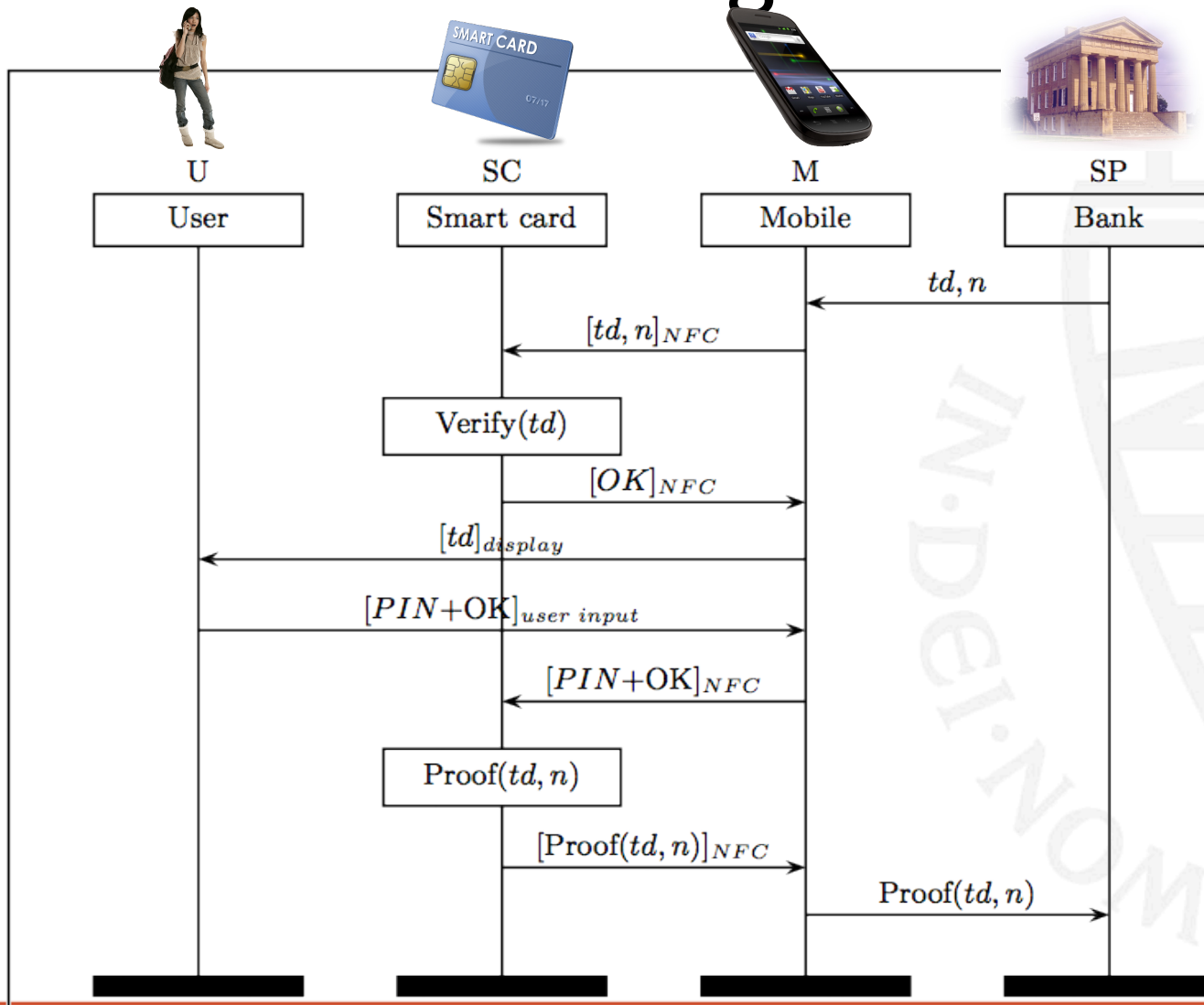
⑤ supply claims

Anonymity requirements

- Untraceability
- Multi-show unlinkability
- Selective disclosure
- Attribute property proof



On-line banking with NFC



Switch →

Switch → Trusted mode (TM)

Threat model

- Phishing
- Network attacker
  - Eavesdropping
  - Active adversary
- Phone theft
- Malware
- Smart card theft

Tap2: summary and open issues

- User-friendly and privacy-friendly applications
- Credentials on smart cards (issued by trusted parties)
- Mobile phones instead of readers
- Hardware switch for PIN:
  - Requires conscious choice
  - Secure
- Tap2Prove:
  - Cigarette machine: Age() > 18
  - Identity proof at an eGovernment site
- Tap2Bill
- Tap2P2P

Gergely Alpár, Lejla Batina, Roel Verdult. Using NFC Phones for Proving Credentials, PILATES 2012, LNCS 7201, Kaiserslautern, Germany, 2012.

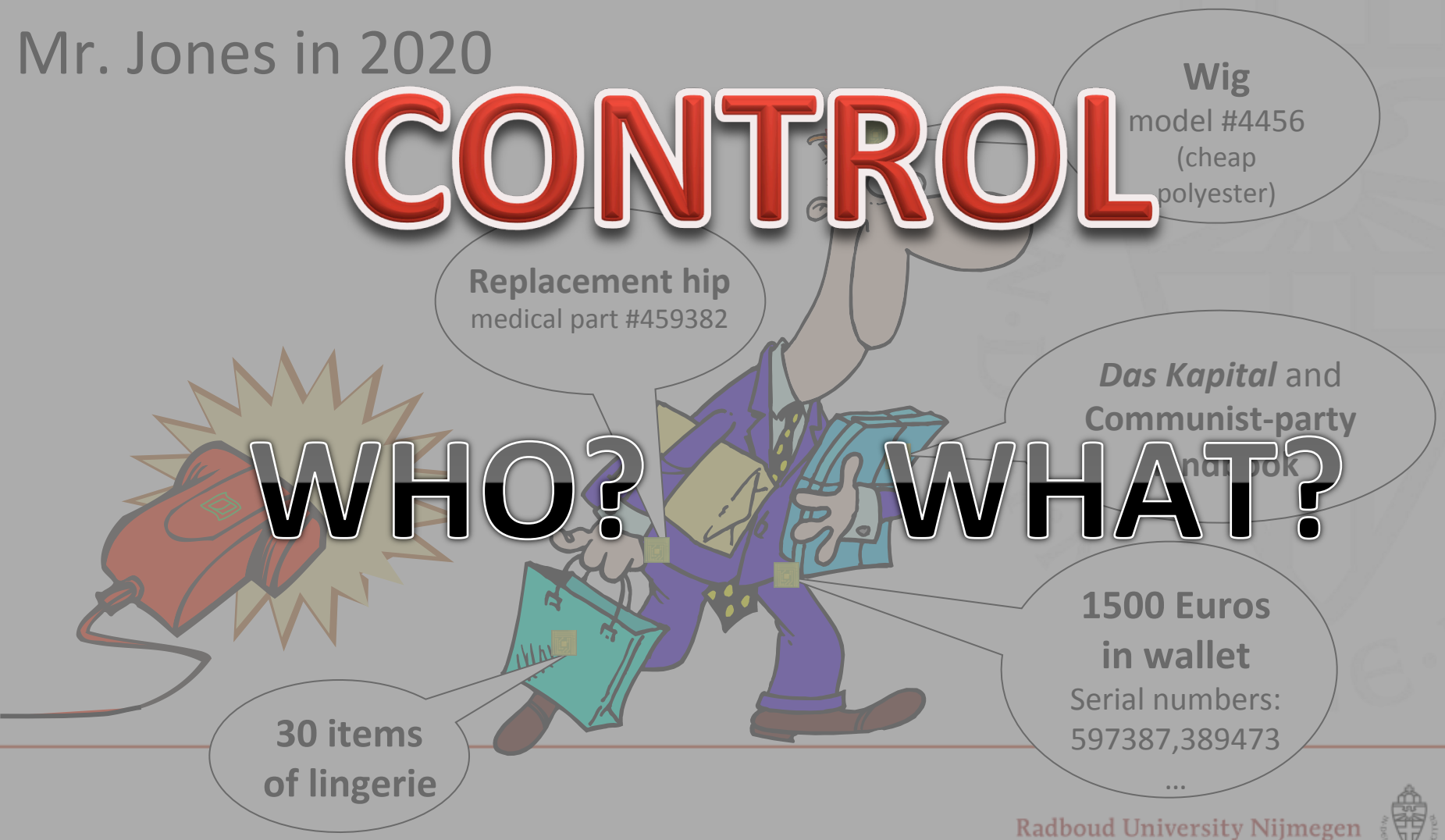
Designated attribute-based proofs for pervasive applications

joint work with Gergely Alpar and Wouter Lueks

The consumer privacy problem

Source: Ari Juels, RSA Laboratory

Mr. Jones in 2020



More attributes

PASSPORT

1. Passport id
2. Name
3. Nationality
4. Expiry date

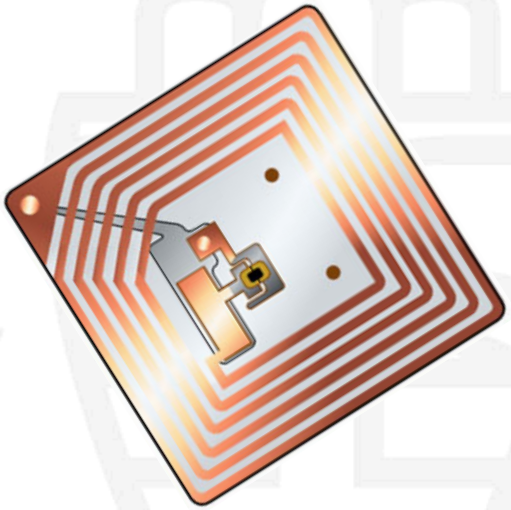
…

MEDICINE

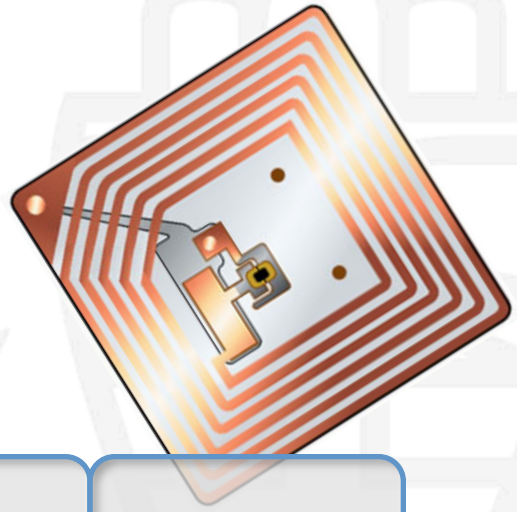
1. Name
2. Disease
3. Permission number

…

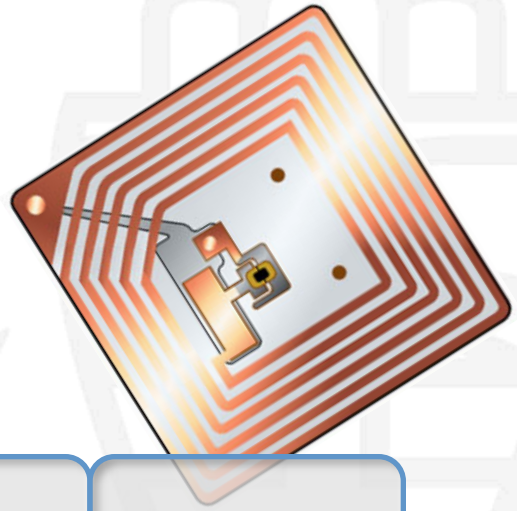
Instead of only one, …



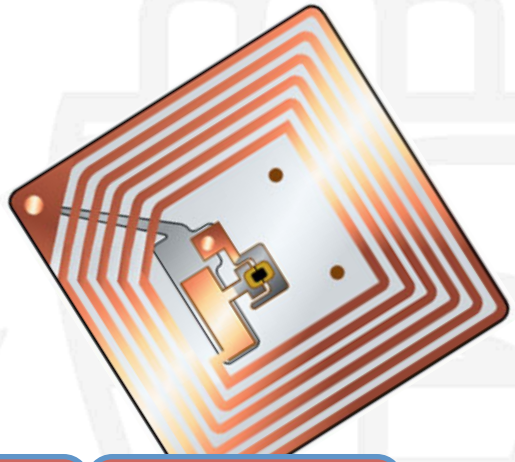
… multiple attributes



Only legitimate (designated) readers



Limited access to attributes



So, we need

- Designation → only legitimate readers
- Multiple attributes → on the tags
- Possibility to reveal only one attribute

Related schemes

Randomized Schnorr, 2008

Valid tag identifiers

Schnorr (1990)

Prover Secret: x	$P, I = xP$	**Verifier**	
$\alpha \in_R \mathbb{Z}_p$			
$A := \alpha P$	$\xrightarrow{A}$		*Commitment*
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_p^*$	*Challenge*
$r := c \cdot x + \alpha \pmod p$	$\xrightarrow{r}$	Verification:	*Response*
		$cI \stackrel{?}{=} rP - A$	

$$I \stackrel{?}{=} c^{-1}\left(rP - A\right)$$

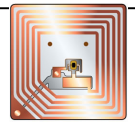
Randomized Schnorr (2008)

Schnorr

Prover Secret: x	$P, I = xP$	**Verifier**
$\alpha \in_R \mathbb{Z}_p$ $A := \alpha P$ $r := c \cdot x + \alpha \pmod p$	$\xrightarrow{A}$ $\xleftarrow{c}$ $\xrightarrow{r}$	 $c \in_R \mathbb{Z}_p^*$ Verification: $I \stackrel{?}{=} c^{-1}(rP - A)$

Randomized Schnorr

Prover $x, I = xP$	$P, V = vP$	**Verifier** v
$\alpha, \beta \in_R \mathbb{Z}_p$ $A_1 := \alpha P$ $A_2 := \beta V$ $r := c \cdot x + \alpha + \beta \pmod p$	$\xrightarrow{A_1, A_2}$ $\xleftarrow{c}$ $\xrightarrow{r}$	 $c \in_R \mathbb{Z}_p^*$ Verification: $I = c^{-1}(rP - A_1 - v^{-1}A_2)$ check whether I is a valid identifier



Related schemes

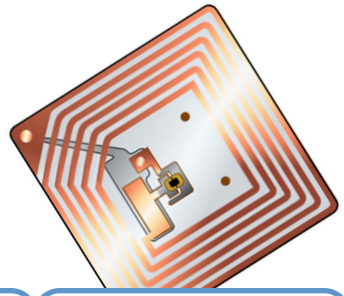
Randomized Schnorr, 2008

Brands' U-Prove, 1999

U-Prove showing, i.e. DL-REP proof

Prover	$P_0, \ldots, P_l$	**Verifier**
$x_0, \ldots, x_l$	$I = \sum_0^l x_i P_i$	
$\alpha_i \in_R \mathbb{Z}_p, \quad i \in \{0, \ldots, l\}$		
$A := \sum_0^l \alpha_i P_i$	$\xrightarrow{A}$	
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_p^*$
$r_i := c \cdot x_i + \alpha_i \pmod p$	$\xrightarrow{(r_i)_{i \in \{0,\ldots,l\}}}$	Verification: $I \stackrel{?}{=} c^{-1} \left(\sum_0^l r_i P_i - A \right)$

Combining?

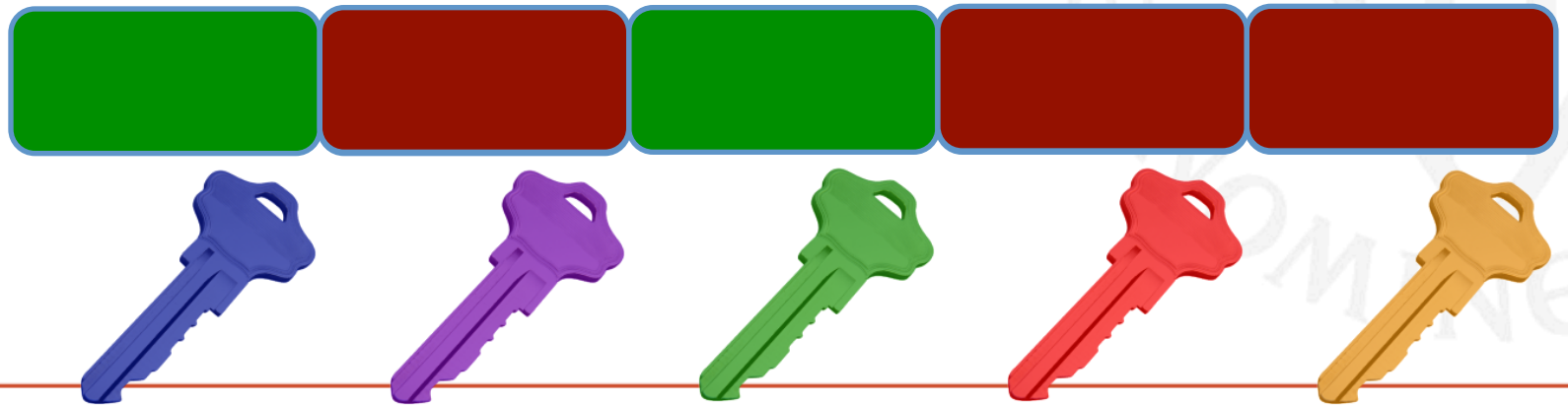


Designated DL-REP proof

Prover		**Verifier**
$x_0, \ldots, x_l$ $I = \sum_0^l x_i P_i$	$P_0, \ldots, P_l$ $V = v \cdot \sum_0^l P_i$	v
$\alpha_0, \ldots, \alpha_l, \beta \in_R \mathbb{Z}_p$ $A_1 := \sum_0^l \alpha_i P_i$ $A_2 := \beta V$ $\forall i \in 0, \ldots, l :$ $r_i := c \cdot x_i + \alpha_i + \beta \pmod p$	$\xrightarrow{A_1, A_2}$ $\xleftarrow{c}$ $\xrightarrow{r_0, \ldots, r_l}$	$c \in_R \mathbb{Z}_p^*$ Verification: $I := c^{-1}(\sum_0^l r_i P_i - A_1 - v^{-1} A_2)$ check whether I is a valid identifier

Designation keys (reader)

$$\mathcal{E} = \{1, 3\}$$



Designated partial DL-REP proof

Prover		**Verifier**
$x_0, \ldots, x_l$	$P_0, \ldots, P_l$	$v, (v_i)_{i \in \mathcal{E}}$
$I = \sum_0^l x_i P_i$	$\forall i \in \mathcal{D}: \; V_i = v_i P_i$ $V = v \cdot \sum_0^l P_i$	
$\alpha_0, \ldots, \alpha_l, \beta \in_R \mathbb{Z}_q^*$ $A_1 := \sum_0^l \alpha_i P_i$ $A_2 := \beta V$ $B_i = (\alpha_i + \beta) V_i \quad \forall i \in \mathcal{D}$	$\xrightarrow{A_1, A_2, (B_i)_{i \in \mathcal{D}}}$ $\xleftarrow{c}$	$c \in_R \mathbb{Z}_q^*$
$\forall i \in 0, \ldots, l:$ $r_i := c \cdot x_i + \alpha_i + \beta \pmod p$	$\xrightarrow{r_0 \ldots r_l}$	First verify that the identifier is correct: $I = c^{-1}(\sum_0^l r_i P_i - A_1 - v^{-1} A_2)$ Then for each $j \in \mathcal{D} \cap \mathcal{E}$ and attribute C_j: $C_j = I - c^{-1}(\sum_{i \neq j} r_i P_i - A_1 - v^{-1} A_2 + v_j^{-1} B_j)$

Your bag, your privacy!

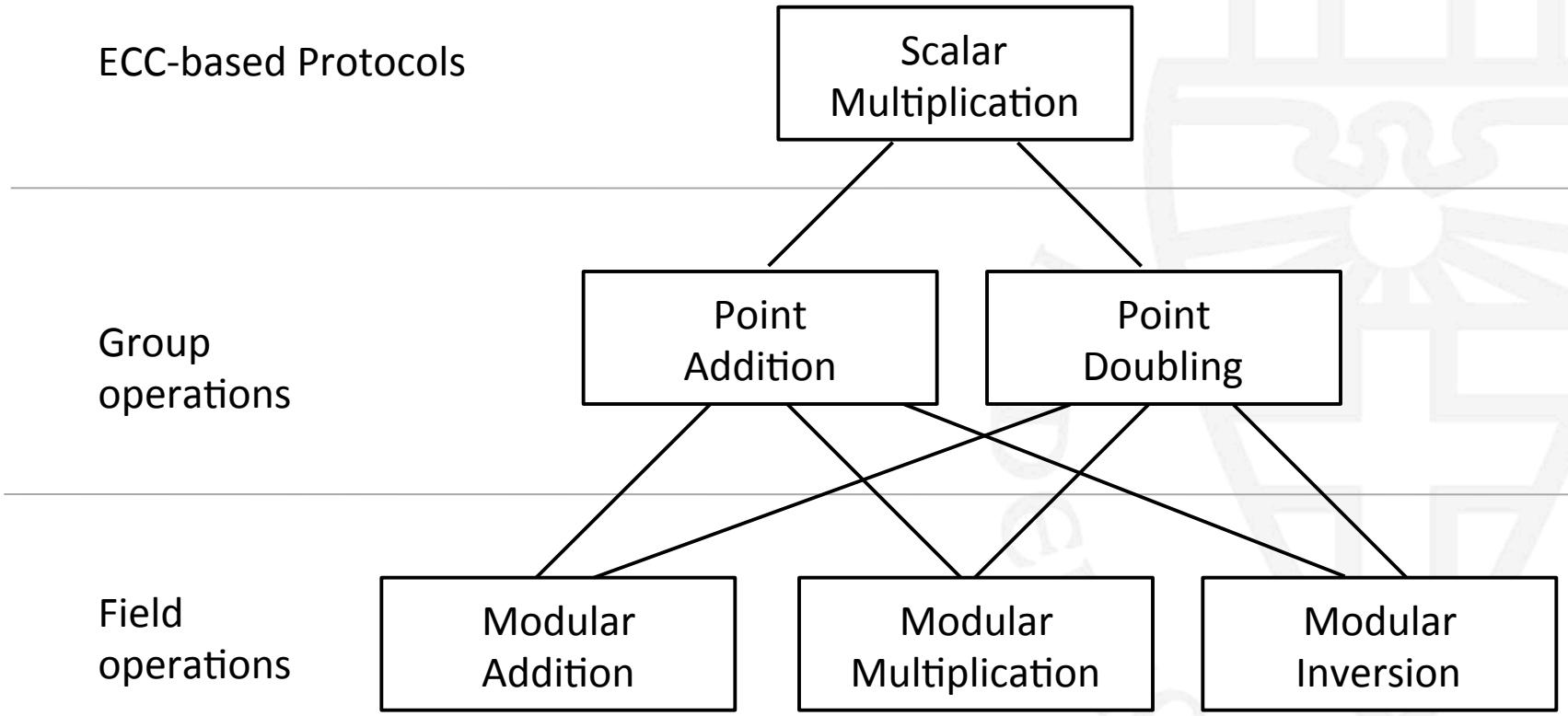
- Designated selective disclosure provides fine-grained access control
- An arbitrary reader can only read what it's entitled to
- A step forward in RFID authentication

Comparing costs of several authentication protocols

Protocol	Number of EC scalar multiplications on the tag side	Number of EC scalar multiplications on the reader side
Schnorr	1	2
Randomized Schnorr	2	3
Proof of knowledge of DL-REP of *I*	$l+2$	$l+3$
Designated selected disclosure	$l+2+d$	who cares

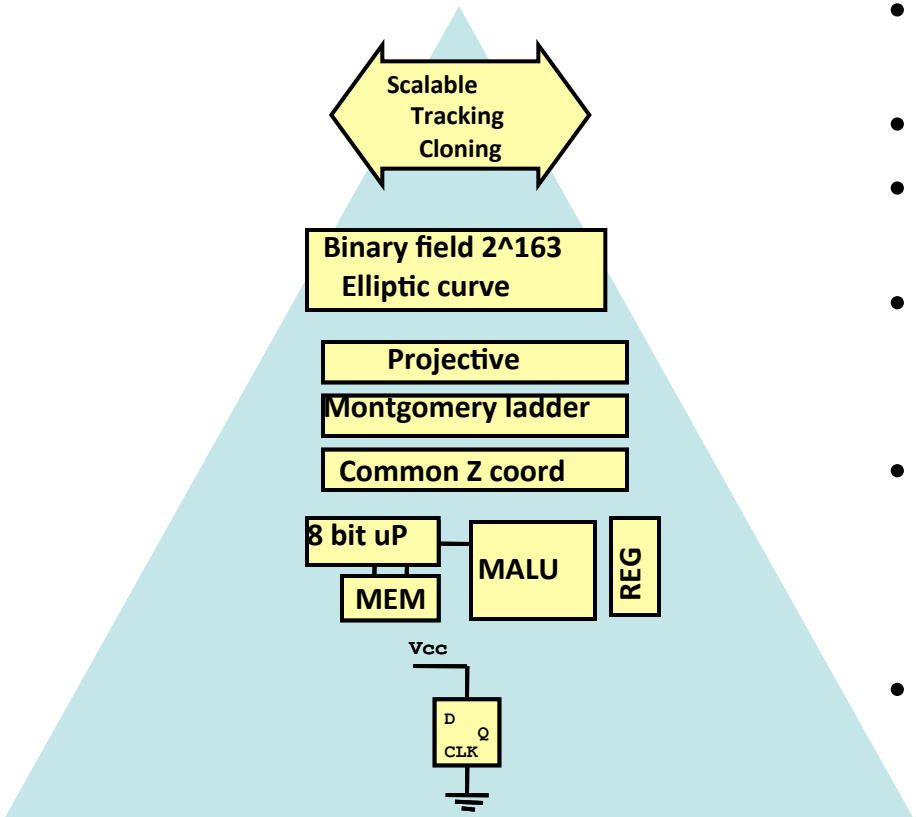
Lightweight PKC i.e.
ECC for RFID applications

Point operations - ECC



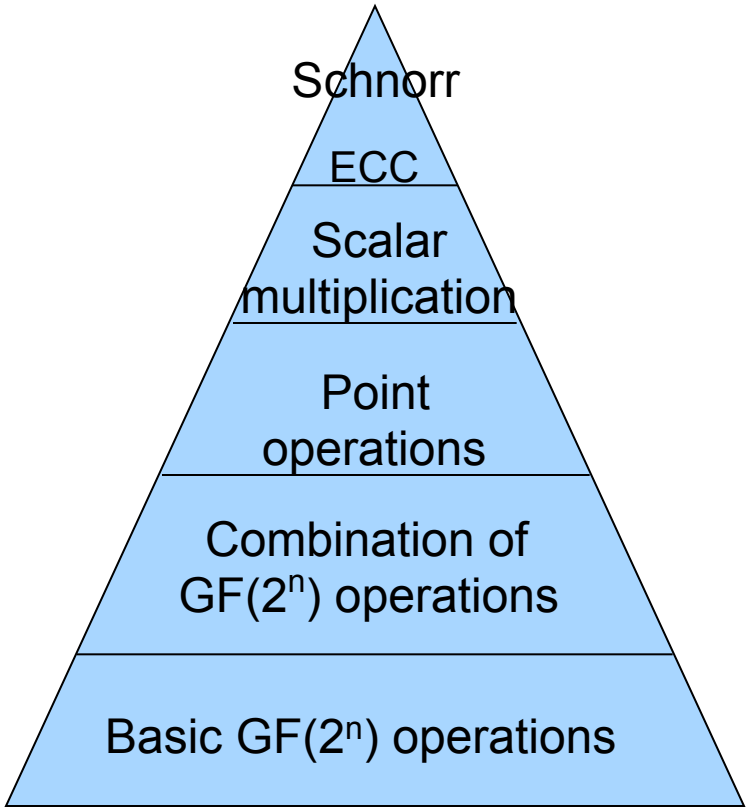
Challenge: low power public key …

Address at all design abstraction levels!



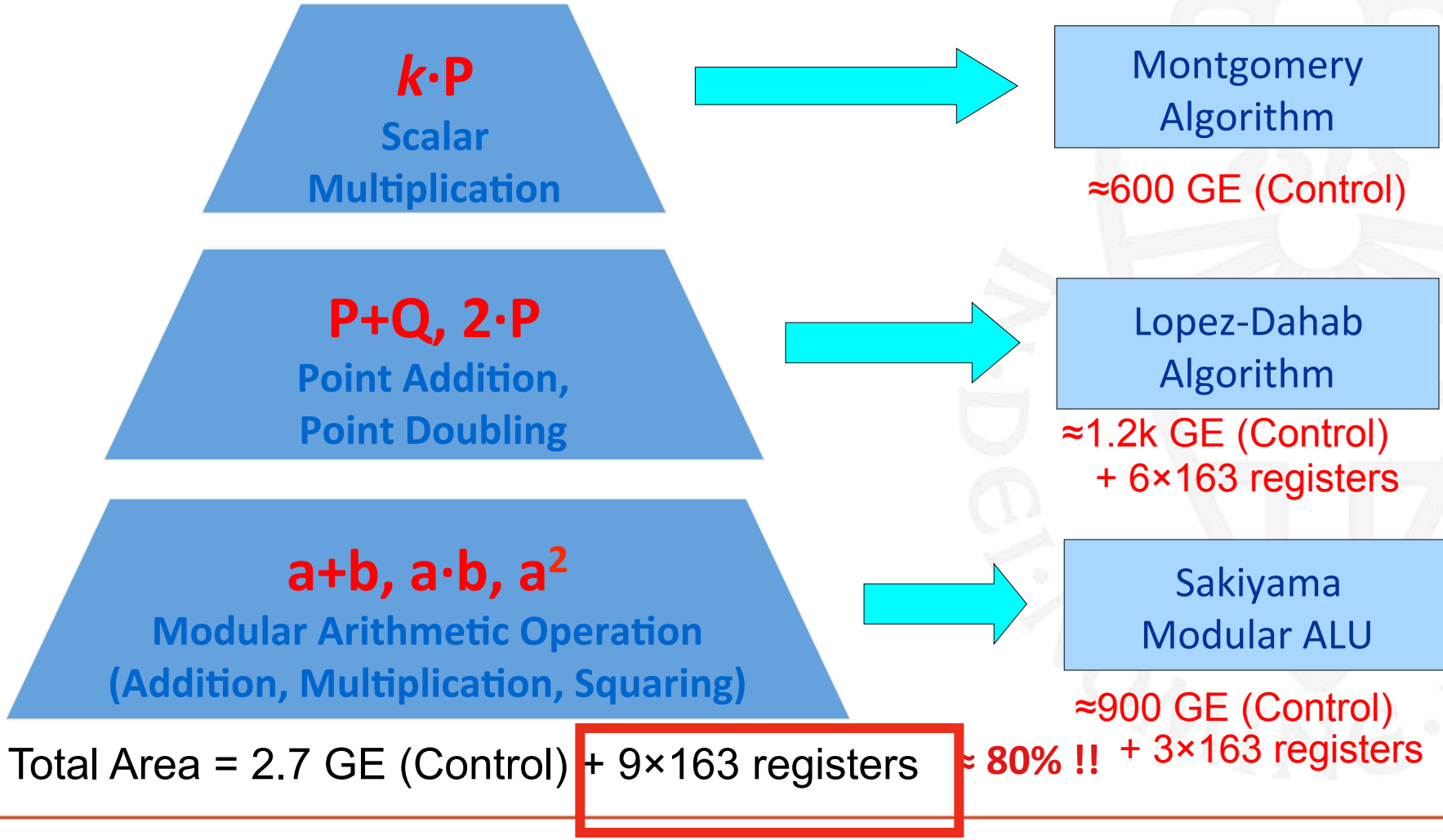
- **Protocol** : asymmetric (most work for the reader)
- **Algorithm**: Elliptic curve (163 bits)
- **Field Operation**: Binary fields - easier field operations (carry-free arithmetic)
- **Projective** coordinate system:
  - (X, Y, Z) instead of (x,y): no field inversions
- **Special coordinate system**: no need to store Y coordinates (Lopez-Dahab) and common Z (only one Z coordinate)
- **Minimize storage**: Only 5 registers (with mult/add/square unit) or 6 registers (with mult/add-only unit)

Computation needs



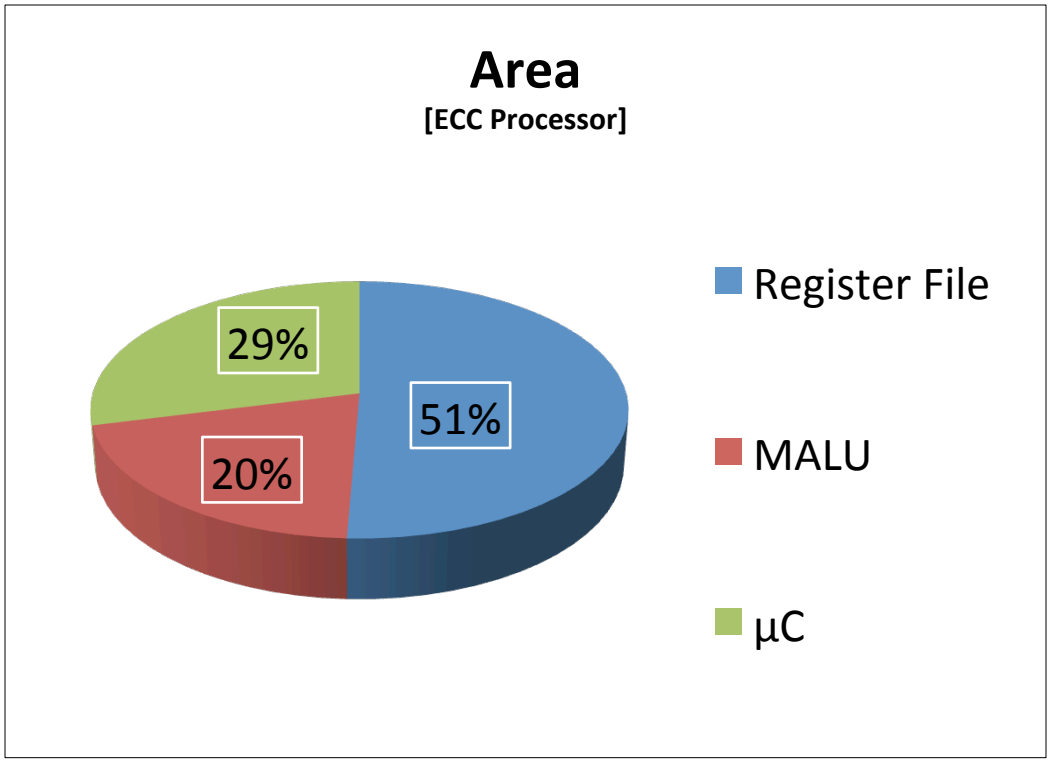
- One (simple) Schnorr protocol requires **one** elliptic curve point multiplication (compared to **two** on the reader's side)
- With modified Lopez –Dahab common Z coordinate, one point addition and point doubling requires **7** field multiplications, **4** squarings
- One field multiplication requires 163/d clock cycles (d= digit size).
- For digit size 4, 79000 cycles (should stay below 100K)

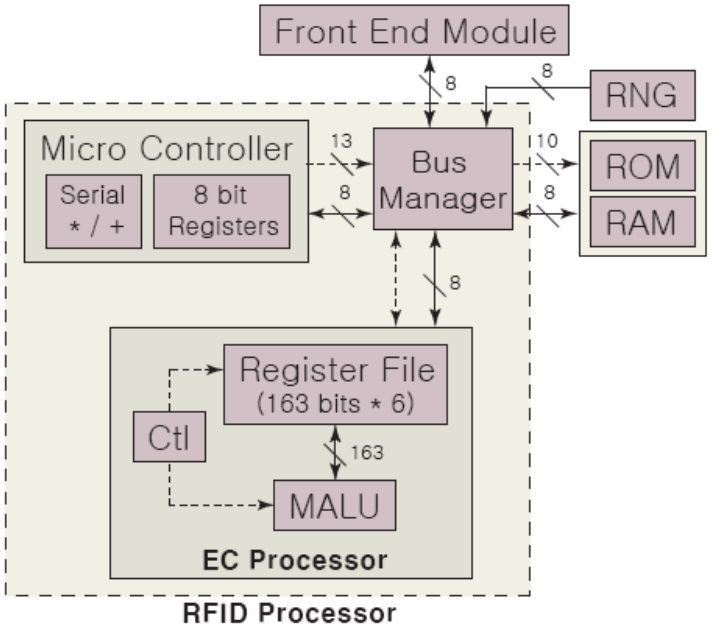
Step 3: EC Point Multiplication



* GE: Gate Equivalent (a 2-input NAND)

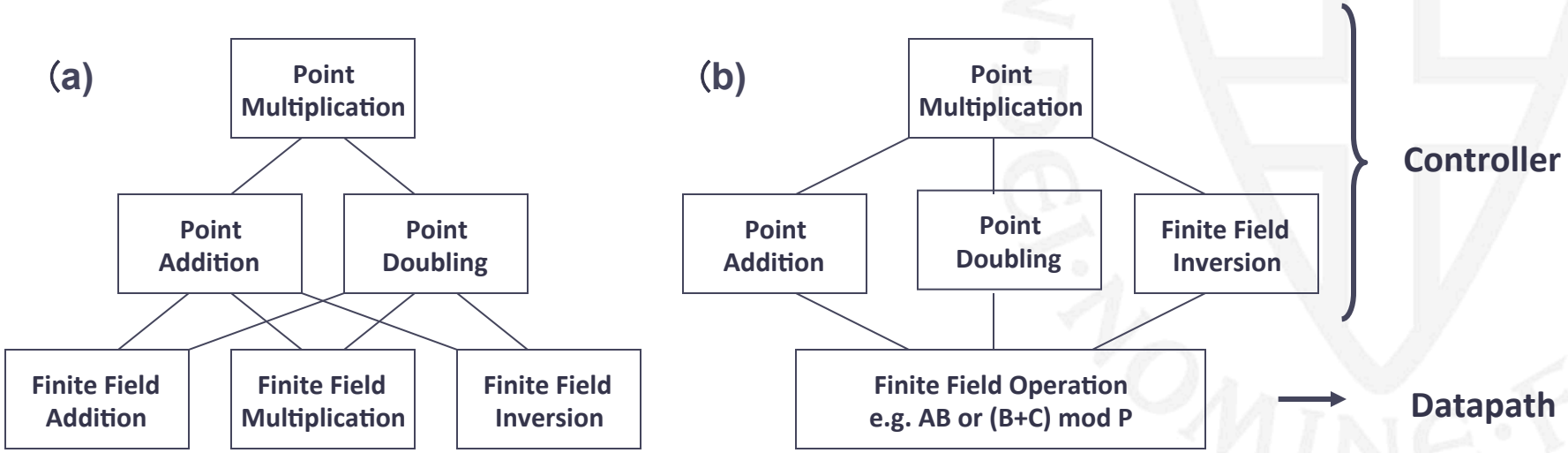
Example: compact ECC processor





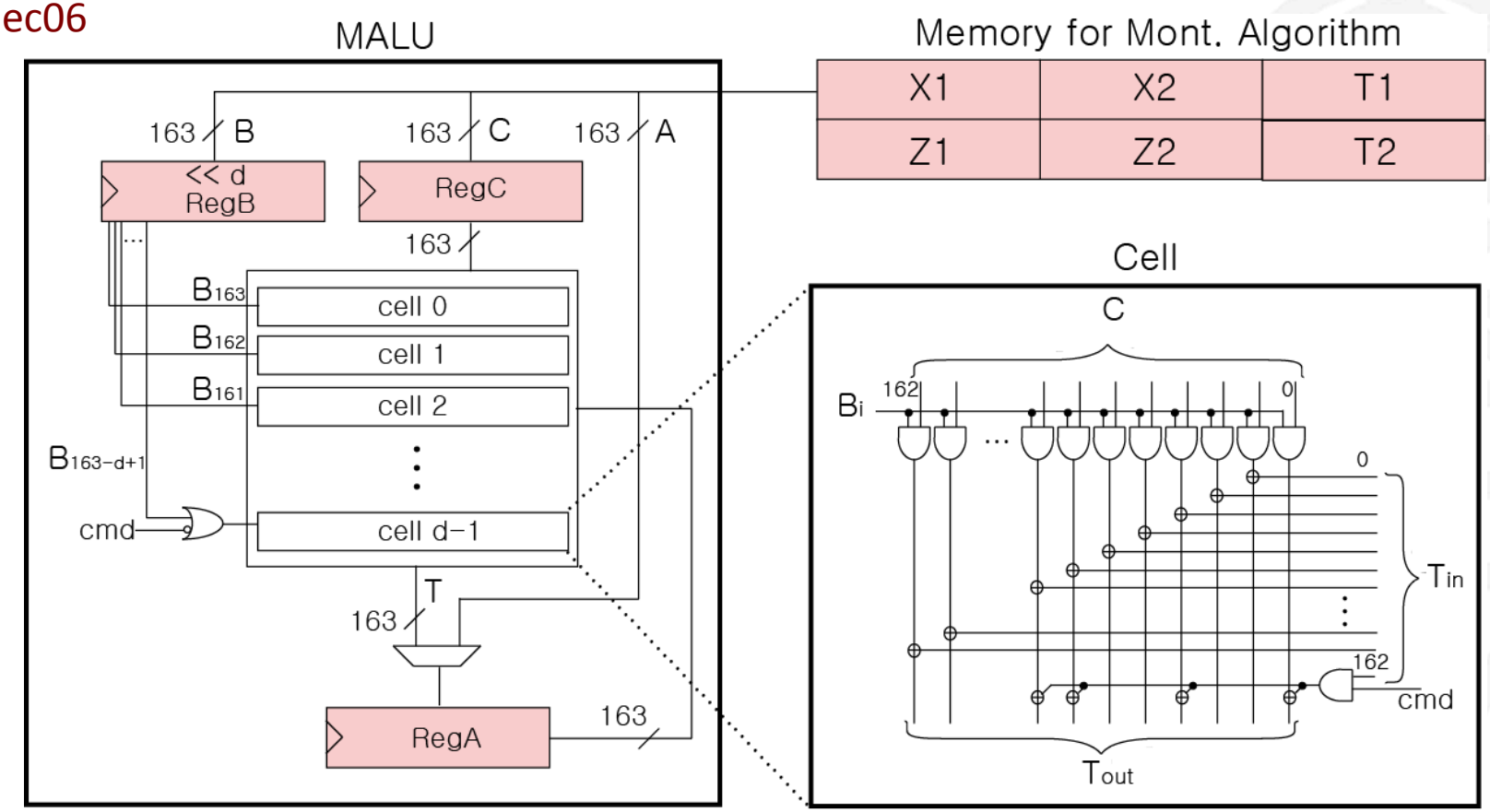
ECC operations: Hierarchy

- ECC computes point multiplication, kP
  - (a) Conventional hierarchy
  - (b) Compact datapath architecture



MALU: arithmetic unit for ECC processor

RFIDSec06

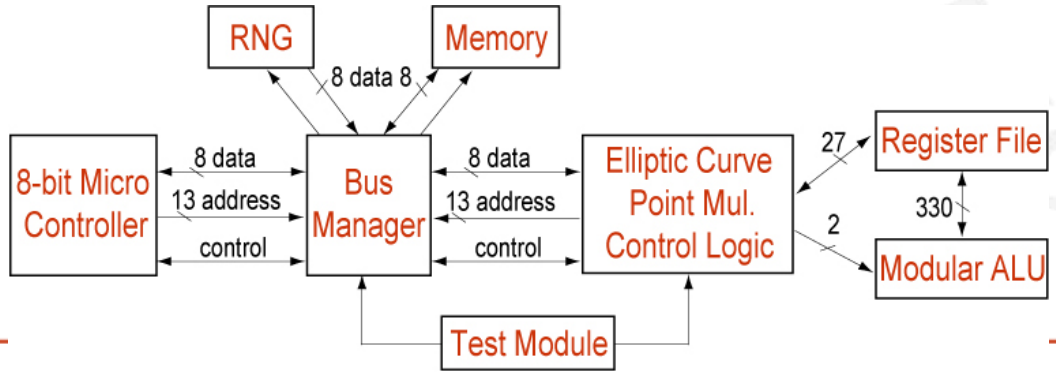


The required registers for MALU : A, B, C (**3 registers**)

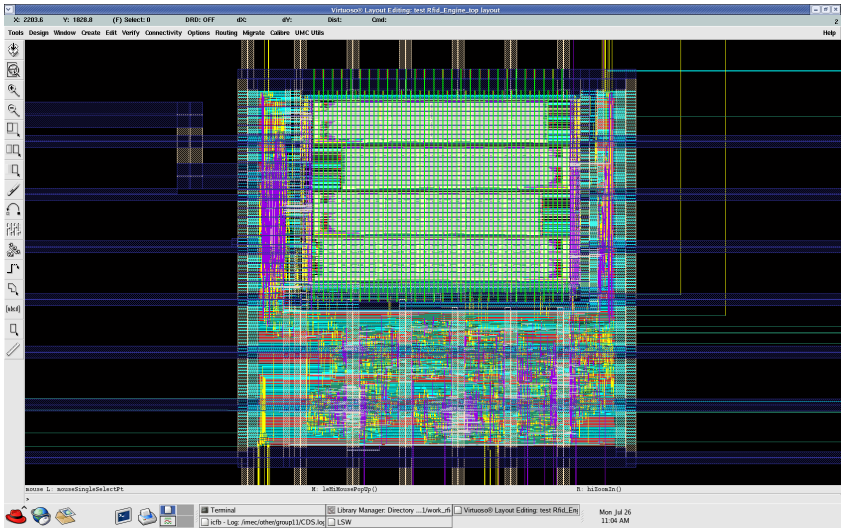
Registers for Algorithm : **6 registers**

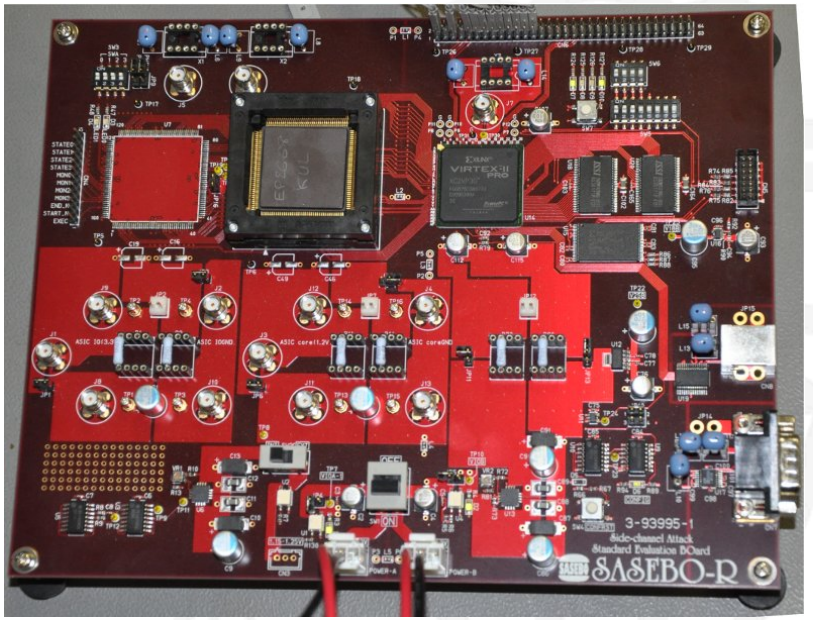
Results

- Results: ECC co-processor that can compute:
  - ECC point multiplications (163 by 4)
  - Scalar modular operations (8 bit processor with redundancy)
- Schnorr: **one** PM = 84224 cycles
- More advanced protocols: up to **four** PM on tag
- area = 0.54 mm^2
- At 847.5 KHz, corresponds to 50.4 µWatt (at V_{dd}= 1 V) and 9.8 PM per sec
- One point multiplication = **5.1 µJoule**



RFID co-processor prototype





- Combination full-custom – standard cells
- HW and SW co-design
- Side channel testing

What can we do with 1 microJoule energy

- 110 000 bits KATAN64 (80 bits of security)
- 11 000 bits AES encryption
- 500 bits SHA3 hash
- 1/5 of one point multiplication

- PK remains awfully expensive, but it gives more

IRMA card

www.irmacard.org

Digital Credentials in Use

Credential: “a document or certificate proving a person's identity or qualifications.” [New Oxford American Dictionary]

Credential: “an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so”. [Wikipedia]

- Username / Password
- Token
- Biometrics
- Certificate on a public key
- Attribute certificate

A case for ABC in Holland

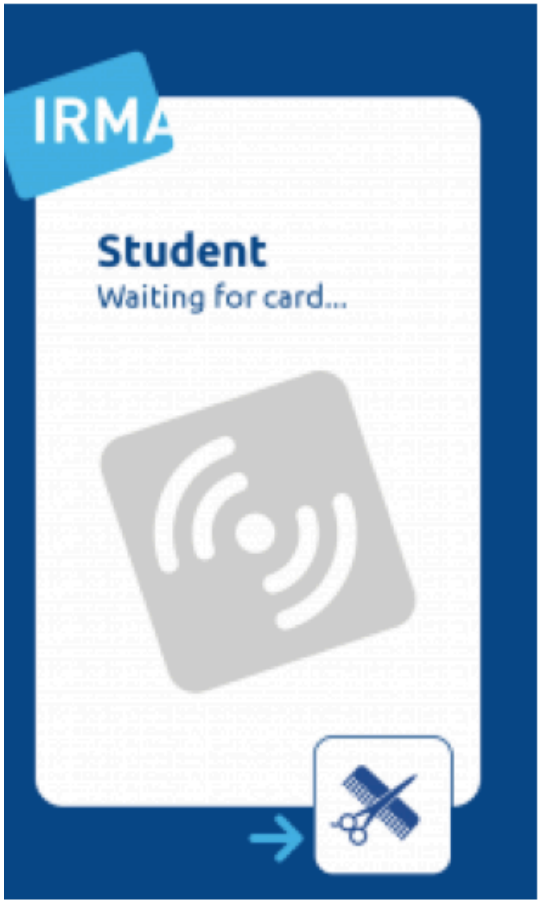
I Reveal My Attributes

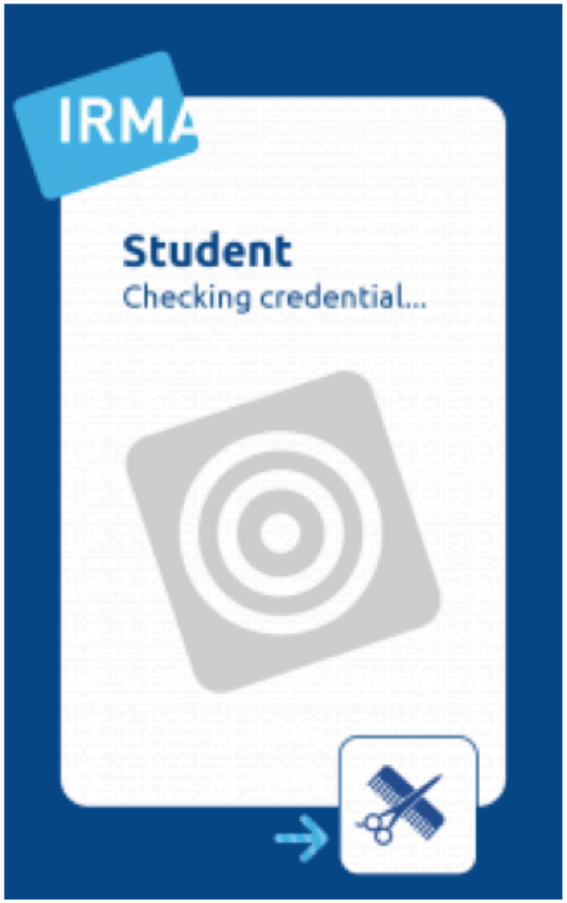
- Radboud University Nijmegen, Digital Security
- Pilot project and Proof of Concept
- Objective: Broad applicability
- Some simplifications
- Smart-card based (Idemix)
- Security, privacy, efficiency, usability
- Open approach

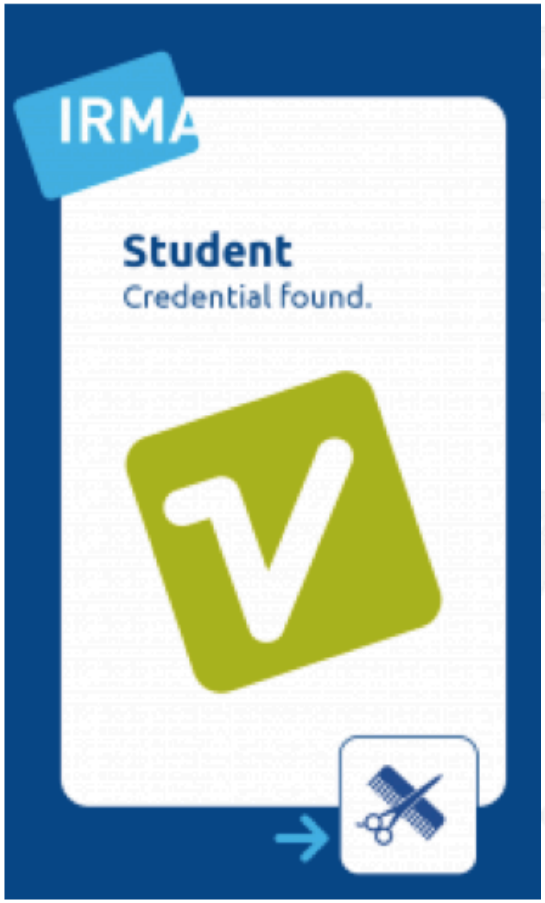
IRMA card

- name and date of birth are stored as attributes
- an IRMA card can communicate to computers via card readers or directly using the NFC technology

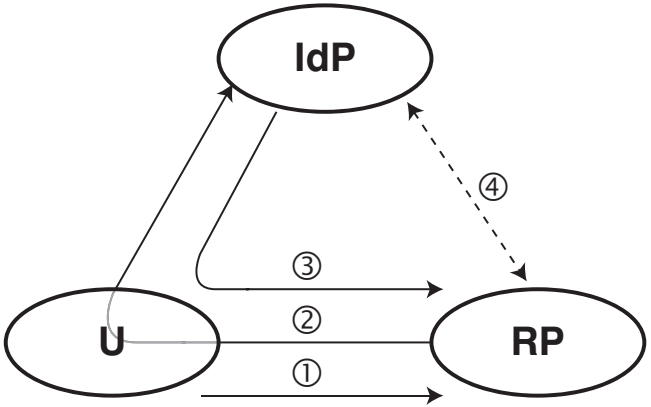
How does it work







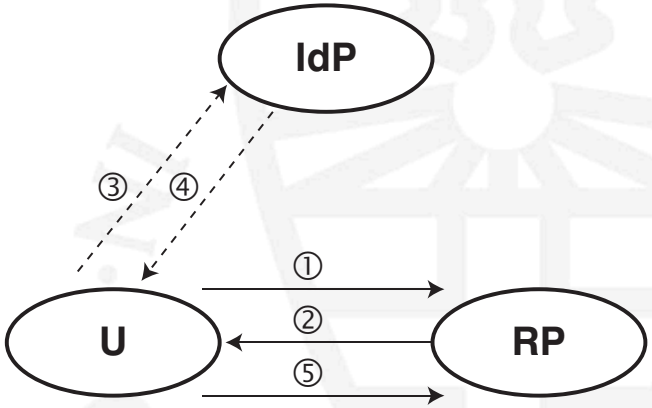
Credential Flow



① request service
② authenticate at IdP
③ authentication result

optional step
④ *exchange additional info*

network-based



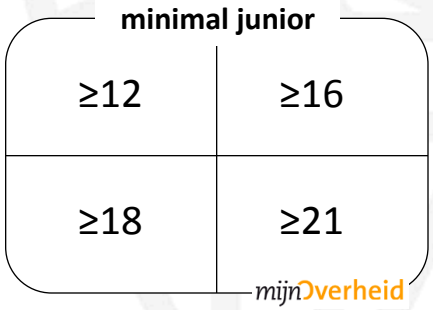
'cachable' steps
③ *authenticate*
④ *send claims*

① request service
② send policy
⑤ supply claims

claim-based

Use Cases

- Student card credential
  - Printing and cheap coffee
- Age credential
  - offline (supermarket)
  - online (video)
- Account credential
  - log in



Technical details and performance

- Implementation of selective disclosure functionality
- MULTOS card with Infineon SLE78 chip
- Selective disclosure: 0.75-1.3 sec
- Issuing credentials: 1.75-1.8 sec (depending on the number of attributes)

Pim Vullers, and Gergely Alpár. Efficient Selective Disclosure on Smart Cards using Idemix, Policies and Research in Identity Management, 3rd IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013.

References

- Gergely Alpár and Bart Jacobs. Credential Design in Attribute-Based Identity Management. In Bridging distances in technology and regulation, pages 189-204, 3rd TILTing Perspectives Conference, Tilburg, NL, 2013.
- Gergely Alpár, Lejla Batina, Wouter Lueks. Designated Attribute-Based Proofs for RFID Applications, In RFID Security and Privacy (RFIDsec), LNCS 7739, Nijmegen, The Netherlands, pages 59–75. Springer, 2012.
- Stefan A. Brands. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, MA, USA, 2000.
- Julien Bringer, Herve Chabanne, and Thomas Icart. Cryptanalysis of EC-RAC, a RFID Identification Protocol. Cryptology and Network Security, volume 5339 of LNCS, 2008.
- Y. K. Lee, K. Sakiyama , L. Batina, and I. Verbauwhede, Elliptic Curve Based Security Processor for RFID. IEEE Transactions on Computers, 57(11), pp. 1514-1527, 2008.
- Gergely Alpár, Lejla Batina, Roel Verdult. Using NFC Phones for Proving Credentials, PILATES 2012, LNCS 7201, Kaiserslautern, Germany, 2012.
- K. Sakiyama, L. Batina, N. Mentens, B. Preneel, and I. Verbauwhede, Small-footprint ALU for public-key processors for pervasive security, In *Workshop on RFID Security 2006*, 12 pages, July 12-14, 2006, Graz, Austria.
- Junfeng Fan, Oscar Reparaz, Vladimir Rožić , Ingrid Verbauwhede, Low-Energy Encryption for Medical Devices: Security Adds an Extra Design Dimension, DAC 2013.
- Pim Vullers, and Gergely Alpár. Efficient Selective Disclosure on Smart Cards using Idemix, Policies and Research in Identity Management, 3rd IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013.

Thank you for your attention!