Security Protocols for Mobile Ubiquitous E-Health Systems

Pablo Picazo-Sanchez

ppicazo@eui.upm.es

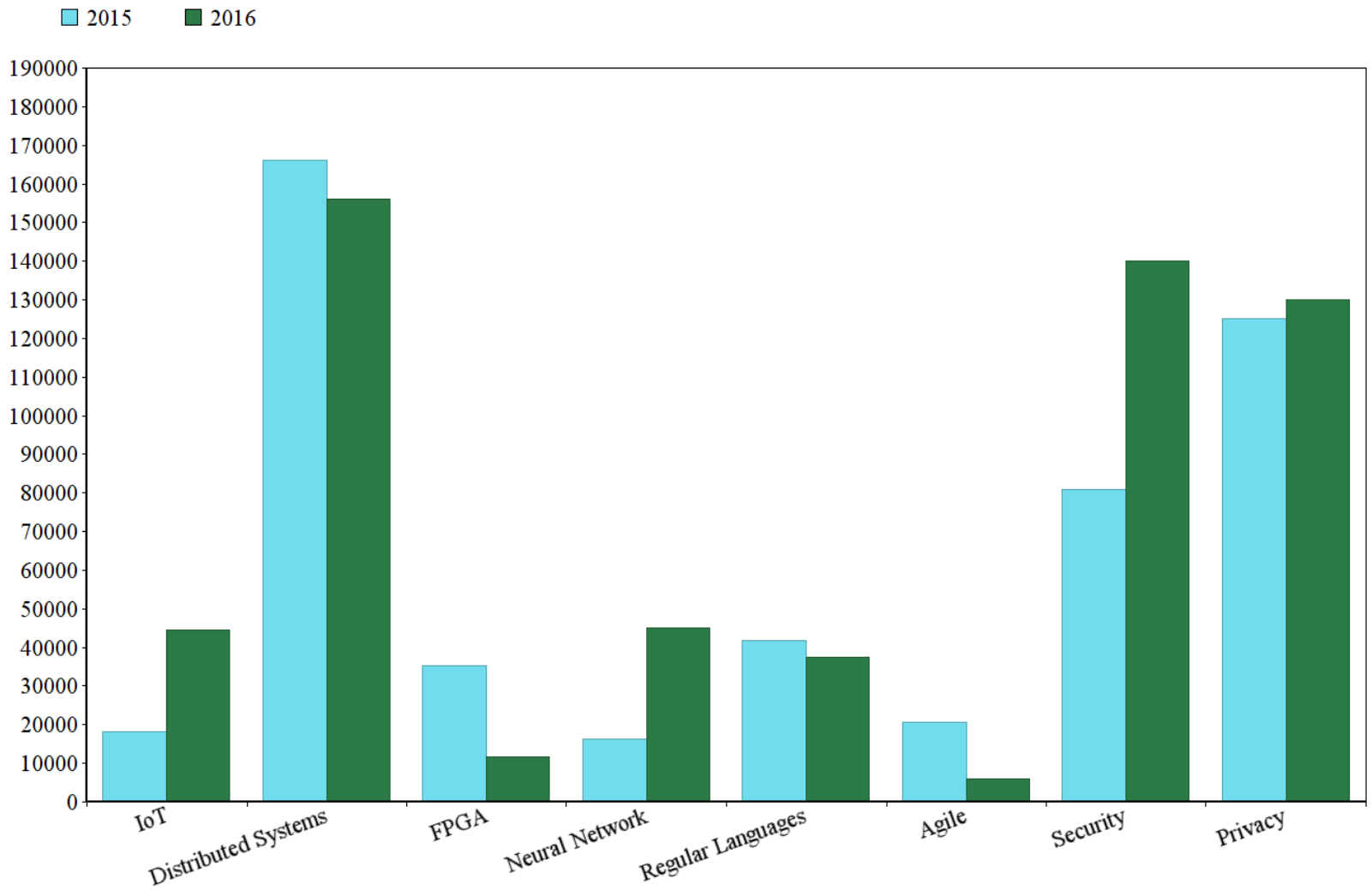
April 18, 2016

Overview

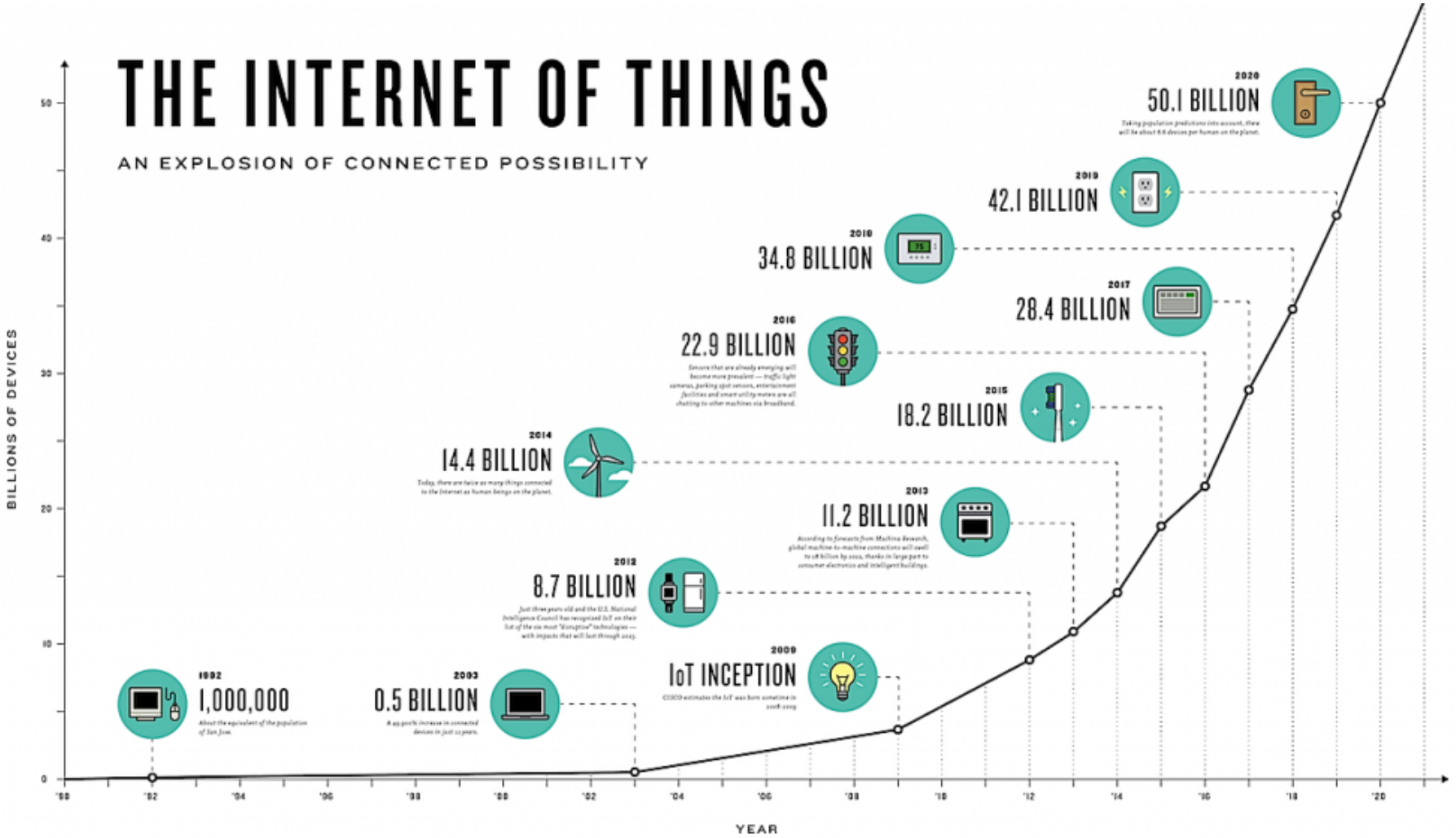
1. Introduction
2. RFID Protocols in Healthcare Environments
3. Secure Publish-Subscribe Protocols for Heterogeneous Medical WBANs
4. Decentralised Ciphertext Attribute-Based Encryption with Keyword Search (DCP-ABSE)
5. Conclusions

Introduction

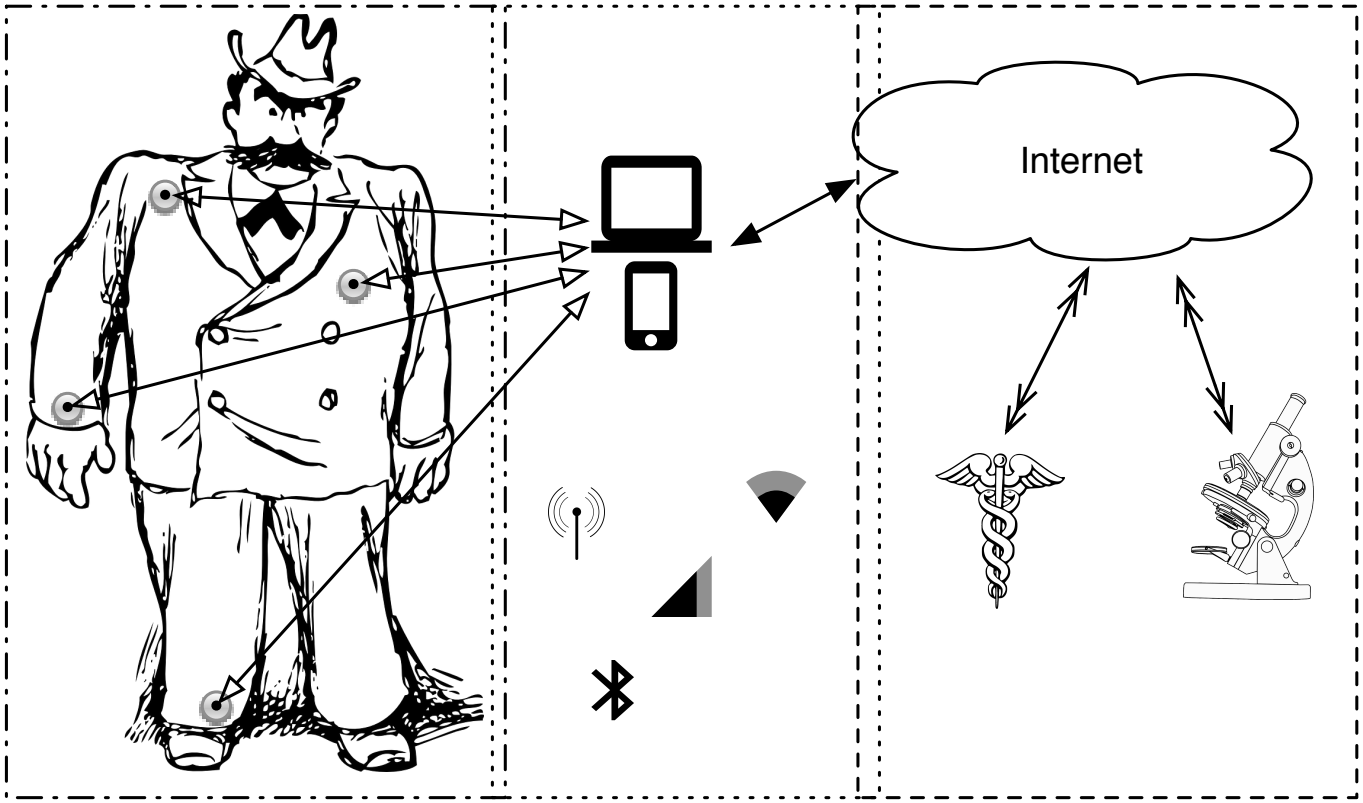
State of the Art



IoT


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
YEAR
1992
1,000,000
2003
0.5 BILLION
2009
IoT INCEPTION
2012
8.7 BILLION
2013
11.2 BILLION
2014
14.4 BILLION
2015
18.2 BILLION
2016
22.9 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION

IoT - Healthcare



Six Nations Rugby championship 2015, in a stadium equipped with a WiFi connection and millions of data were measured directly from the players.

IoT - Healthcare Applications

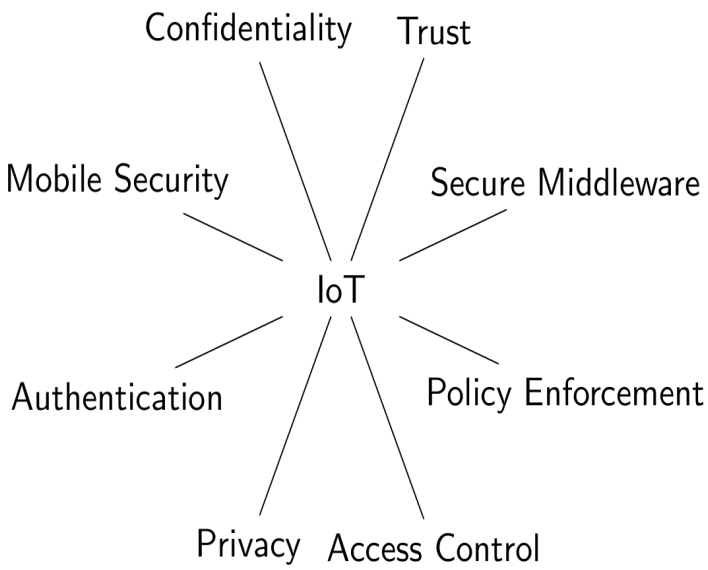
Patient Traceability	[Najera, 2011, Yao, 2010]
Asset Management	[Oztekin,2010, Qu,2011]
Medication Administration	[Aronson, 2009, Yen, 2012]
Handling Errors	[ChanChoi,2012, Parlak,2012]
Ownership Transfer Procedures	[Yang,2012, Zhou,2012]
Efficiency Management	[Parlak,2012, Yao,2011]
Cost Savings	[Bunduchi,2011, Yao, 2010]

Table: Some IoT applications in healthcare environment

Just born abduction

It is claimed that in the last 50 years more than 300,000 newborns were abducted in Spain. Similar cases have been reported in Australia or USA.

IoT - Security Issues



Cybersecurity

- The worldwide cybersecurity market: from $75 billion in 2015 to $170 billion by 2020 (Gartner).
- Cyber attacks costing businesses $400 billion to $500 billion + a year (Lloyds).
- $1-per-Thing is a starting point (Cybersecurity Market Report).

Electronic Health Records Hacked

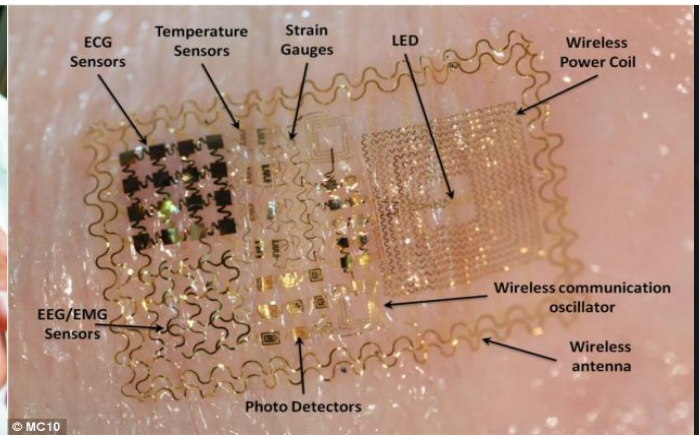
As a recent example, in 2010 personal data from more than 26 millions of veterans were stolen from the Department of Veterans Affairs database in the US by an employee who had access to the database

RFID Protocols in Healthcare Environments

Introduction

RFID EPC Generation 1 Class 2 standard

- Tags are passive.
- UHF band (860960 MHz) up to 10m.
- High constrained resources and storage capabilities.
- 16-bit for PRNG and for Cyclic Redundancy Code checksum.
- Traditionally, not enough footprint for standard cryptographic primitives.
- Still a problem but not that acute.



Motivation

Khor *et al.*'s proposal

- Khor *et al.* proposed an authentication protocol named Fingerprint in [Khor,2011] EPC-G1C2 compliant.
- Impersonation, traceability, de-synchronization, DoS and full disclosure attacks.

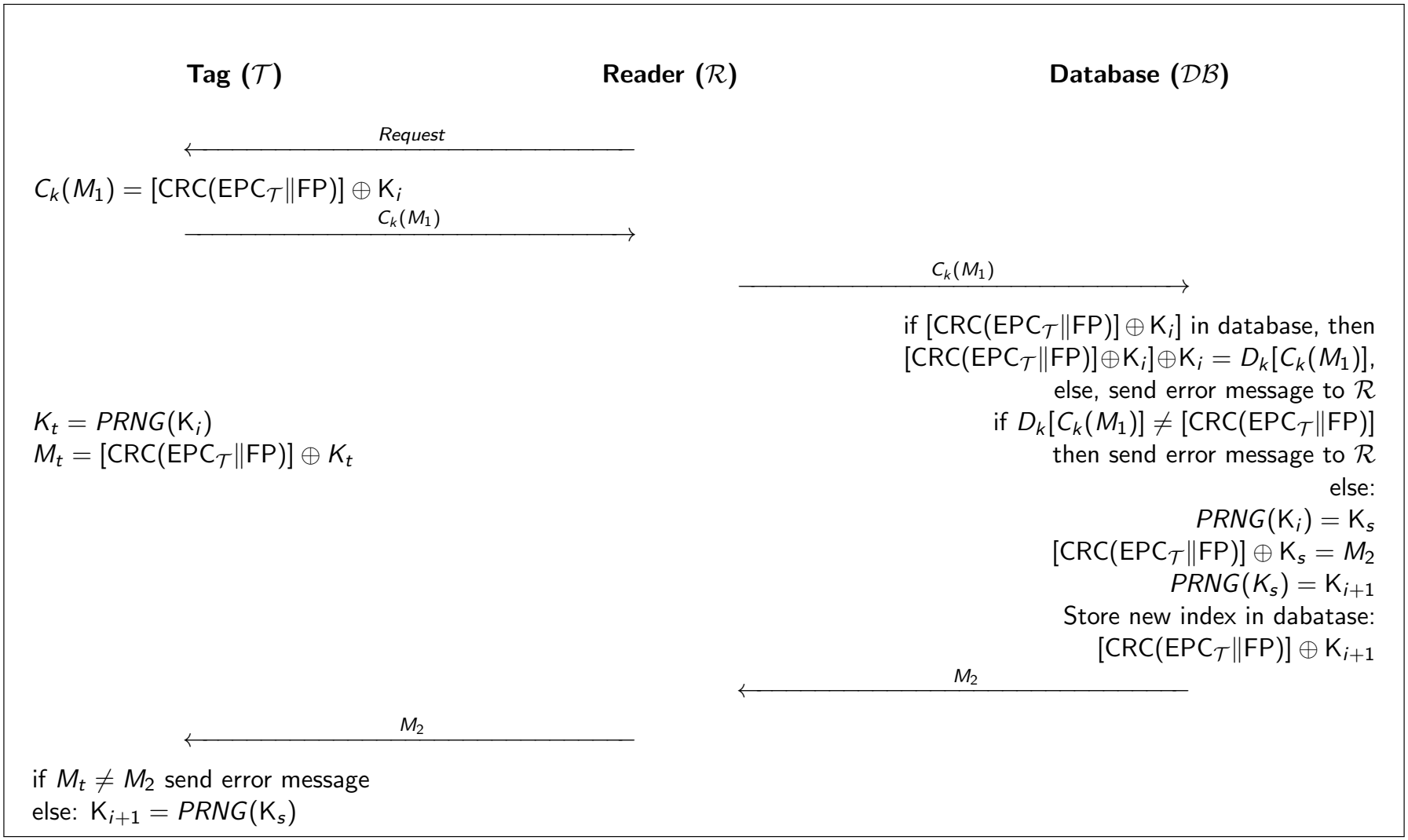
Wu *et al.*'s proposal

- Wu *et al.* proposed an authentication protocol in [Wu, 2013].
- This protocol is vulnerable to a traceability attack that allows an adversary to compromise the location privacy

Objective

- To cryptoanalyze both Khor *et al.* and Wu *et al.* proposals.
- Propose new improved protocols.

Khor *et al.* - Authentication phase



Khor *et al.* - Desynchronization Attack

Adversary's goal

$\mathcal{T}$ and $\mathcal{DB}$ will be desynchronized if both have different keys. This will make future authentications infeasible.

Authentication protocol pitfall

Fingerprint protocol does not use any mechanism for recovering from desynchronized states. $\mathcal{A}$ performs the next steps:

1. Forwards $C_k(M_1)$ to $\mathcal{R}$ and passes M_2 message to $\mathcal{T}$.
2. Simulates the incorrect reception of M_2 and sends an error message to $\mathcal{R}$.
3. Finally, $\mathcal{T}$ updates its K_i while the back-end server does not update it.

Khor *et al.* - Traceability Attack

Adversary's goal

$\mathcal{A}$ tries to establish a link between $\mathcal{T}$ and the bearer so she is going to be tracked wherever she goes.

Relay Attack

$\mathcal{A}$ captures the M_2 message sent to $\mathcal{R}$, alters it and sends it to $\mathcal{T}$ in order to avoid the key updating phase and thus a constant value will always be used.

Desynchronization Attack

$\mathcal{A}$ performs a desynchronization attack so that $\mathcal{T}$'s bearer is always using the same values $[\mathrm{CRC}(\mathrm{EPC}_{\mathcal{T}} \| \mathrm{FP})] \oplus \mathrm{K}_i$

Khor *et al.* - Full Disclosure Attack

$2^{16} - 1$ computations

PRNG outputs 16-bit values to be compliant with EPC-G1C2 standard.

Both channels

```
for i in range( 2^16 - 1 ):
    #i = CRC(EPC_T ⊕ FP)
    K̂_i = C_k(M_1) ⊕ i
    M̂_2 = i ⊕ PRNG(K̂_i)
    if M̂_2 == M_2 :
        return K̂_i, i
```

One channel

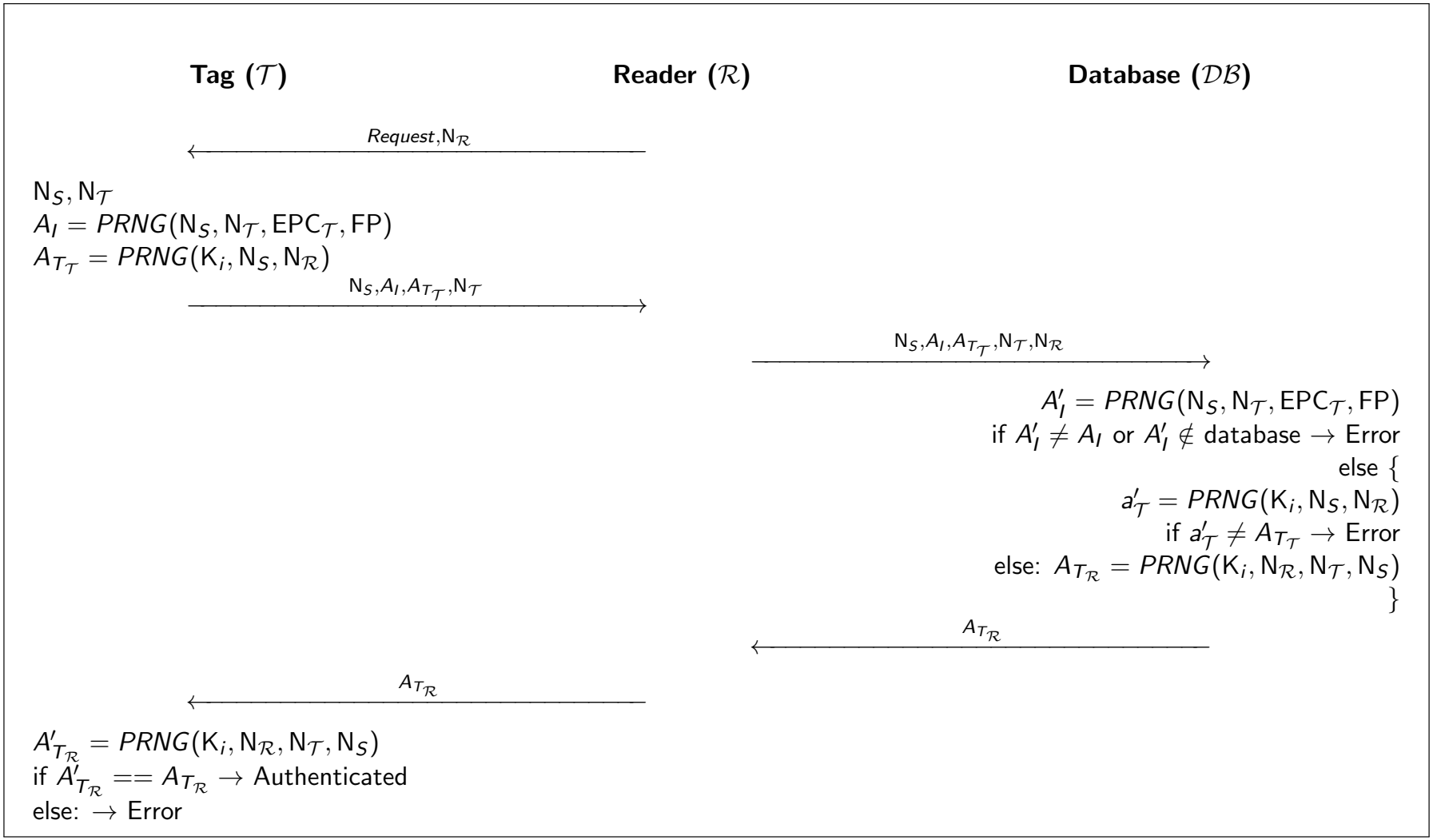
$M_{2_m} = [CRC(\text{EPC}_{\mathcal{T}} \oplus \text{FP})] \oplus \text{K}_i$

$M_{2_{m+1}} = [CRC(\text{EPC}_{\mathcal{T}} \oplus \text{FP})] \oplus \widehat{\text{K}_i}$

$\#\widehat{\text{K}_i} = PRNG(\text{K}_{i+1}) = PRNG^2(\text{K}_i)$

```
for i in range( 2^16 - 1 ):
    Aux= M_{2_{m+1}} ⊕ M_{2_m}
    if (Aux == (i ⊕PRNG^2(i) )) :
        return Aux, i
```

Improved Protocol: Fingerprint$^+$



Wu *et al.* - Notation

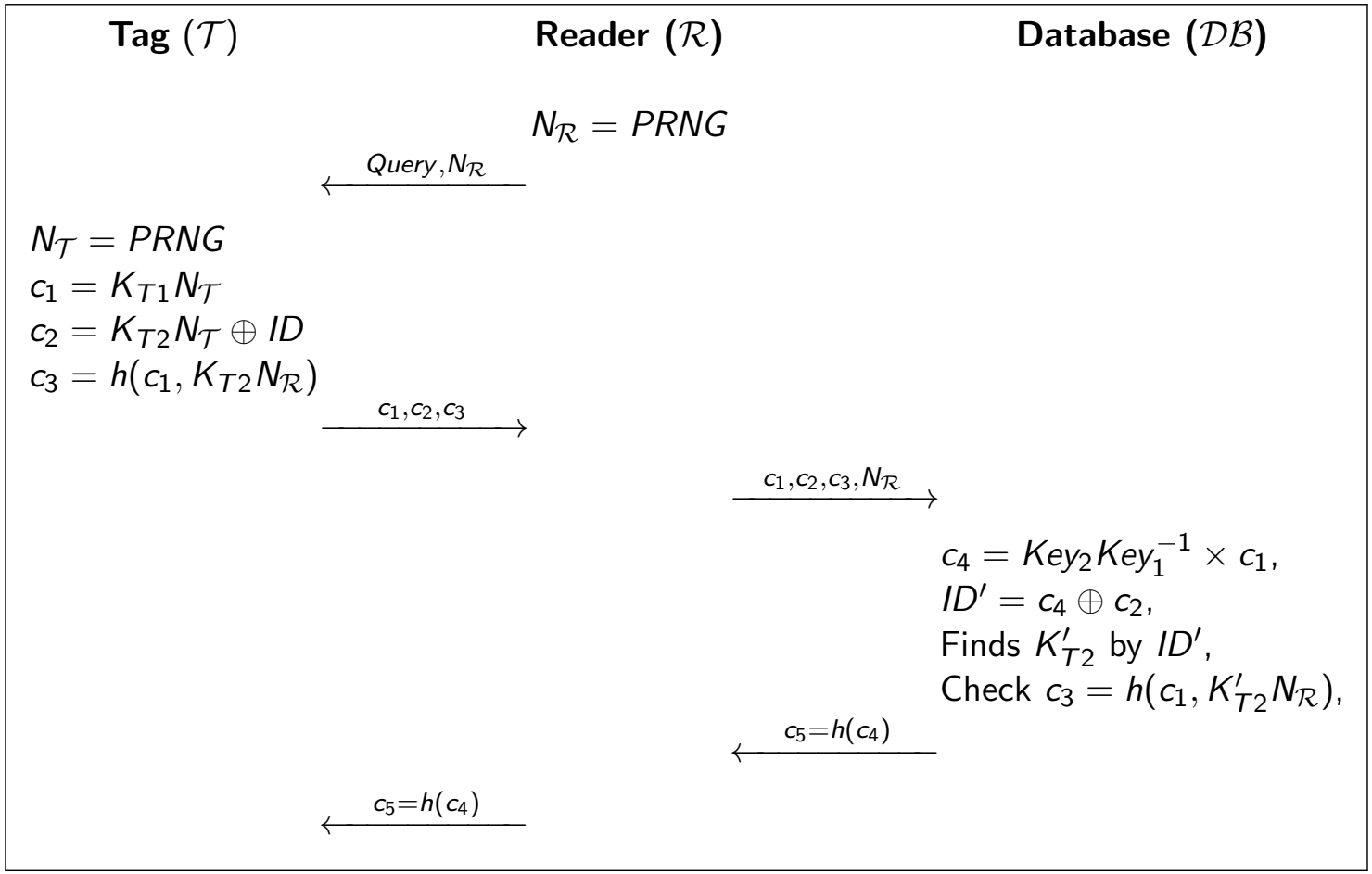
Wu *et al.* have recently proposed a new RFID authentication protocol for healthcare environments [Wu, 2013].

- Two different phases: setup and execution.
- In the Setup phase, server generates:
  - A nonsingular binary matrix Key_1 of size $d \times d$
  - A binary matrix Key_2 of size $d \times d$
  - A singular binary matrix Key_3 of size $d \times d$
  - A random matrix S_T of size $d \times d$
  - Two matrix keys for each tag: $K_{T1} = Key_1 Key_3 S_T$ and $K_{T2} = Key_2 Key_3 S_T$

Security & Privacy Issues

This protocol is vulnerable to a traceability attack that allows an adversary to compromise the location privacy

Wu *et al.* - Protocol



Wu *et al.* - Location Attack I

Assume that $(A)_i$ denotes the i-th column of matrix A. Let X and X' be random binary matrices of size $d \times d$, and Y and Y' fixed binary matrices of size $d \times r$.

1. If $(X)_i = (X')_j$ and $Y = Y'$, then $(Y \times X)_i = (Y' \times X')_j$ with probability 1.
2. If $(X)_i = (X')_j$ and $Y \neq Y'$, then $(Y \times X)_j = (Y' \times X')_j$ with probability 2^{-d}.

In particular we have $c_1 = K_{T1} N_{\mathcal{T}}$ and $c_2 = K_{T2} N_{\mathcal{T}} \oplus ID$. Thus, if $(N_{\mathcal{T}})_i = (N'_{\mathcal{T}})_j$ then:

$$(K_{T1} N_{\mathcal{T}})_i = (K_{T1} N'_{\mathcal{T}})_j$$

$$(K_{T2} N_{\mathcal{T}} \oplus ID)_i = (K_{T2} N'_{\mathcal{T}} \oplus ID)_j$$

Wu *et al.* - Location Attack II

Learning Phase:

1. $\mathcal{A}$ generates a matrix Tab of size N sessions. At each run $1 \leq j \leq N$:
   - $\mathcal{A}$ sends $N_{\mathcal{R}}^{j}$ to the tag $\mathcal{T}$. It computes c_1^j and c_2^j and sends them back to $\mathcal{A}$ to store them in the $j-th$ row of Tab.

Execution Phase:

1. Given a tag $\mathcal{T}$', $\mathcal{A}$ generates a matrix Tab' proceeding exactly as in the learning phase.

Decision Phase:

1. Trivial when $(c_1)_i \in Tab = (c_1')_j \in Tab'$ and $c_2 \in Tab = c_2' \in Tab'$
2. $Pr[A^{\mathcal{T} \neq \mathcal{T}'} \Rightarrow 1] = \left(2^{-d}\right)^{(N \times r) \times (N' \times r) \times 2^{-d}}$

Wu *et al.* - Location Attack III

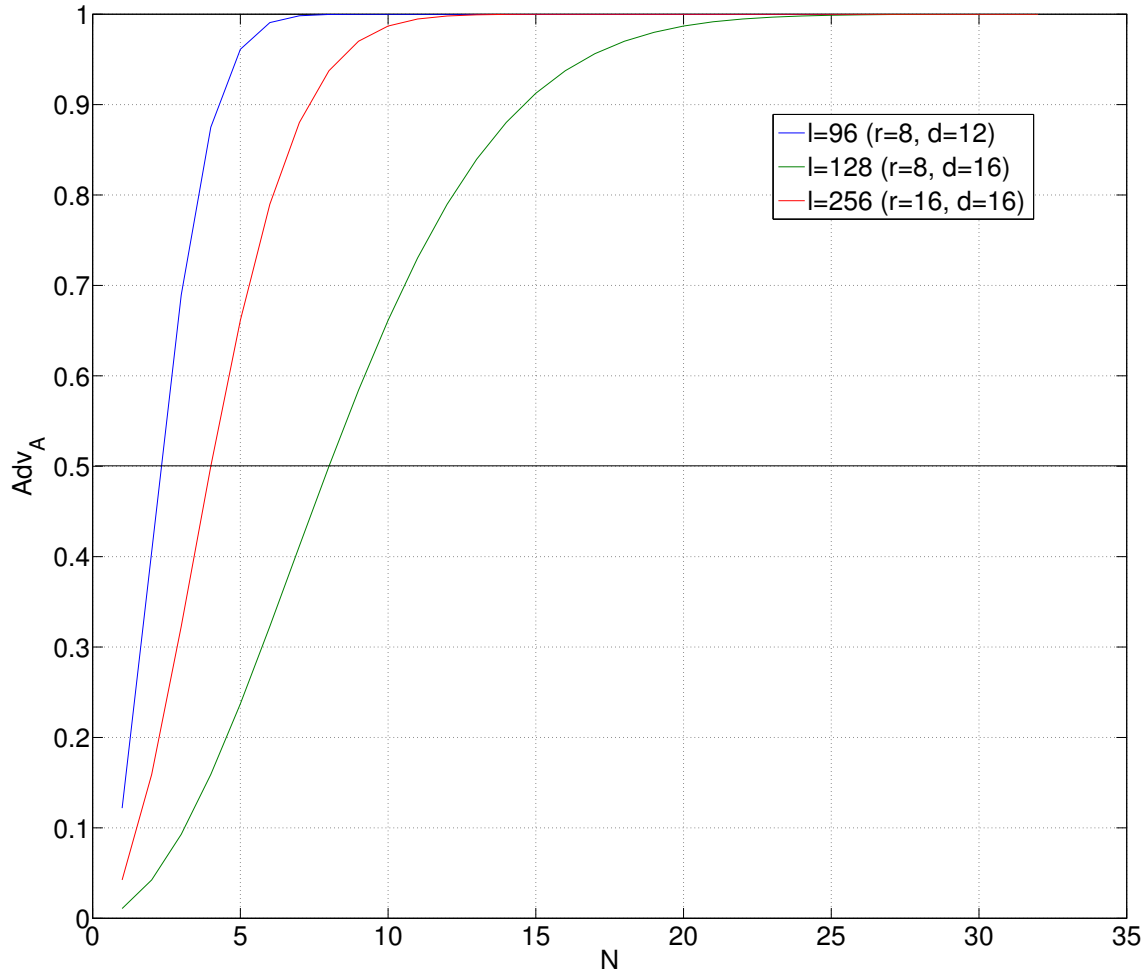
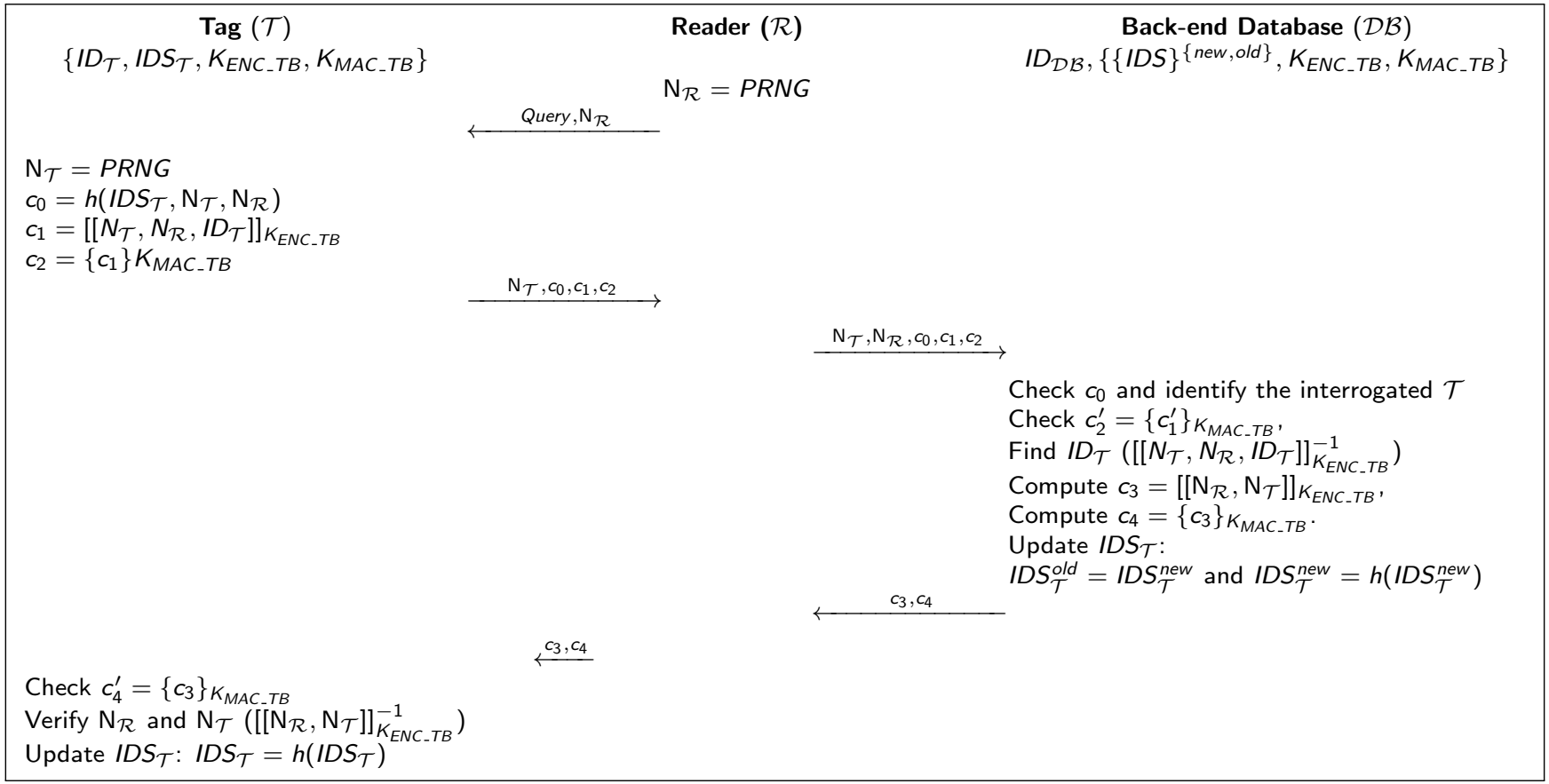


Figure: Probability of success of the location attack as a function of the number of eavesdropped sessions.

Proposal I: RFID Entity Authentication



Proposal II: IMD Secure Messaging Protocol I

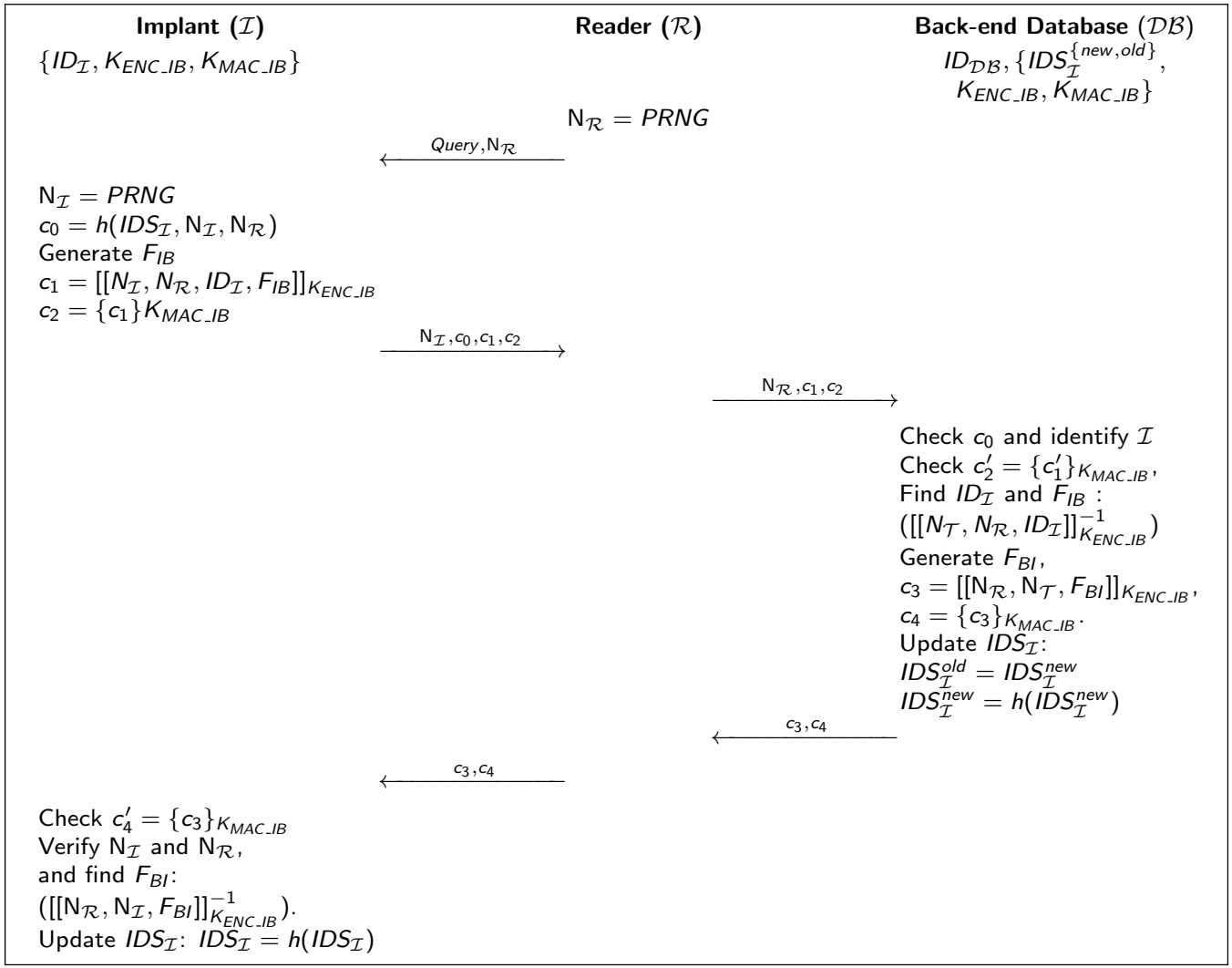


Figure: Mutual Authentication & Key Exchange [Picazo, 2014]

Proposal II: IMD Secure Messaging Protocol II

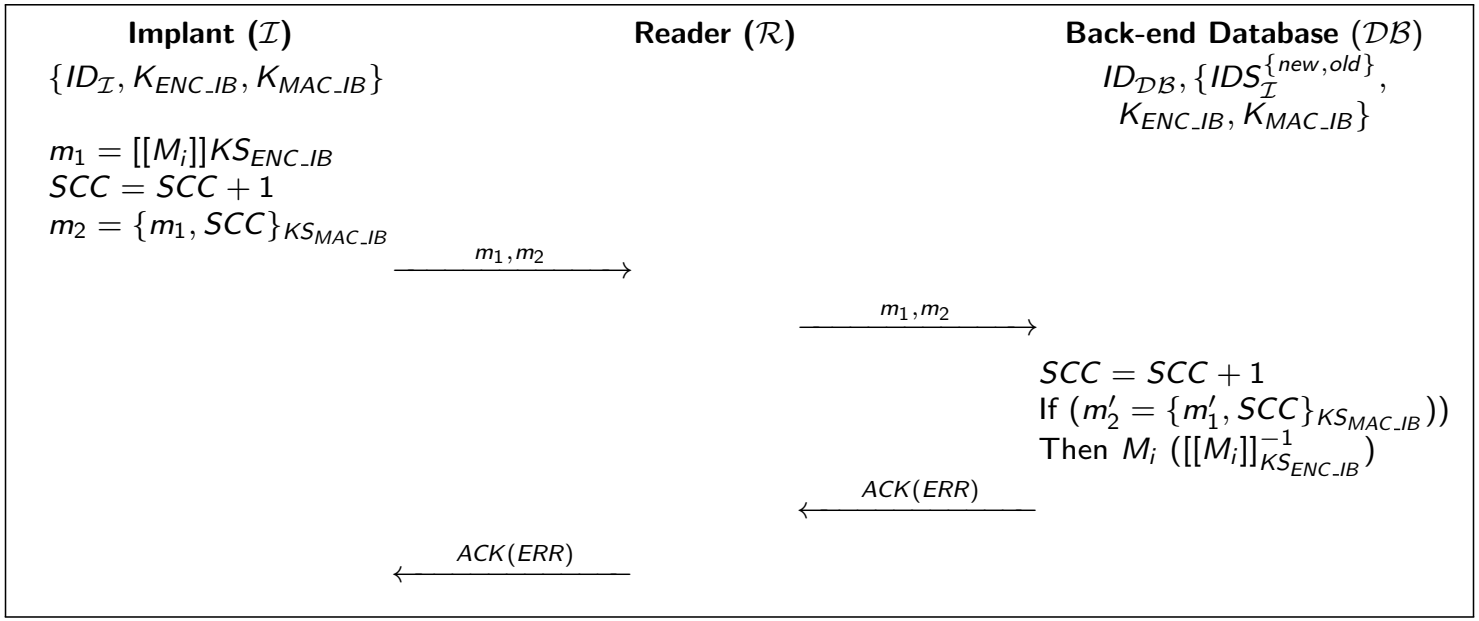


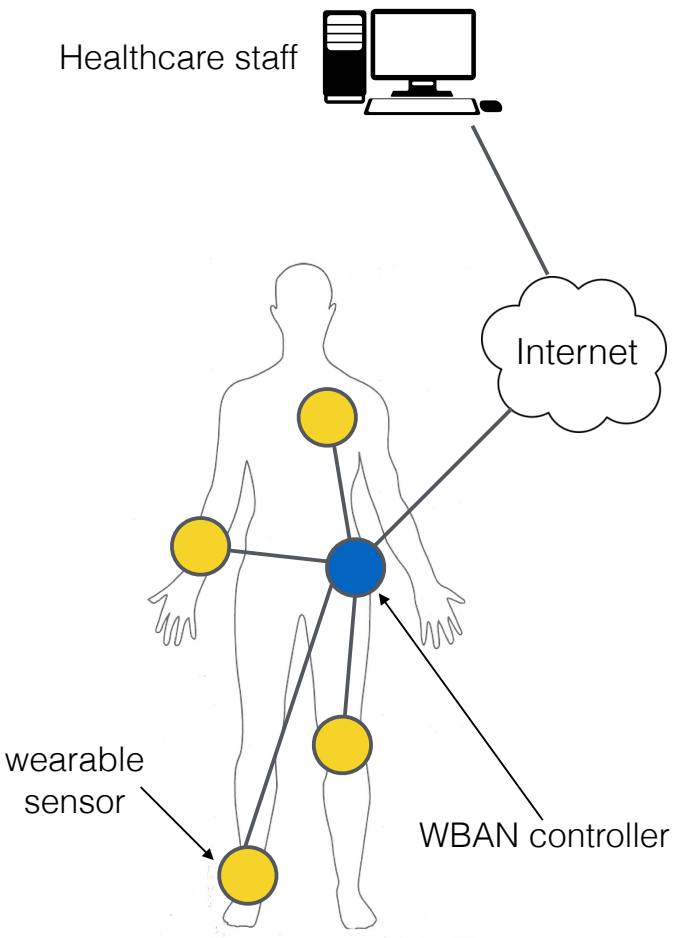
Figure: Secure Messaging [Picazo, 2014]

Conclusions

- An attacker, equipped with a domestic PC, can execute a full disclosure attack against Fingerprint protocol in only a few minutes.
- Fingerprint$^+$ solves all above issues and it is compliant with both ISO/IEC 9798-2 and EPC-G1C2 standards (equivalently ISO/IEC 18000-6C).
- Security of Fingerprint$^+$ has been formally proven using BAN logic.
- In general, security issues are due to two main reasons: (i) the use of non-standard constructions; and (ii) informal and/or non-rigorous security analysis.
- Two new RFID protocols for healthcare environments conformed to ISO/IEC 9798, 11770 and NIST recommendations have been proposed.

Secure Publish-Subscribe Protocols for Heterogeneous Medical WBANs

Motivation I



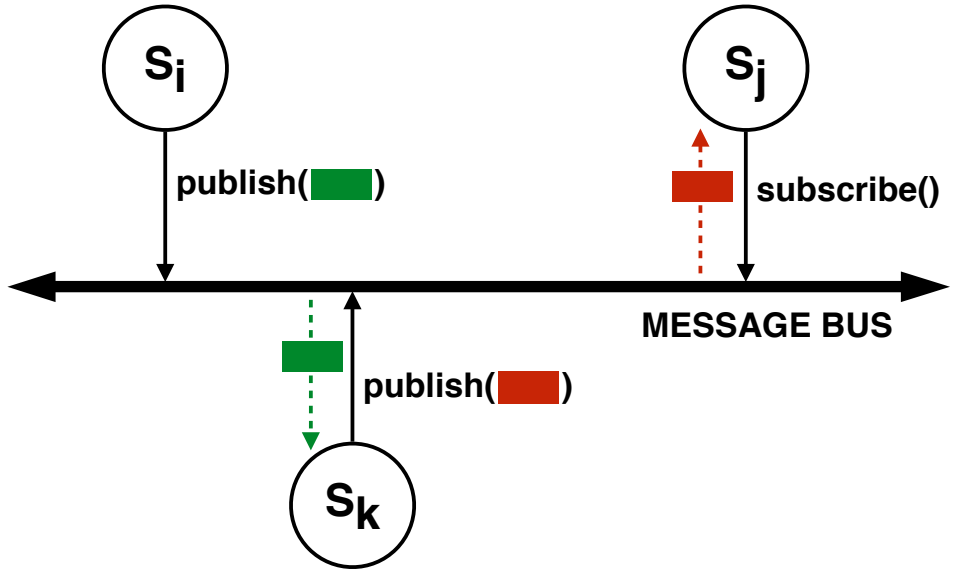
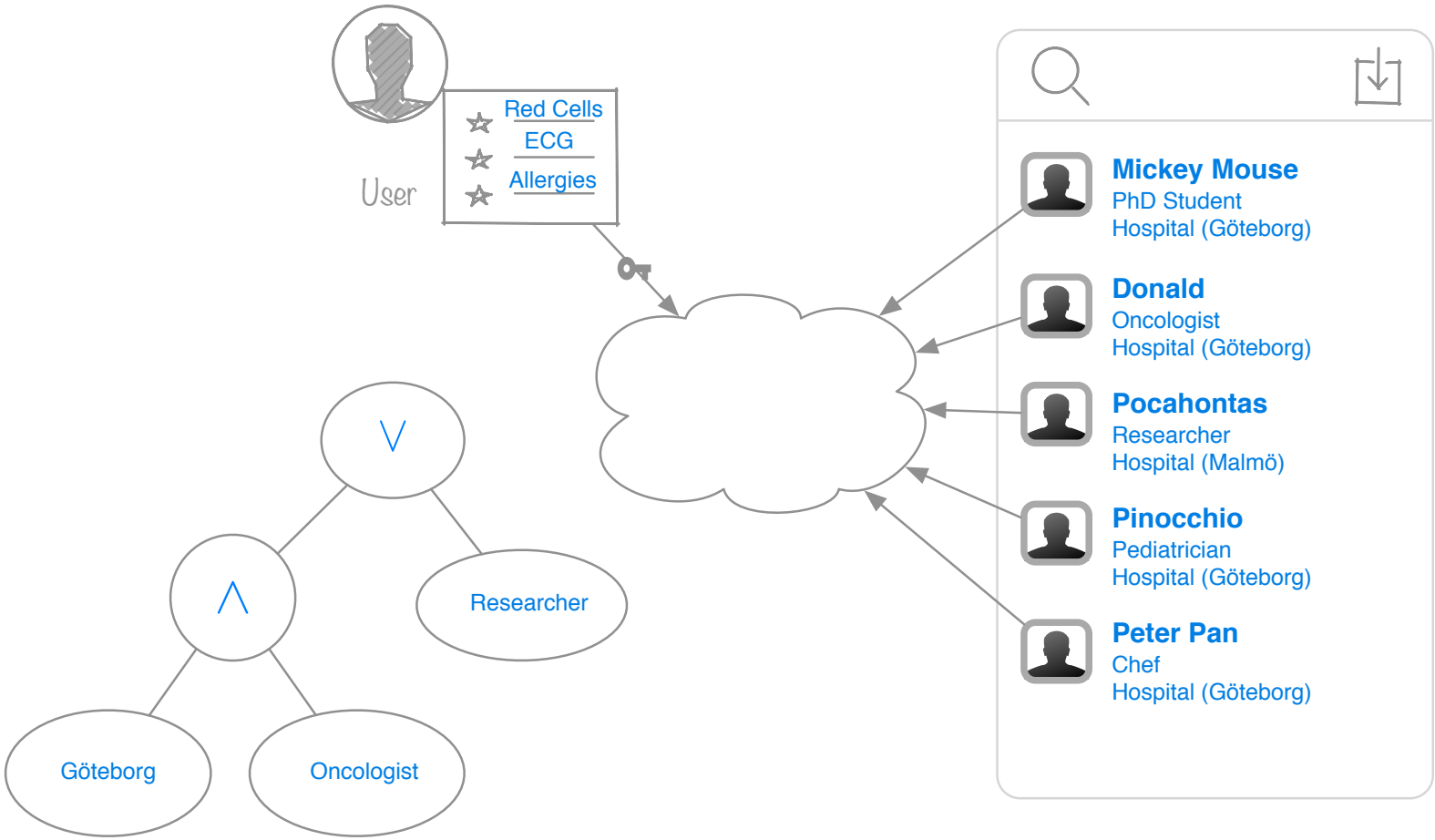


Figure: WBAN architecture: (a) physically as a network of wearable devices; (b) logically as a publish-subscribe messaging system.

Motivation II



(a) Attribute Based Encryption Example

Ciphertext-Policy Attribute Based Encryption

Pros

- Anyone can encrypt data under a given access policy $\mathcal{A}$
- Decryption performed only by users whose public attributes satisfy $\mathcal{A}$
- Based on ECC and thus $\rightarrow$ Decisional Discrete Logarithm Problem

Cons

- The more attributes the protocol has, the worse the performance is
- Decryption can be a computational demanding operation

Symmetric	RSA	ECC
56	512	112
80	1024	163
112	2240	233
128	3072	283
256	15360	571

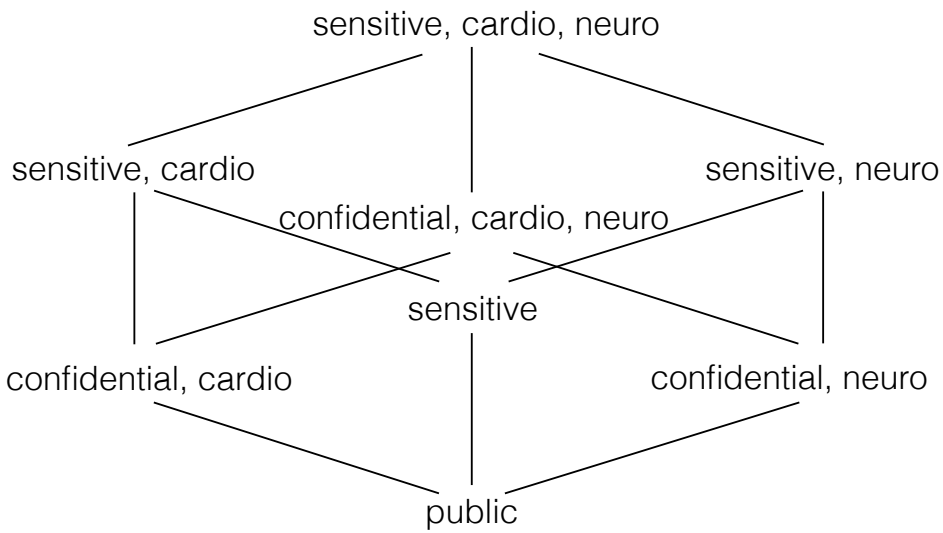
Table: Size in bits

RSA Size	RSA	ECC
1024	0.16	0.08
2240	7.47	0.18
3072	9.80	0.27
7680	133.90	0.64
15360	679.06	1.44

Table: Key Generation in seconds

Goals

- Based on [Guo, 2014]:
  - Only AND policies are supported.
  - Allow lightweight devices to run decryption CP-ABE.
  - CP-ABE with constant-size decryption keys independent of the number of attributes.
- 2 protocols: data sharing and reconfiguration mode
- Data encryption: symmetric scheme $\rightarrow$ AES [AES,2013]
- Keys encryption: asymmetric scheme $\rightarrow$ CP-ABE [Bethencourt, 2007]
- Lattice-based Access Control (LBAC) compliant



Publishers

$Sensor_i$ (S_i) publishes the access structure ($\mathcal{A}$):

$$\mathcal{A} = \text{PubPolicy(Data)}$$

Each sensor keeps a list of $\mathcal{A}$ and the associated access token (AT):

$$\text{AT} = \{id(k), \mathcal{A}, E_A(PK_{S_i}, K, \mathcal{A}), t_{exp}\}$$

S_i publishes Message $\mathcal{M}$ to the bus:

$$\mathcal{M} = \{S_i, t, id(k), E_K(Data \| t)\}.$$

$S_i \longrightarrow$ Sensor identifier

$\text{id}(k) \longrightarrow$ identifier of the AT (symmetric key) K.

$E_{\mathcal{A}}(PK_{S_i}, K, \mathcal{A}) \longrightarrow$ CP-ABE encryption of the symmetric key K.

$t_{\text{exp}} \longrightarrow$ Time after AT is no longer valid.

$t \longrightarrow$ Timestamp.

$E_K(Data \| t) \longrightarrow$ Symmetric encryption of $Data \| t$ using key K.

Subscribers

When a Subscriber (R) wants to access to a given data published on the bus:

Gets secret key K:

$$\mathrm{K} = Decrypt(PK_R, E_{\mathcal{A}}(PK_{S_i}, K, \mathcal{A}), SK_R)$$

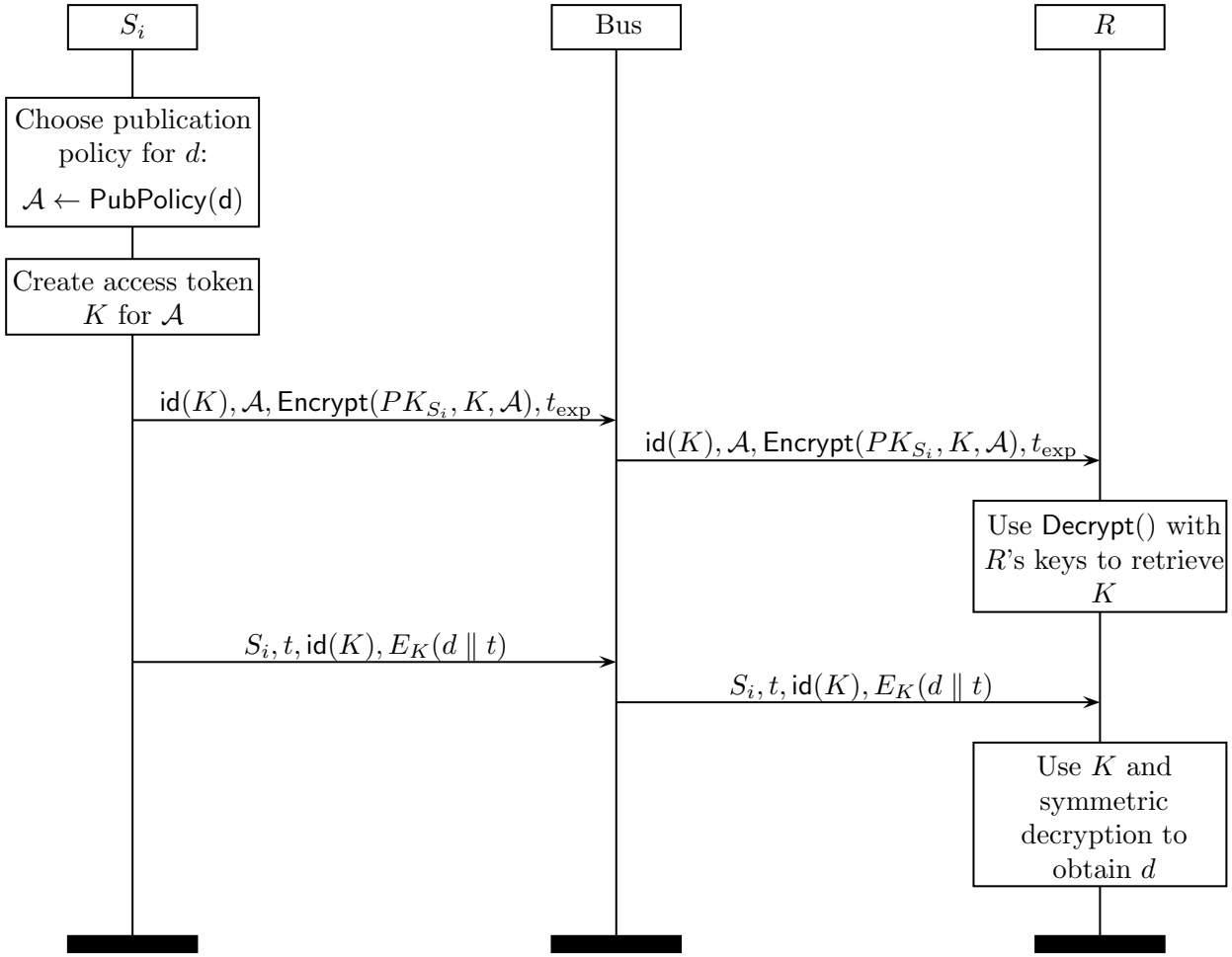
Decrypts Data with the secret key K:

$$Data \| t = D_k(E_k(Data \| t))$$

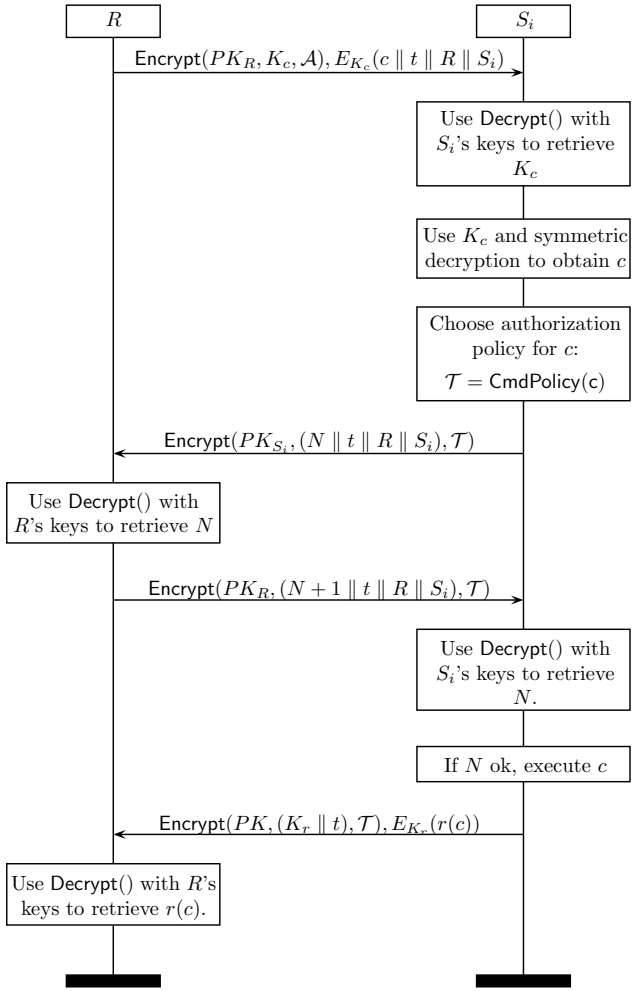
Checks whether both timestamps are equal:

$$t \stackrel{?}{=} t_{exp}$$

Scheme I: Data Sharing

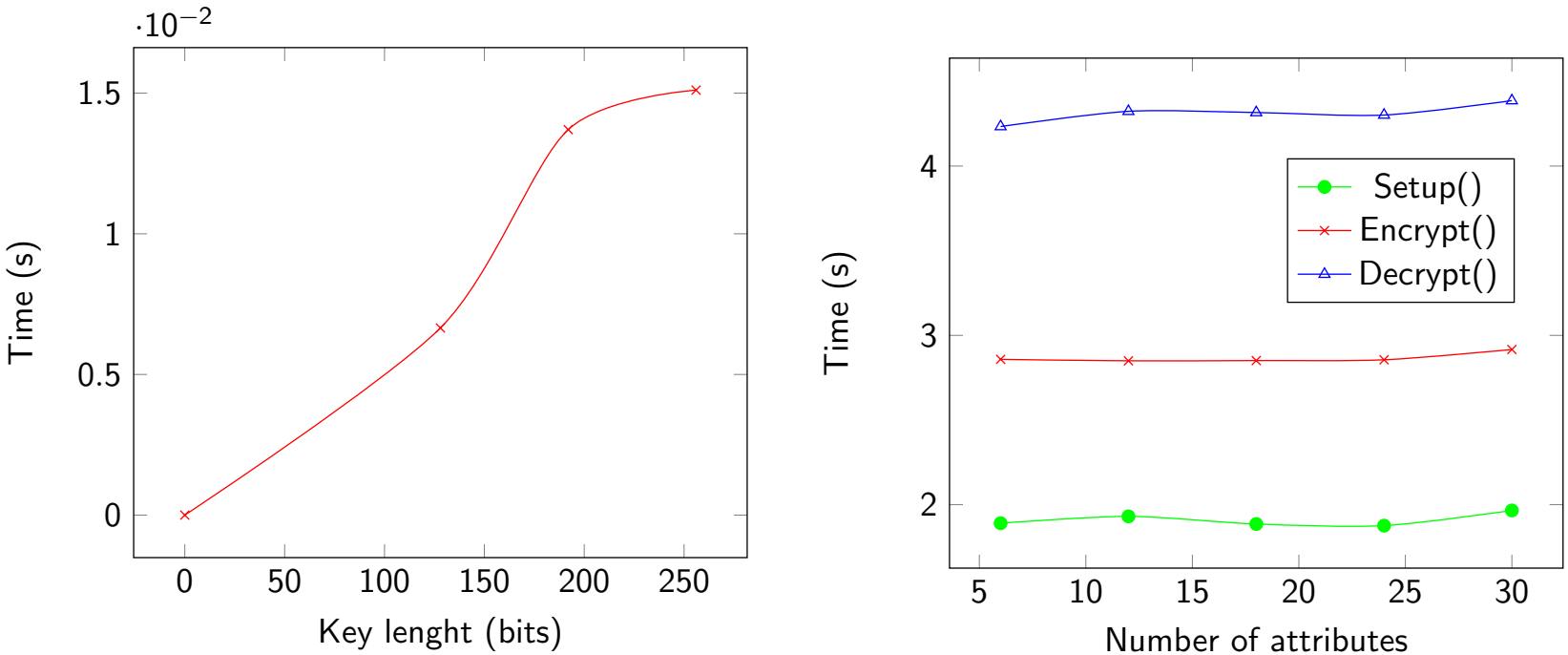


Scheme II: Reconfiguration Mode



Tests

Experiments have been run on a Google Nexus 4 smartphone.



(a) (b)

Figure: Execution time: (a) AES; (b) CP-ABE.

Conclusions

- The versatility offered by CP-ABE is used to propose protocols that allow sensors to subscribe to the data feeds published by other sensors.
- The privileges required to access each particular data are set by the sensor's policy.
- External actors can get access to such data feeds and also reconfigure or request specific data from the sensors provided that they have sufficient privileges to do so.
- Our experimental results confirm that the scheme is suitable for most current sensors, including ARM-based platforms.

Decentralised Ciphertext Attribute-Based Encryption with Keyword Search (DCP-ABSE)

Motivation

Facts

- IoT is generating tons of data... DAILY!
- Data should be constantly updated and reliable.
- Both personal information and queries must be encrypted.
- Are researchers able to do research privately?

Problems

- How to find some values over tons of data?
- Who is able to perform queries?
- Is it possible to split queries and data access privileges?
- Is the database able to learn anything from queries? And from the stored data/keyword?

Goals

	no-CA	MA	no-TA	SE	ABE
Varsha *et al.* [Varsha,2014]	X	✓	✓	X	KP-ABE
Koo *et al.*[Koo,2013]	✓	X	X	✓	CP-ABE
VABKS [Zheng,2014]	✓	X	X	✓	CP/KP-ABE
ARMS [Hongwei,2015]	X	✓	X	✓	CP-ABE
Lewko *et al.* [Lewko,2011]	✓	✓	X	X	CP-ABE
our model	✓	✓	✓	✓	CP-ABE

Table: Comparison of ABSE schemes

CA: Central Authority, MA: Multiple Authorities, TA: Trusted Authority, SE: Searchable Encryption

Objectives

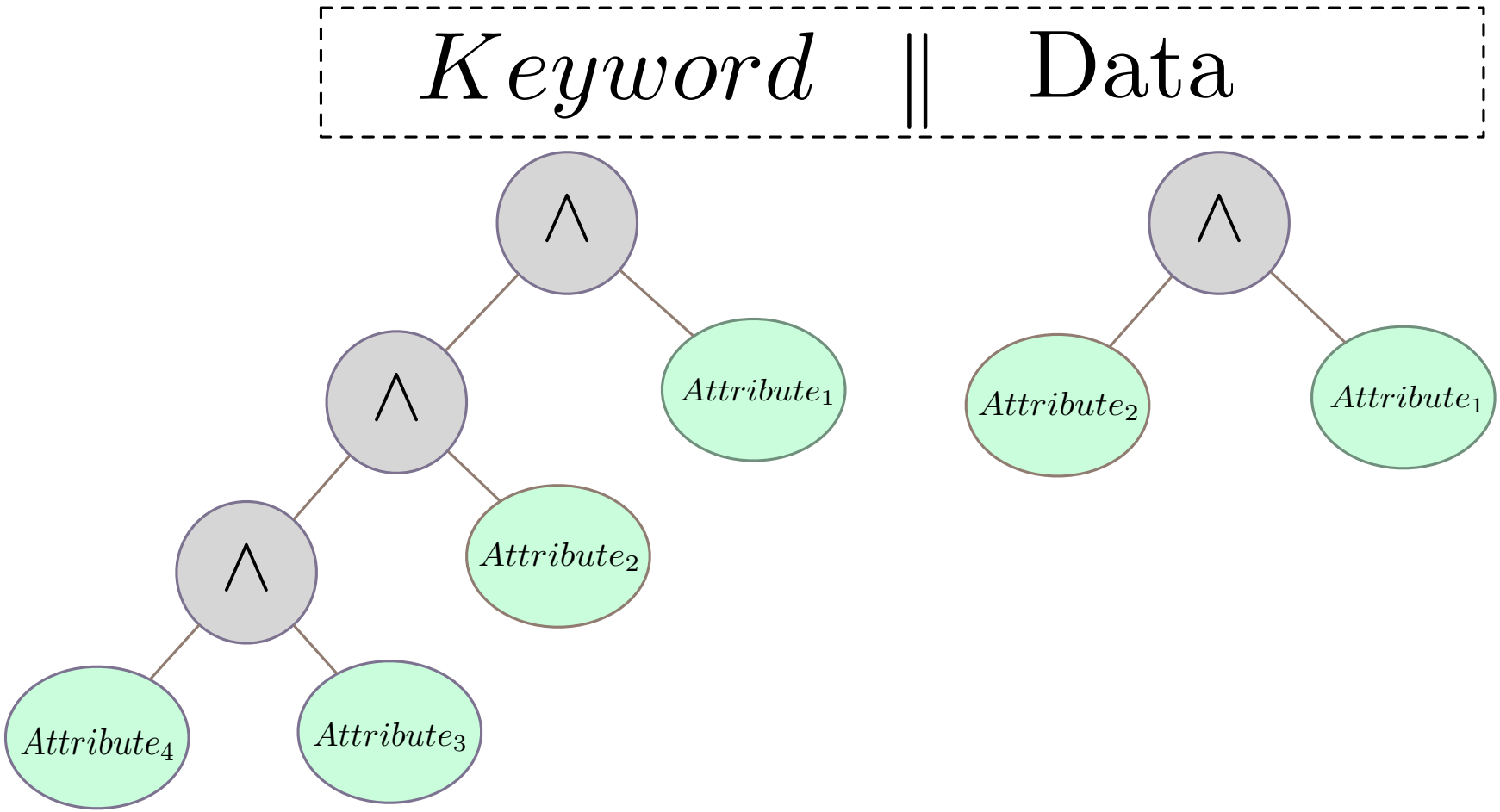
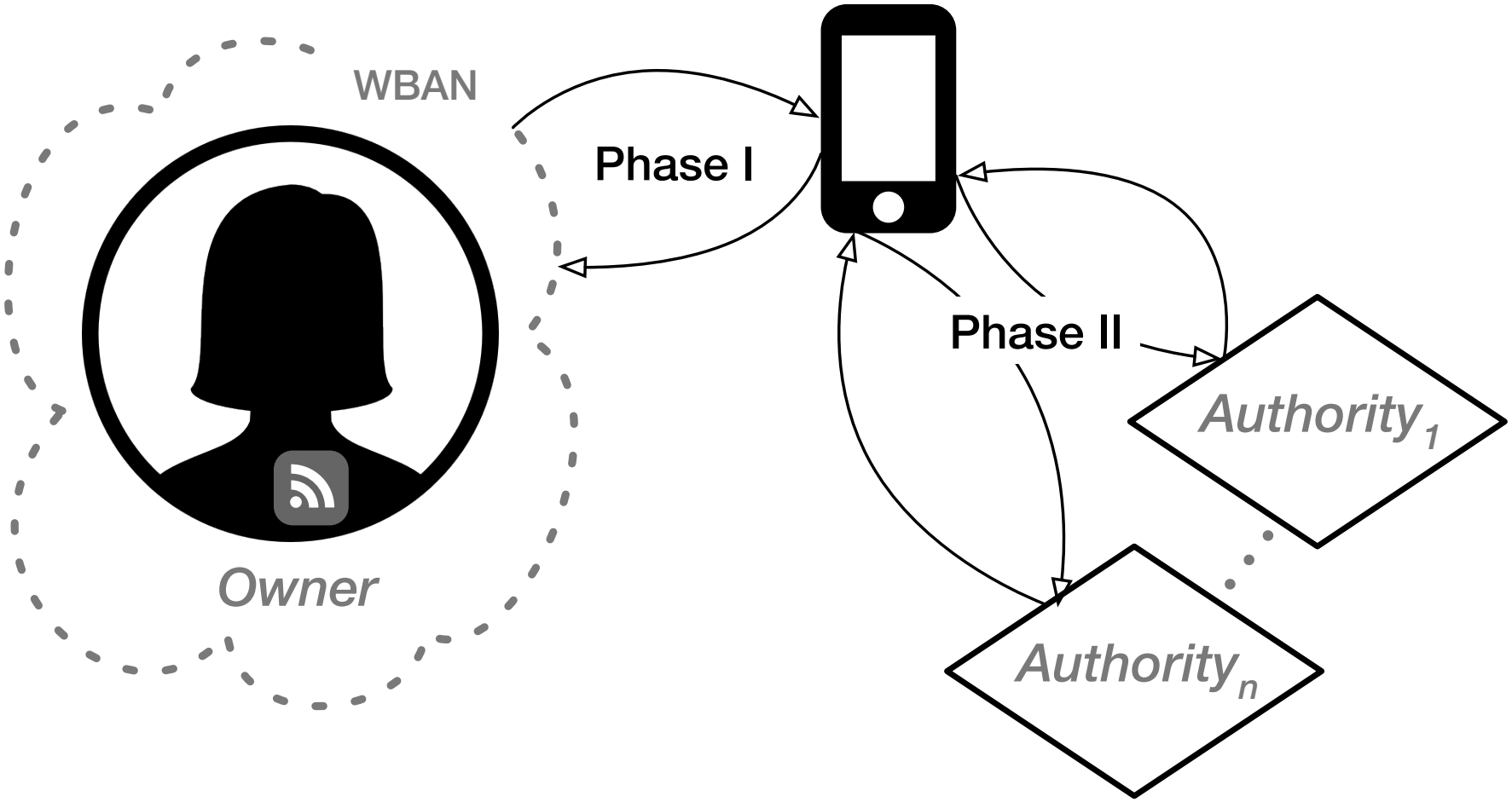
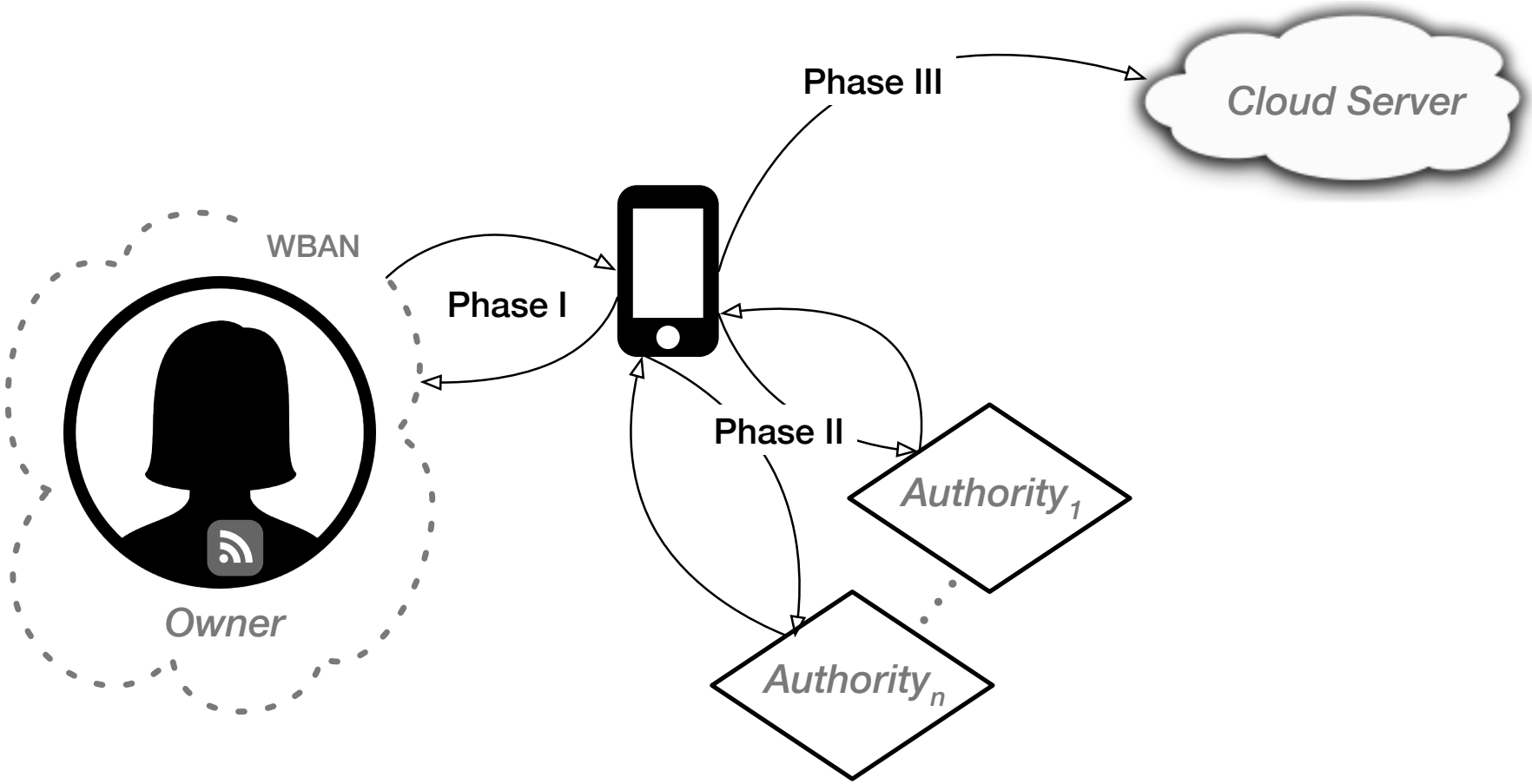


Figure: Keywords and Data Encryption

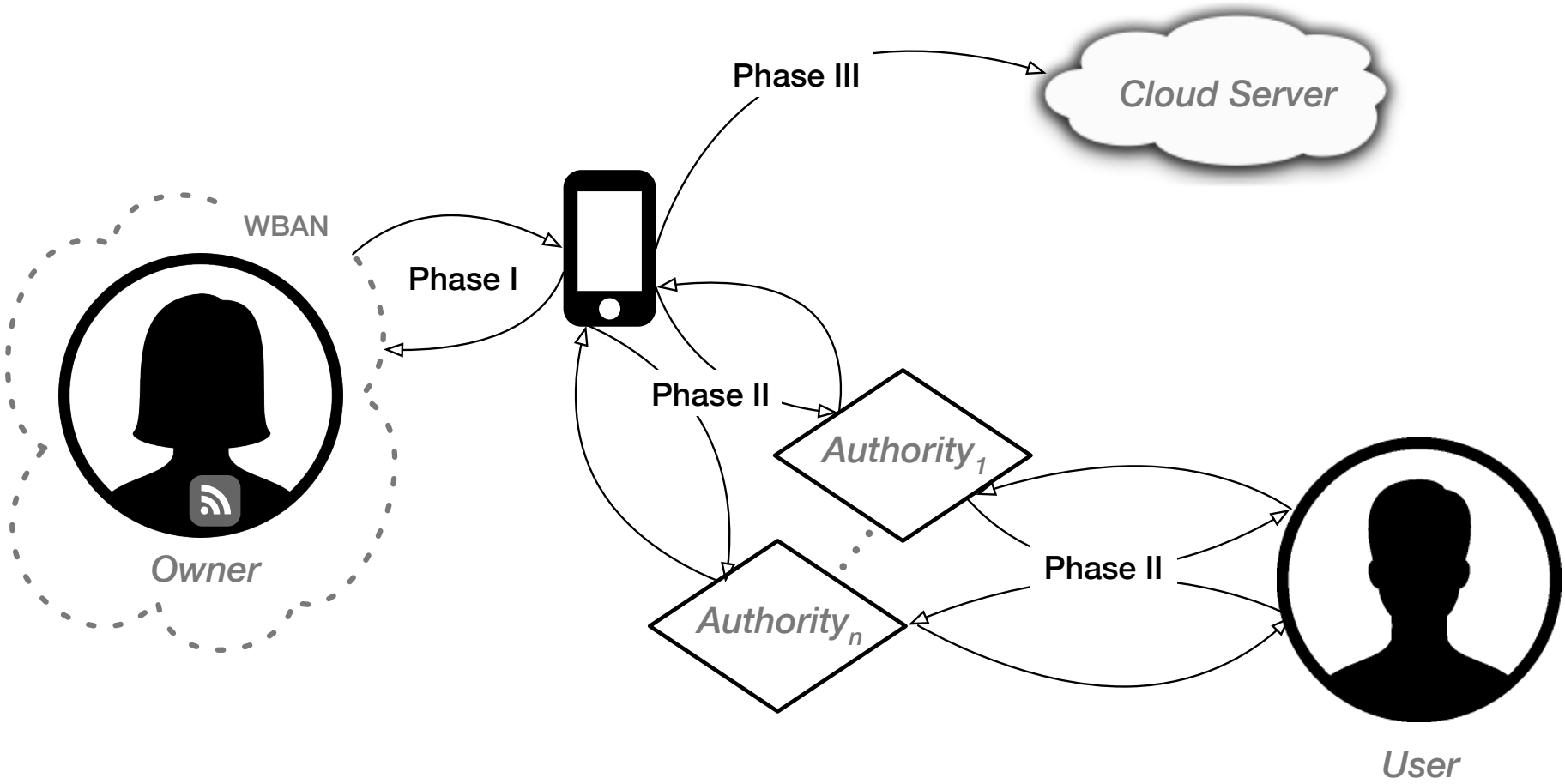
DCP-ABSE - I



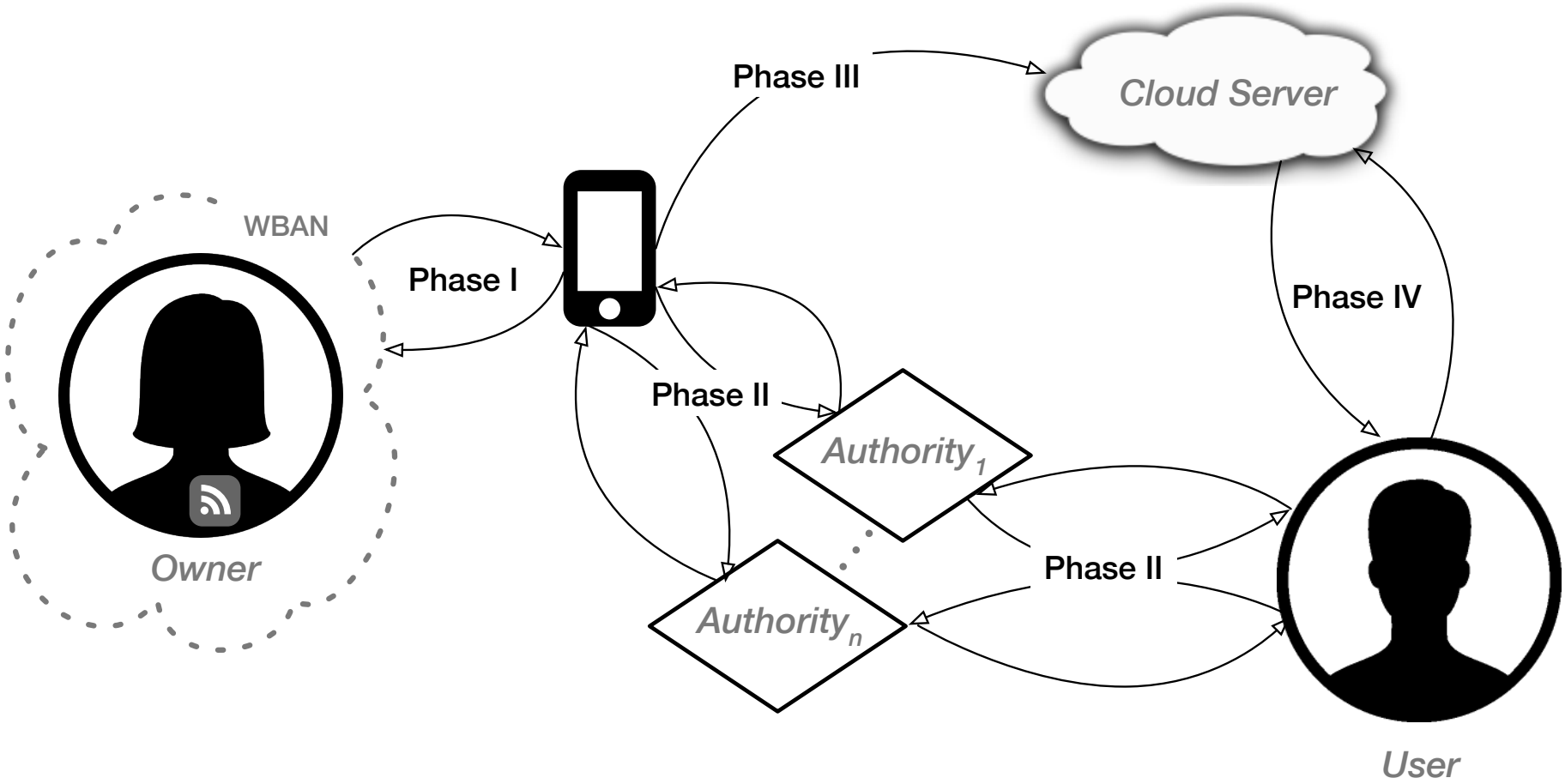
DCP-ABSE - II


Phase III
Cloud Server
WBAN
Phase I
Phase II
Authority 1
Authority n
Owner

DCP-ABSE - III


Phase III
Cloud Server
WBAN
Phase I
Phase II
Authority 1
Authority n
Phase II
Owner
User

DCP-ABSE - IV


Phase III
Cloud Server
WBAN
Phase I
Phase IV
Phase II
Authority 1
Phase II
Authority n
Owner
User

Experiments I

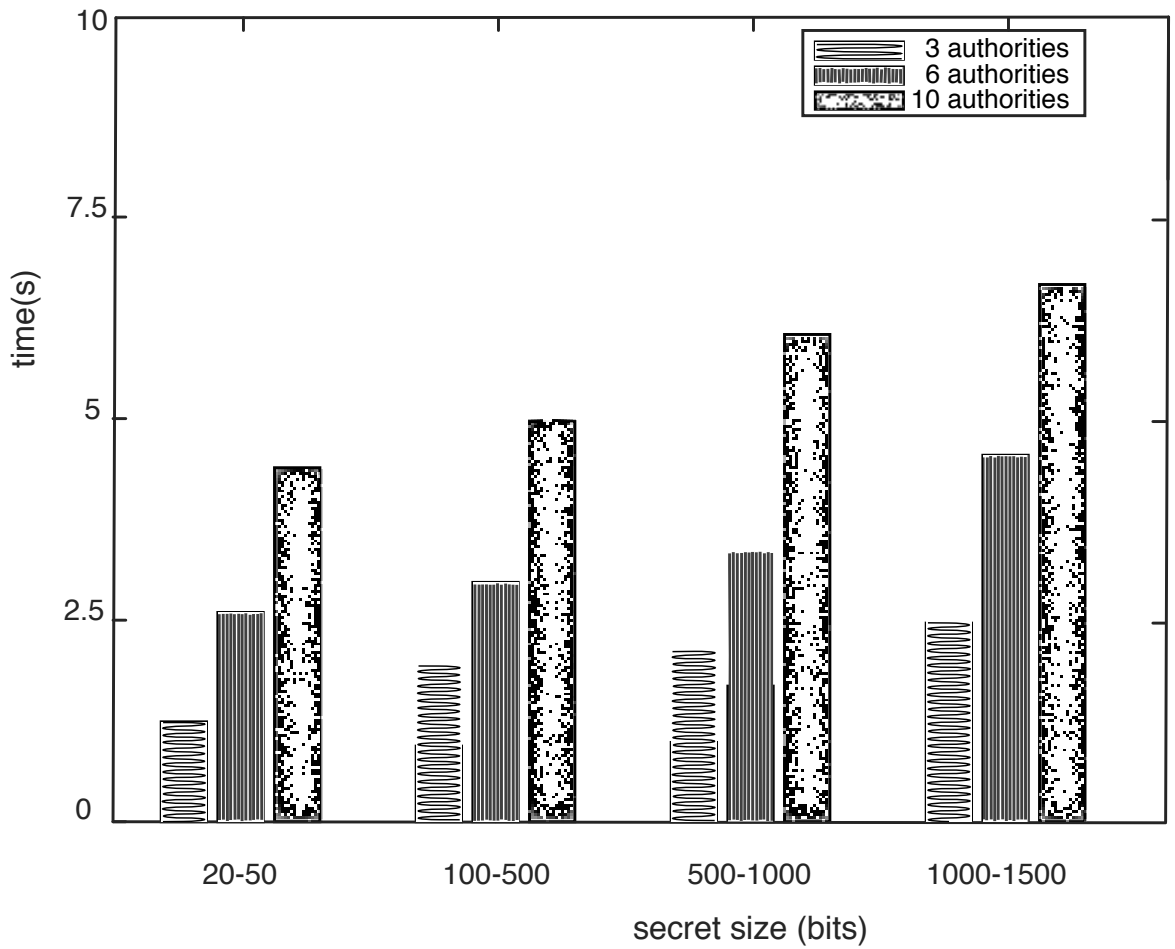


Figure: SMPC time vs length

Experiments II

		g^r	$e(g,g)$	$g^r \cdot g^r$	$H_1(att)$
160 bits	Debian	0.002	0.001	0.003	0.004
	Nexus 4	0.246	0.852	0.474	0.806
	Moto G	0.191	0.433	0.334	0.356
384 bits	Debian	0.005	0.003	0.002	0.010
	Nexus 4	0.740	1.749	1.411	0.334
	Moto G	0.470	0.670	0.743	0.158

Table: Comparison of performance operations in seconds

Experiments III

		AS	KeyGen	Enc	Dec
160 bits	Debian	0.019	0.008	0.033	0.016
	Nexus 4	2.488	3.788	4.360	6.694
	Moto G	1.129	1.549	2.200	2.559
384 bits	Debian	0.041	0.012	0.077	0.028
	Nexus 4	5.649	3.159	9.570	10.558
	Moto G	2.787	1.411	4.912	4.896

Table: Comparison of DCP-ABSE methods' performance in seconds (ABE)

Experiments IV

		TokenGen	EKw	Search
160 bits	Debian	0.048	0.058	0.016
	Nexus 4	5.235	2.413	5.280
	Moto G	2.921	1.450	2.196
384 bits	Debian	0.101	0.087	0.037
	Nexus 4	12.364	0.087	8.937
	Moto G	12.364	3.081	4.230

Table: Comparison of DCP-ABSE methods' performance in seconds (SE)

Summary

- Personal information is stored securely on public servers and queries are encrypted.
- Two different Access Policies must be satisfied in order to retrieve and decrypt personal information.
- Multiple Authorities are allowed. No Central Authority is needed.
- SMPC is used to share a common key.

Q & A

References I

John Bethencourt, Amit Sahai, Brent Waters.

Ciphertext-Police Attribute-Based Encryption.

IEEE Symposium on Security and Privacy pp. 321-334, IEEE, 2007

Allison Lewko, Brent Waters

Decentralizing attribute-based encryption.

In Advances in CryptologyEUROCRYPT 2011 (pp. 568-588). Springer Berlin Heidelberg.

Fuchun Guo; Yi Mu; Susilo, W.; Wong, D.S.; Varadharajan, V.

CP-ABE With Constant-Size Keys for Lightweight Devices

Information Forensics and Security IEEE Transactions on , vol.9, no.5, pp.763,771, May 2014 doi: 10.1109/TIFS.2014.2309858

Pablo Picazo-Sanchez, Juan Tapiador, Pedro Peris-Lopez, Guillermo Suarez-Tangil,

Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks.

Sensors, 14(12), 22619-22642. Dec 2014

References II

Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Nasour Bagheri,
Weaknesses of Fingerprint-based Mutual Authentication Protocol.
Software and Communication Networks (2014). doi:10.1002/sec.1161

Z.-Y. Wu, L. Chen, and J.-C. Wu.
A reliable RFID mutual authentication scheme for healthcare environments.
Journal of Medical Systems, 37:19, 2013.

P. Najera, J. Lopez, and R. Roman.
Real-time location and inpatient care systems based on passive RFID.
Journal of Network and Computer Applications, 34(3):980 989, 2011.

W. Yao, C.-H. Chu, and Z. Li.
The use of RFID in healthcare: Benefits and barriers.
In RFID-Technology and Applications (RFID-TA), 2010 IEEE In- ternational Conference on, pages 128 134, june 2010.

References III

J. Aronson.

Medication errors: what they are, how they happen, and how to avoid them.

QJM: An International Journal of Medicine, 102(8):513521, 2009.

Y.-C. Yen, N.-W. Lo, and T.-C. Wu.

Two RFID-based solutions for secure inpatient medication administration.

Journal of Medical Systems, 36(5):2769 2778, 2012.

A. Oztekin, F. M. Pajouh, D. Delen, and L. K. Swim.

An RFID network design methodology for asset tracking in healthcare.

Decision Support Systems, 49(1):100 109, 2010.

X. Qu, L. T. Simpson, and P. Stanfield.

A model for quantifying the value of RFID-enabled equipment tracking in hospitals.

Advanced Engineering Informatics, 25(1):23 31, 2011.

References IV

H.-L. Chan, T.-M. Choi, and C.-L. Hui.

RFID versus bar-coding systems: Transactions errors in health care apparel inventory control.

Decision Support Systems, 54(1):803 811, 2012.

S. Parlak, A. Sarcevic, I. Marsic, and R. S. Burd.

Introducing rfid technology in dynamic and time-critical medical settings: Requirements and challenges.

Journal of Biomedical Informatics, 45(5):958 974, 2012.

M. H. Yang.

Secure multiple group ownership transfer protocol for mobile RFID.

Electronic Commerce Research and Applications, 11(4):361 373, 2012.

W. Zhou, E. J. Yoon, and S. Piramuthu.

Simultaneous multi-level RFID tag ownership & transfer in health care environments.

Decision Support Systems, 54(1):98 108, 2012.

References V

S. Parlak, A. Sarcevic, I. Marsic, and R. S. Burd.

Introducing RFID technology in dynamic and time-critical medical settings: Requirements and challenges.

Journal of Biomedical Informatics, 45(5):958 974, 2012.

W. Yao, C.-H. Chu, and Z. Li.

Leveraging complex event processing for smart hospitals using RFID.

Journal of Network and Computer Applications, 34(3):799 810, 2011.

R. Bunduchi, C. Weisshaar, and A. U. Smart.

Mapping the benefits and costs associated with process innovation: The case of RFID adoption.

Technovation, 31(9):505 521, 2011.

W. Yao, C.-H. Chu, and Z. Li.

The use of RFID in healthcare: Benefits and barriers.

In RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on, pages 128 134, june 2010.

References VI

J. H. Khor, W. Ismail, M.I. Younis,M.K. Sulaiman, and M.G. Rahman.

Security problems in an RFID system.

Wireless Personal Communications, 59(1), 17-26. 2011

J. Daemen and V. Rijmen

The design of Rijndael: AES-the advanced encryption standard.

Springer Science & Business Media. 2013

Varsha, B Sri and Suryateja, PS

Using Attribute-Based Encryption with Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud.

International Journal of Computer Science & Information Technologies, 5(5). 2014

Dongyoung K. and Junbeom H. and Hyunsoo Y.

Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage.

Computers & Electrical Engineering. 39(1), 34-46, 2013

References VII

Qingji Z. and Shouhuai X. and Ateniese, G.

VABKS: Verifiable attribute-based keyword search over outsourced encrypted data

INFOCOM, Proceedings IEEE. 522-530, 2014

Hongwei L. and Dongxiao L. and Kun J. and Xiaodong L.

Achieving authorized and ranked multi-keyword search over encrypted cloud data

Communications (ICC), 2015 IEEE International Conference on, 7450-7455, 2015

Decentralizing Attribute-Based Encryption

Advances in Cryptology. EUROCRYPT, 568-588. 2011