Nils gentschen Felde, Sophia Grundner-Culemann, Tobias Guggemos

Munich Network Management-Team

Ludwig-Maximilians-Universität München

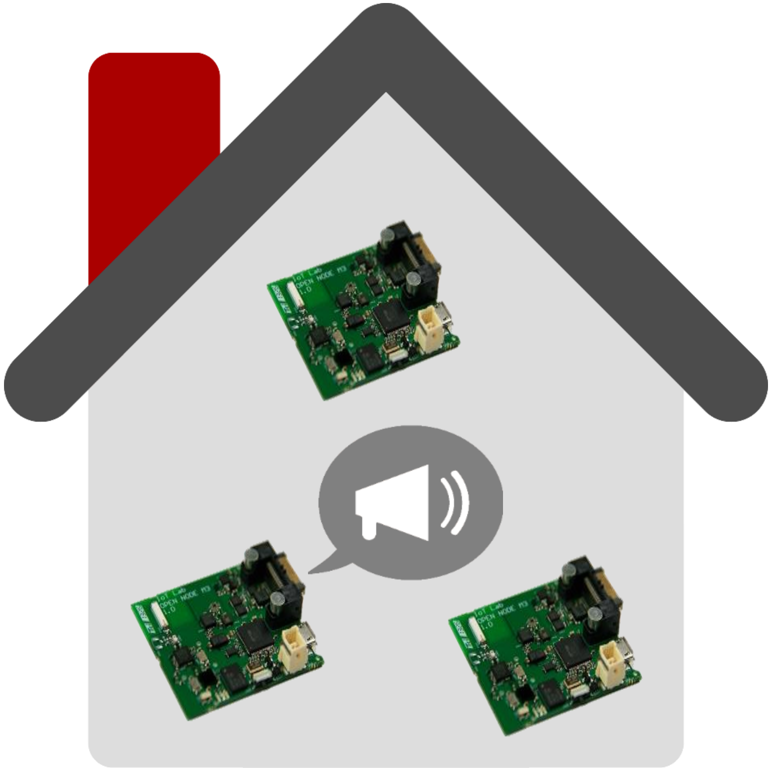
Authentication in dynamic groups using Identity-based Signatures

October 16, 2018

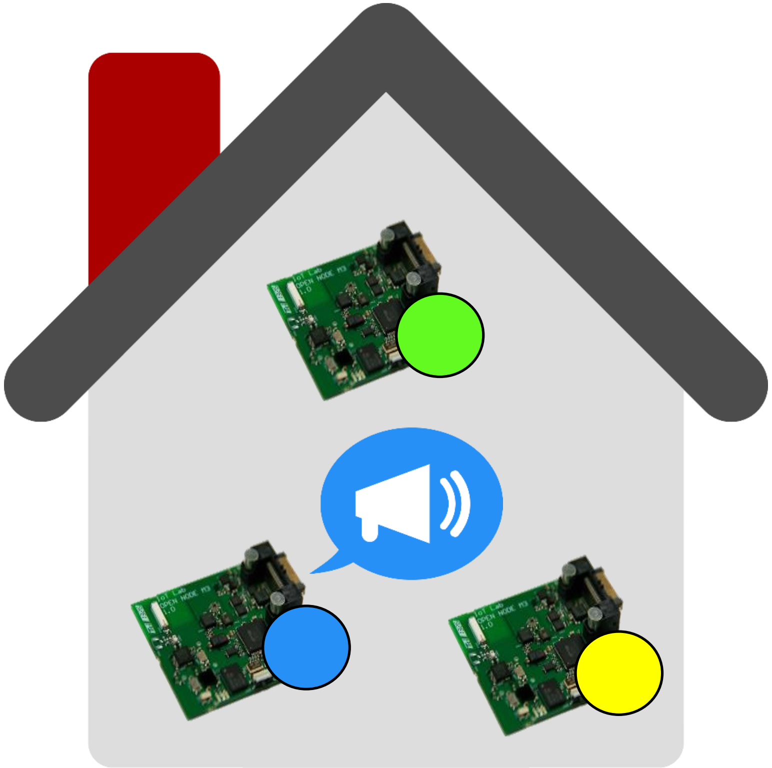
IEEE WiMob 2018

Limassol, Cyprus

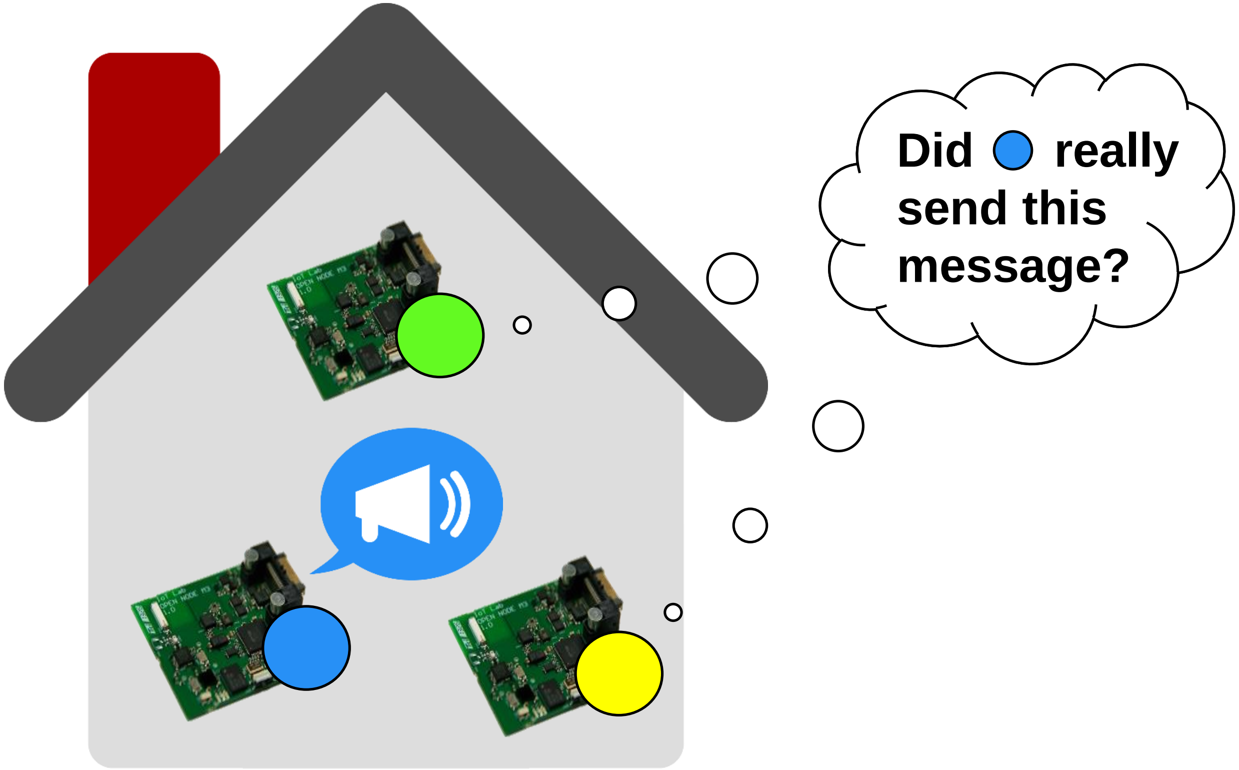
group communication



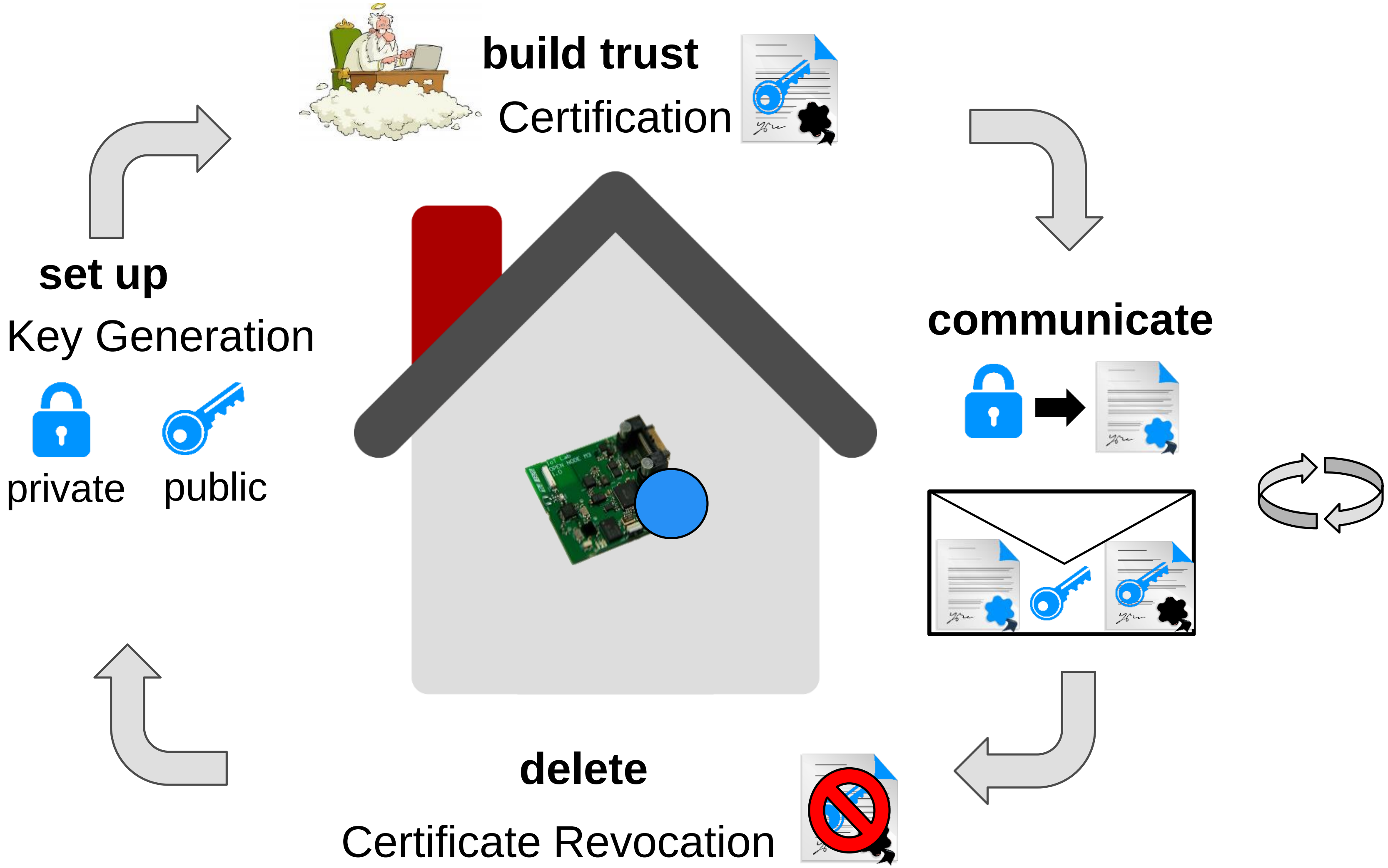
verify message authenticity



verify message authenticity



classic authentication



set up

Key Generation

private public

build trust

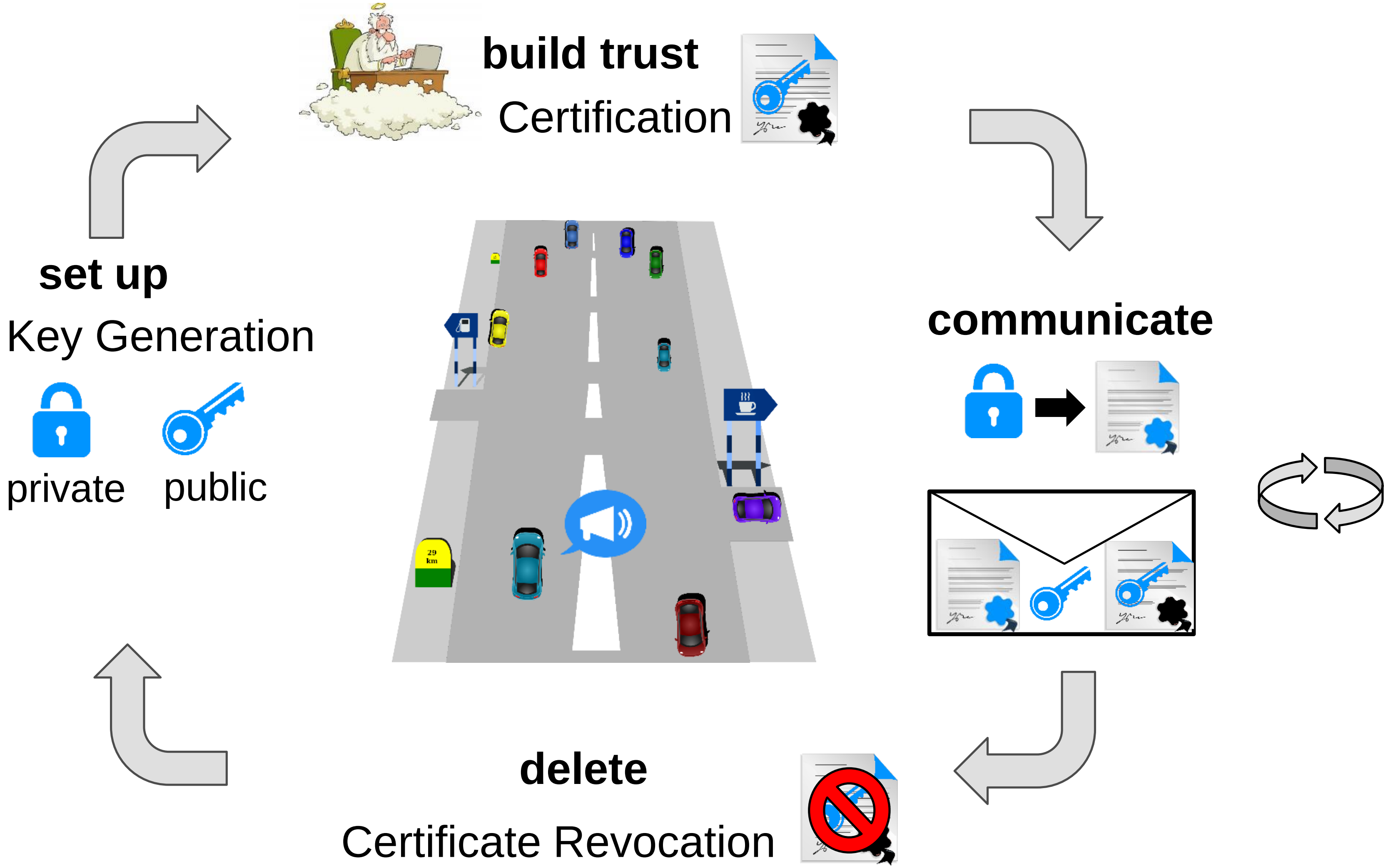
Certification

communicate

delete

Certificate Revocation

Dynamic groups



build trust

Certification

communicate

delete

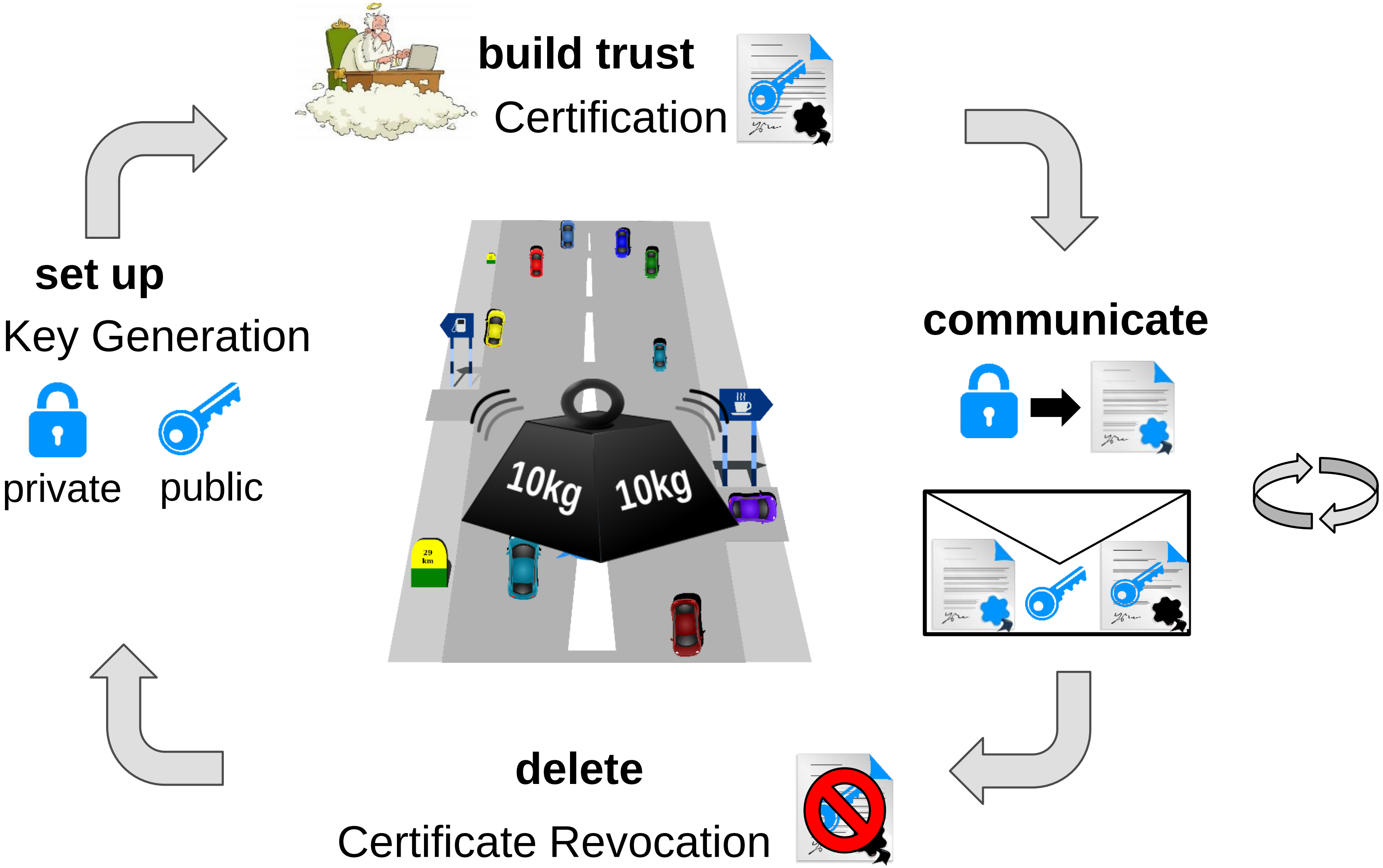
Certificate Revocation

set up

Key Generation

private public

Classic approach too expensive



build trust

Certification

communicate

delete

Certificate Revocation

set up

Key Generation

private public

Authentication in dynamic groups using identity-based signatures

Nils gentschen Felde, Sophia Grundner-Culemann, Tobias Guggemos
MNM-Team, Ludwig-Maximilians-Universität München, Munich, Germany
Email: {felde, grundner-culemann, guggemos}@nm.ifi.lmu.de

***Abstract*—Group communication in constrained networks lately sparked broader interest as it allows dealing more efficiently with the few available resources. Both sender authentication and membership verification are serious issues to be tackled despite the lack of resources. Identity-based signatures (IBS) offer an alternative to certificate-based authentication by mathematically binding a user's public key to its identity. To utilize the consequently smaller network load, this paper proposes an IBS-based lightweight solution to achieve authentication and membership verification for group communication in constrained environments. An infrastructure for managing IBS-based authentication is introduced together with a taxonomy for the selection of suitable IBS schemes. An implementation and practical evaluation on basis of an IoT-lab completes this, demonstrating that IBS is a viable option for very constrained devices. To the best of our knowledge, this is the first fully operational implementation and proof of applicability of IBS in such a scenario.**

***Keywords*-IoT; Multicast; Security; Group Communication; Authentication; Identity-Based Signatures**

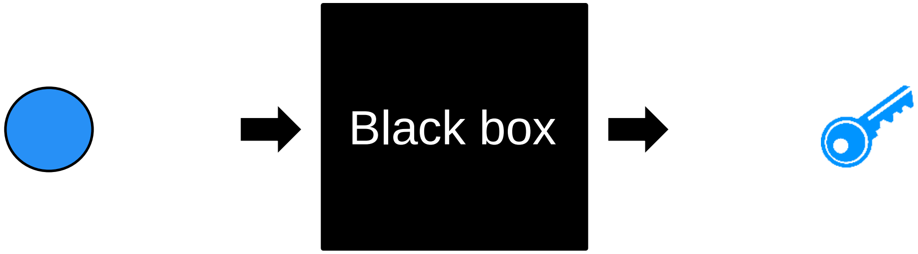
this case meaning frequently changing group settings, for which IBS is second to none in terms of messages to be exchanged. Even though X.509 certificate compression has already been addressed by the IETF [2], access management is typically enforced using costly revocation lists. Frameworks such as SAML (Security Assertion Markup Language) or OAuth (Open Authorization) offer optimizations based on so-called access tokens. They can also be used to grant both group access and group authentication. However, individual sender authentication is not covered.

Talking about IBS and its use for authenticated group communication, it is inevitable to define the term authenticity in the scope of group communication. A well-suited definition is given in an earlier publication [3]: "*A message is authentic, if the message originates from its stated sender. Similar to message integrity, in group communication scenarios one can differentiate two types of message authenticity: a) a message can be proven to originate from within the communication*

Sender authentication with Identity-Based Signatures (IBS)

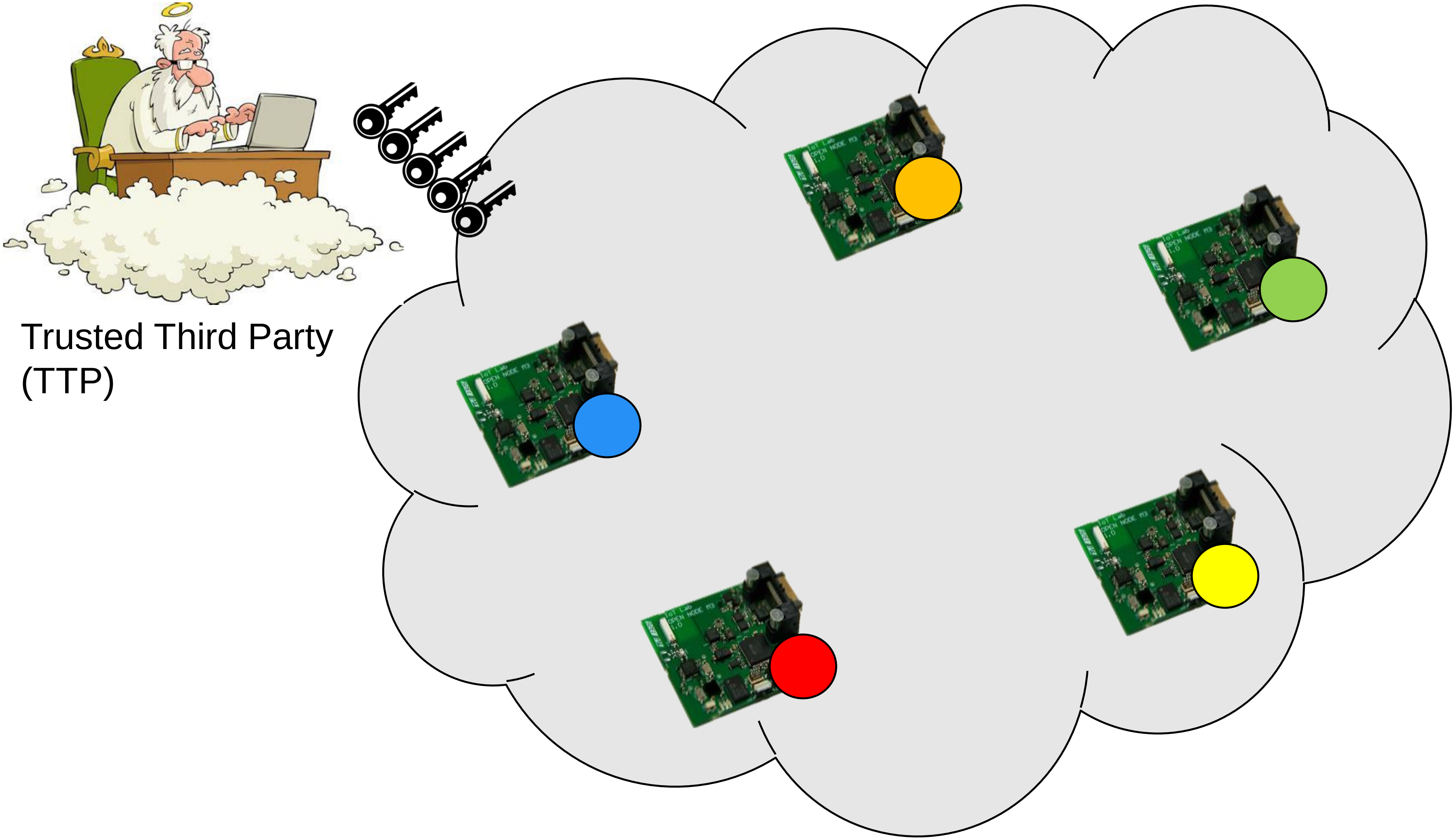
Idea:
(Shamir, 1984)

Compute public key from identifying information



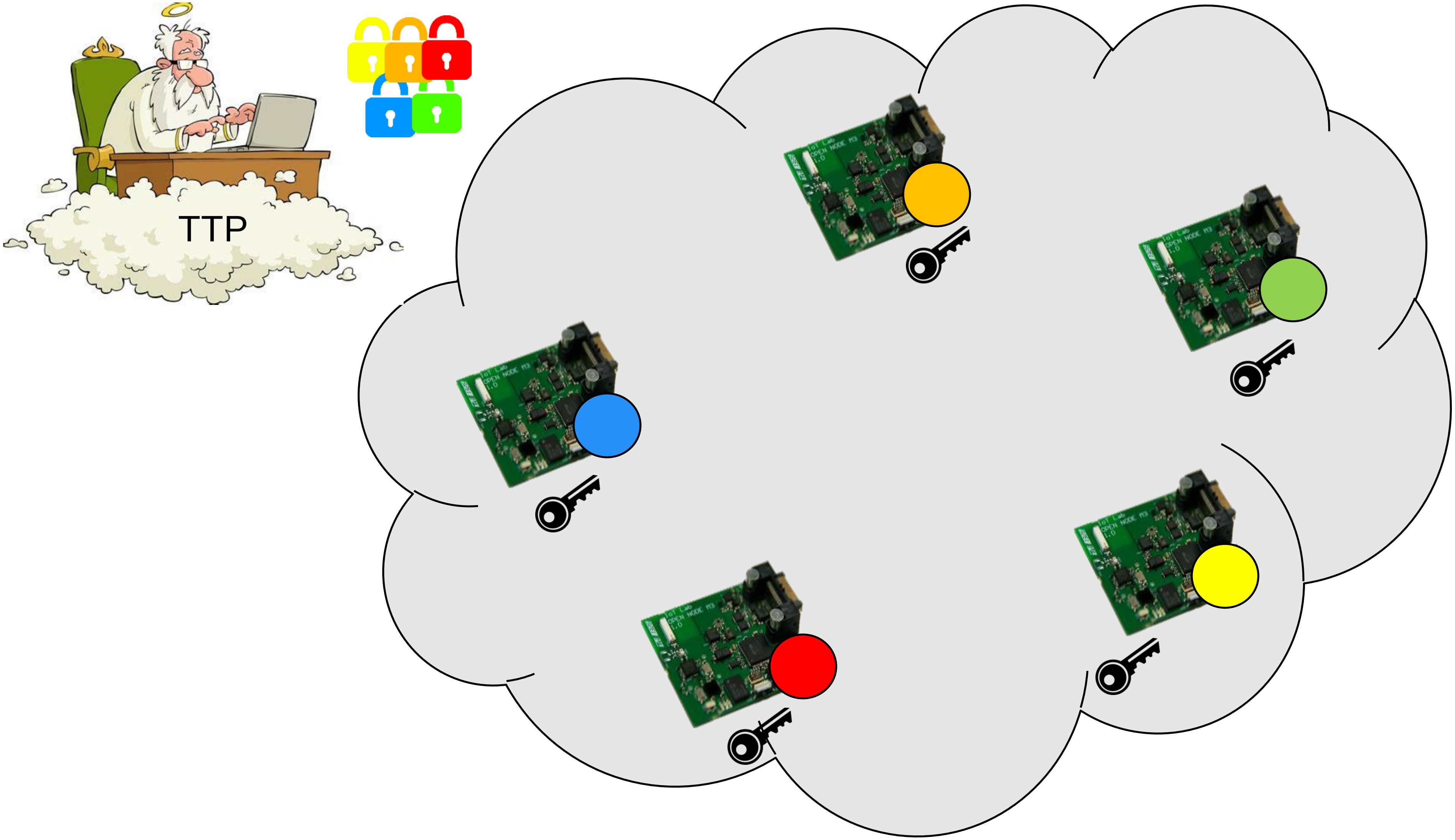
Black box

Sender authentication with Identity-Based Signatures (IBS): master public key distribution

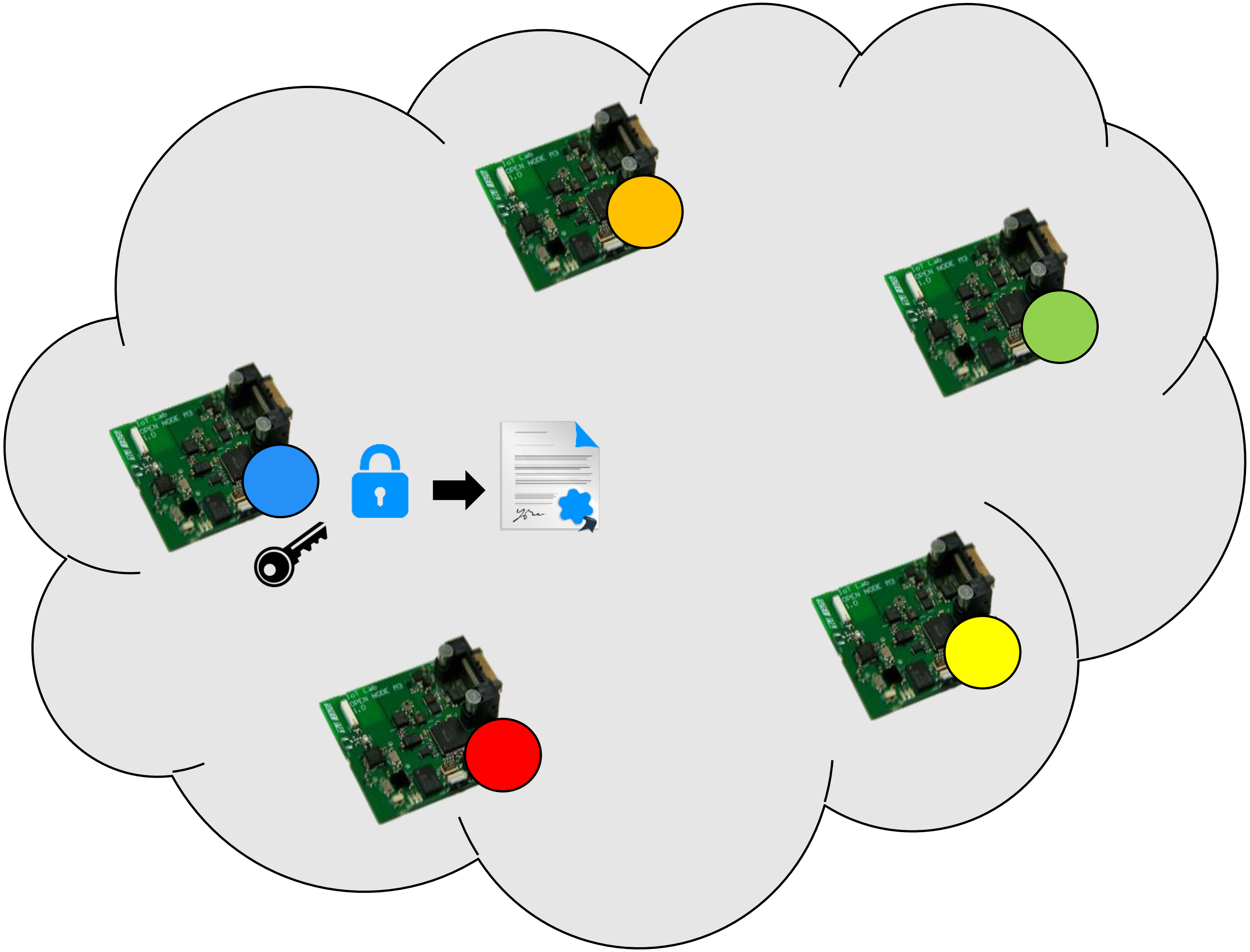


Trusted Third Party (TTP)

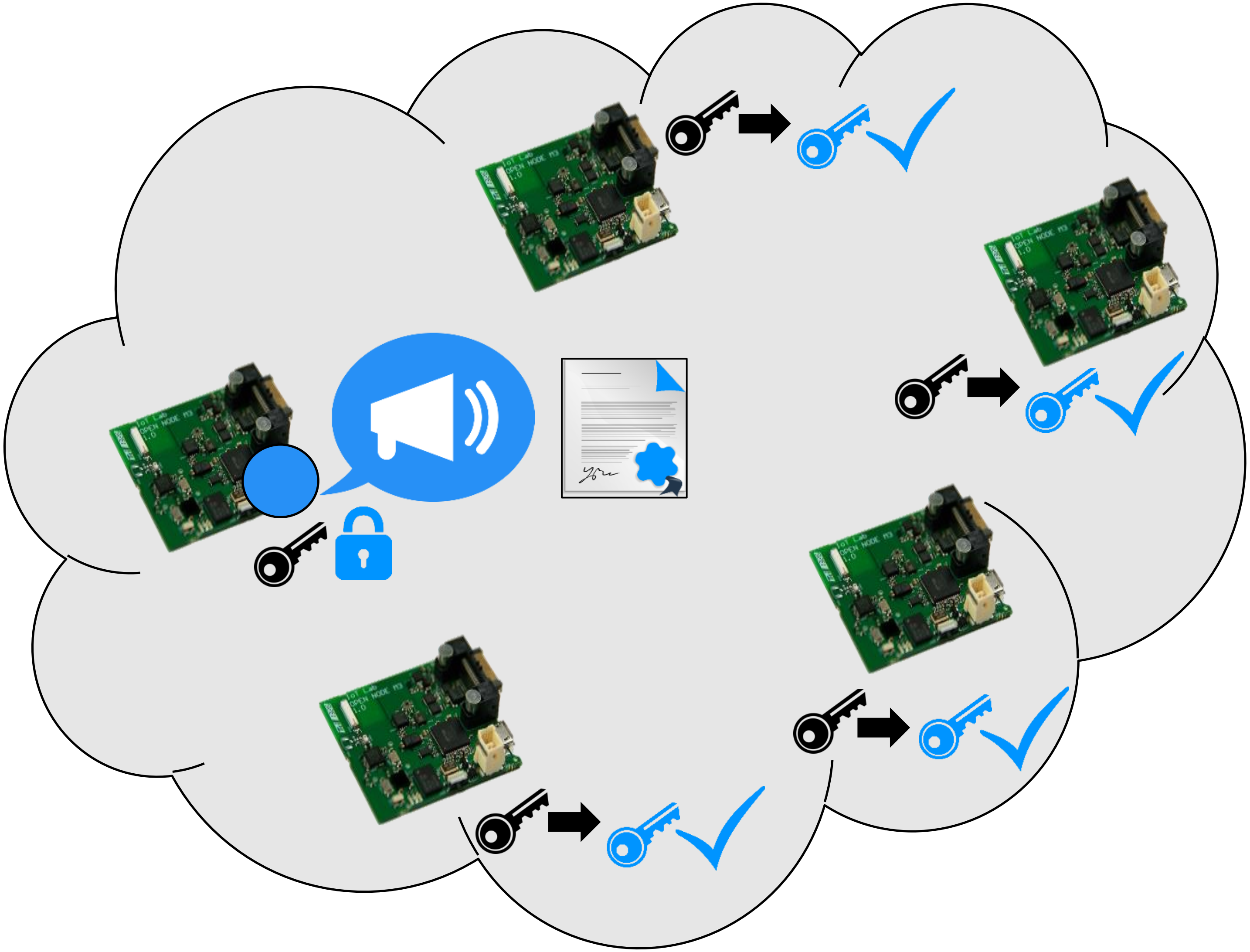
Sender authentication with IBS: private key distribution



Sender authentication with IBS: signature generation



Sender authentication with IBS:
signature verification



Related work

Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps

Paulo S. L. M. Barreto[2], Benoît Libert[3]*,
Noel McCullagh[1]**, and Jean-Jacques Quisquater[3]

[1] School of Computer Applications
Dublin City University
Ballymun, Dublin 9, Ireland.
noel.mccullagh@computing.dcu.ie
[2] PCS, Escola Politécnica, Universidade de São Paulo
Av. Prof. I
BR
[3] UCL, Mi
Place du Lev
Telephone : -
lib

Abstract. In this p
(IBSC) scheme built
more efficient than a

A Schnorr-Like Lightweight Identity-Based Signature Scheme

David Galindo[1,*] and Flavio D. Garcia[2,**]

[1] University of Luxembourg
david.galindo@uni.lu
[2] Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands
flaviog@cs.ru.nl

stract. The use of concatenated Schnorr signatures [Sch91] for the
rarchical delegation of public keys is a well-known technique. In this
per we carry out a thorough analysis of the identity-based signature
eme that this technique yields. The resulting scheme is of interest
ce it is intuitive, simple and does not require pairings. We prove
t the scheme is secure against existential forgery on adaptive cho-
message and adaptive identity attacks using a variant of the Forking
nma [PS00]. The security is proven in the Random Oracle Model
ler the discrete logarithm assumption. Next, we provide an estima-
n of its performance, including a comparison with the state of the art
identity-based signatures. We draw the conclusion that the Schnorr-
identity-based signature scheme is arguably the most efficient such
eme known to date.

ywords: identity-based signature, lightweight cryptography, provable
urity, Schnorr, random oracle model.

IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks

Xuefei Cao *, Weidong Kou, Lanjun Dang, Bin Zhao

State Key Laboratory of Integrated Service Networks, Xidian University, P.O. Box 119, 710071 Xi'an, China

Available online 22 October 2007

cast authentication enables a large number of users to join in and broadcast messages to wireless sensor networks
and authentically. Public-key-based schemes have been proposed to provide such services; however, none of them
lability and efficiency simultaneously. This paper presents IMBAS, an identity-based multi-user broadcast authen-
h strong security, sound scalability and efficiency for WSN. IMBAS divides broadcasts into two categories and
yptographic primitives. Users' broadcasts are secured with vBNN-IBS, a novel pairing-free identity-based signature
ure size, which is proposed in this paper to achieve security, scalability and efficiency; the sink's broadcast is secured
ure with partial message recovery to further optimize the efficiency. Password-based user private key protection is
sist proactively the compromise attack. Theoretical analysis demonstrates that IMBAS provides strong security
y. Quantitative energy analysis shows that IMBAS reduces energy consumption by at least 41.5 percent compared
ty-based scheme.
'. All rights reserved.

3442 IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 56, NO. 6, NOVEMBER 2007

GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications

Xiaodong Lin, *Student Member, IEEE*, Xiaoting Sun, Pin-Han Ho, *Member, IEEE*, and
Xuemin Shen, *Senior Member, IEEE*

***Abstract*—In this paper, we first identify some unique design requirements in the aspects of security and privacy preservation for communications between different communication devices in vehicular *ad hoc* networks. We then propose a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques. We demonstrate that the proposed protocol cannot only guarantee the requirements of security and privacy but can also provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event. Extensive simulation is conducted to verify the efficiency, effectiveness, and applicability of the proposed protocol in various application scenarios under different road systems.**

***Index Terms*—Conditional privacy, group signature, identity (ID)-based signature, security, vehicular communications.**

the roadside will be densely covered with a variety of RSUs, like traffic lights, traffic signs, and wireless routers, which will provide wireless access to vehicles on the road. In addition, the RSUs could be connected to the Internet backbone to support diversified services, such as transmission control protocol and real-time multimedia streaming applications. Thus, increasing interest has been raised by both industry and academia on the applications of roadside-to-vehicle communication and inter-vehicle communication (IVC), aiming to improve the driving safety and traffic management while providing drivers and passengers with Internet access at the same time.

The creation of a VANET is significant to traffic management and roadside safety. Unfortunately, a VANET also comes with its own set of challenges, particularly security and privacy. As
a special implementation of mobile *ad hoc* networks, a VANET
any security threats, which will lead to
ttacks and service abuses. It is obvious
avior of users, such as a modification and
isseminated messages, could be fatal to
re, conditional privacy preservation must
se that user-related private information,
name, license plate, speed, position,
hicle identification number (VIN) of the
routes, as well as their relationships, has
he authorities should be able to reveal the
senders in case of a traffic event dispute,
cident scene investigation, which can be
sses. Therefore, it is critical to develop a
carefully designed security mechanisms
nd conditional privacy preservation in
can practically be launched. However,
mber of previously reported studies have
d privacy issues of VANETs, in spite of

Efficient Identity Based Signature Schemes Based on Pairings

Florian Hess

Dept. Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB
florian@cs.bris.ac.uk

Abstract. We develop an efficient identity based signature scheme based on pairings whose security relies on the hardness of the Diffie-Hellman problem in the random oracle model. We describe how this scheme is obtained as a special version of a more general generic scheme which yields further new provably secure identity based signature schemes if pairings are used. The generic scheme also includes traditional public key signature schemes. We further discuss issues of key escrow and the distribution of keys to multiple trust authorities. The appendix contains a brief description of the relevant properties of supersingular elliptic curves and

2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing

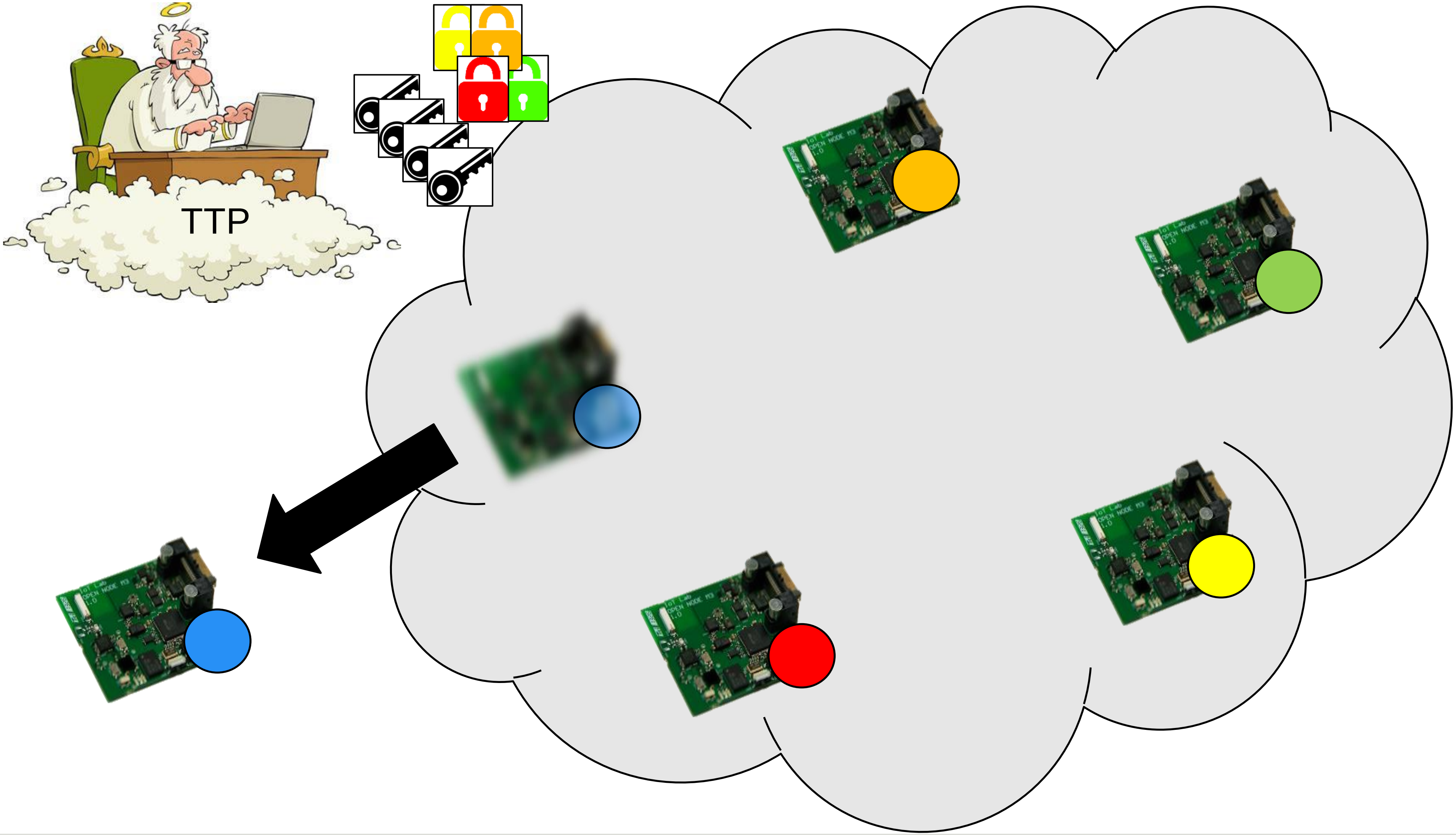
An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature

Joonsang Baek Young-ji Byon Eman Hableel Mahmoud Al-Qutayri
Khalifa University of Science, Technology and Research
Abu Dhabi, United Arab Emirates
Email: joon.baek@kustar.ac.ae

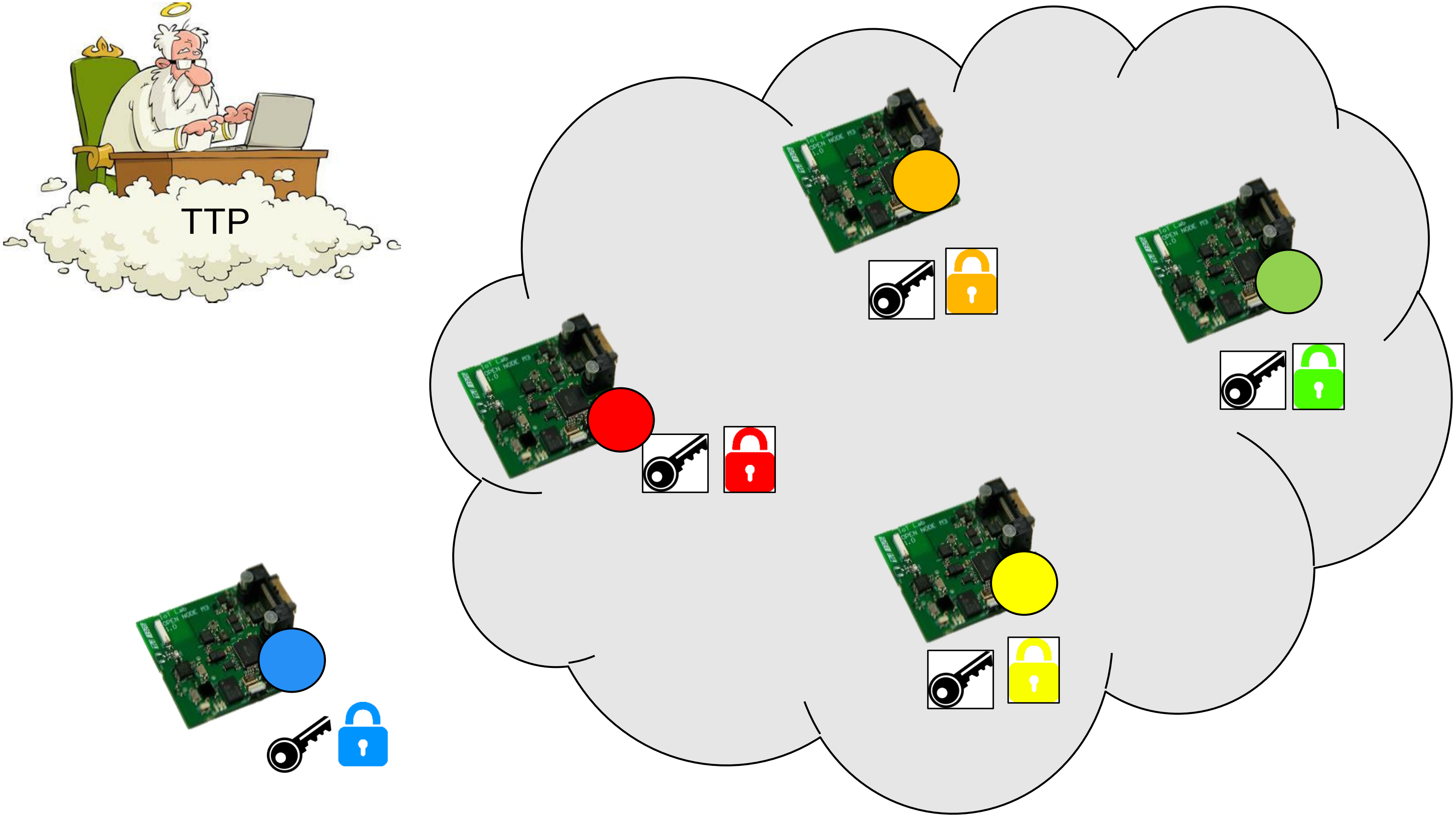
***Abstract*—Automatic Dependent Surveillance Broadcast (ADS-B) is an emerging aircraft surveillance technology with which the concept of Internet of Things (IoT) is being realized in air traffic networks. The future "e-enabled" aircrafts will be equipped with ADS-B devices in order to share precise surveillance and location data among the aircrafts, ground controllers and, possibly, other third parties. ADS-B is expected to reduce air traffic congestion and mitigate Air Traffic Control (ATC) inefficiencies significantly in shared airspace.**

The purpose of the e-enabled aircraft communication system is to provide involving entities with highly integrated information that helps performance of air traffic management in an unpredictable and unforgiving operational environment. Flight deck crews in the e-enabled aircrafts will experience enhanced situational awareness, and their decision-making ability can be improved dramatically. Air traffic controllers can benefit from such systems by optimally

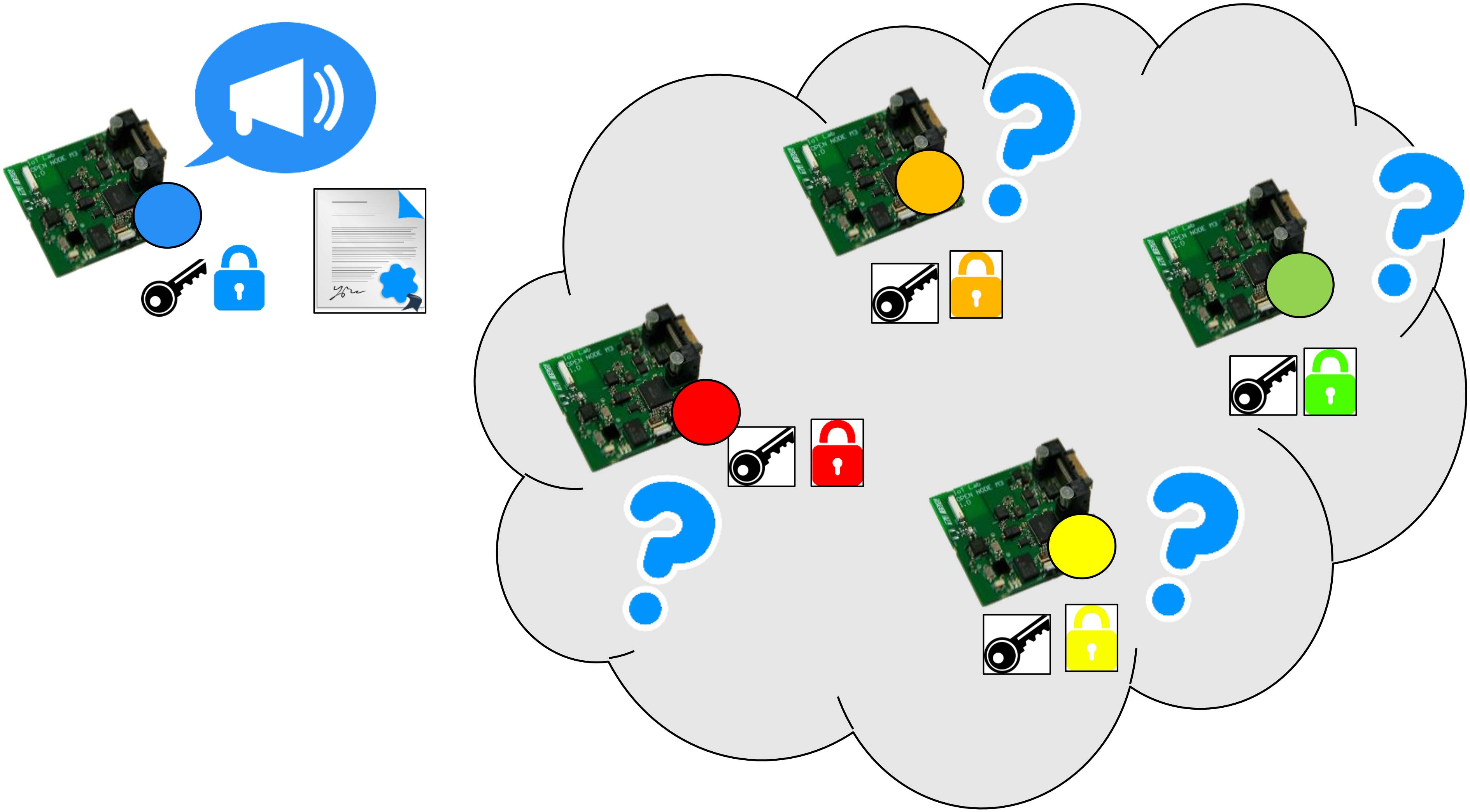
Key revocation in IBS: generation of new key material



Key revocation: formation of new group



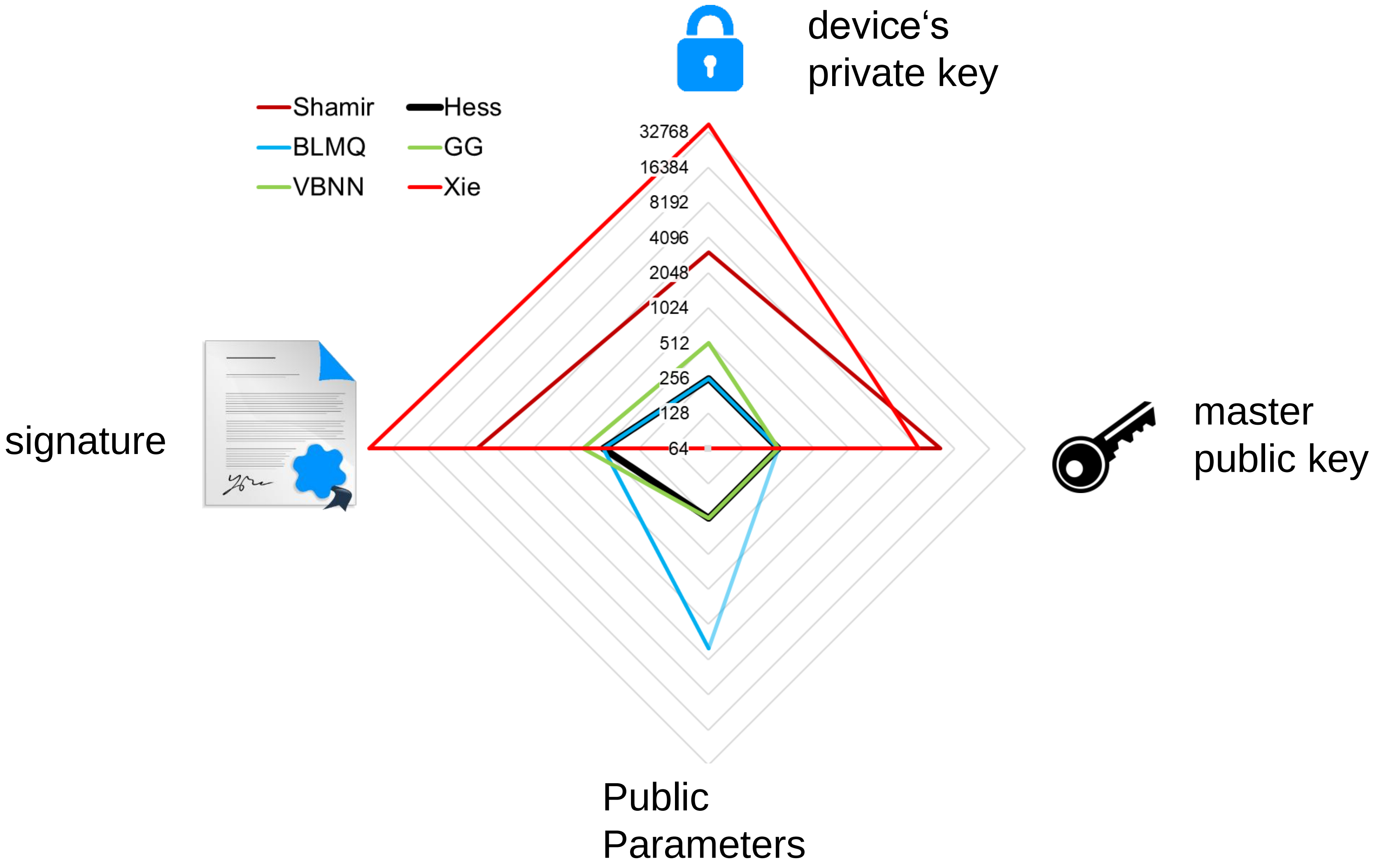
Key revocation: verification fails for excluded devices



Are Identity-Based Signatures viable in constrained networks?

- Parameter sizes
- Power consumption
- Key management

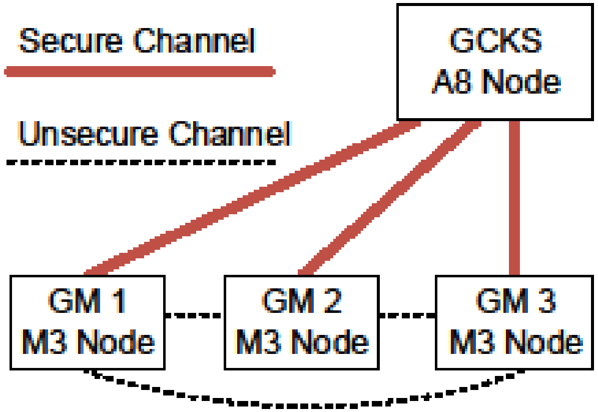
Taxonomy for IBS
comparing sizes in bits



Testing IBS in constrained groups

Tested in IoT-Lab (iot-lab.info):

- 3x M3 Nodes *(= group members)*
  (72 Mhz ARM Cortex M3, 64KB RAM)
  in a multicast domain
- 1x A8 Node *(= TTP)*
  (600 Mhz ARM Cortex A8, 256MB RAM)



Testing IBS in constrained groups

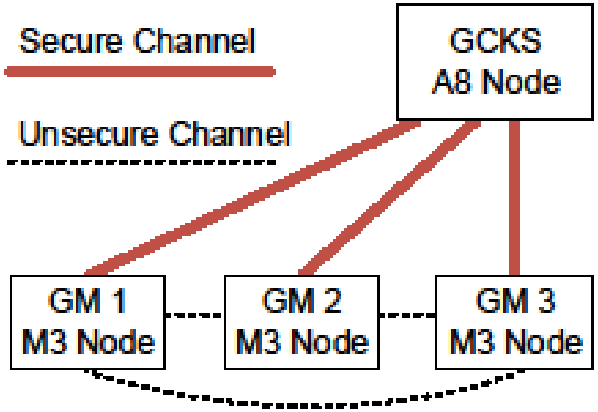
Tested in IoT-Lab (iot-lab.info):

- 3x M3 Nodes *(= group members)*

  (72 Mhz ARM Cortex M3, 64KB RAM)

  in a multicast domain
- 1x A8 Node *(= TTP)*

  (600 Mhz ARM Cortex A8, 256MB RAM)



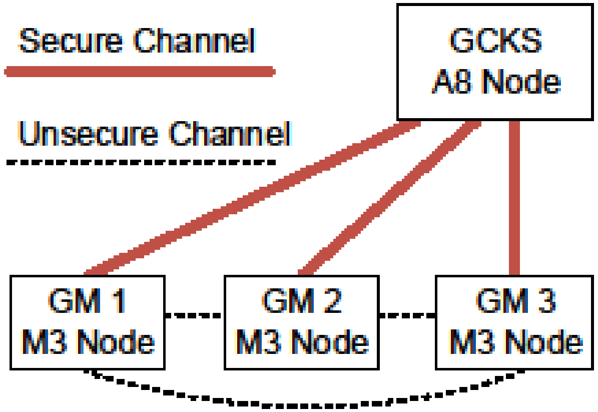
Tested for 2 IBS-schemes

- “VBNN” (Cao et al., 2008, based on Elliptic Curve Cryptography (ECC))
- “BLMQ” (Barreto et al., 2006, based on ECC with pairings)

Testing IBS in constrained groups

Tested in IoT-Lab (iot-lab.info):

- 3x M3 Nodes *(= group members)*
  (72 Mhz ARM Cortex M3, 64KB RAM)
  in a multicast domain
- 1x A8 Node *(= TTP)*
  (600 Mhz ARM Cortex A8, 256MB RAM)



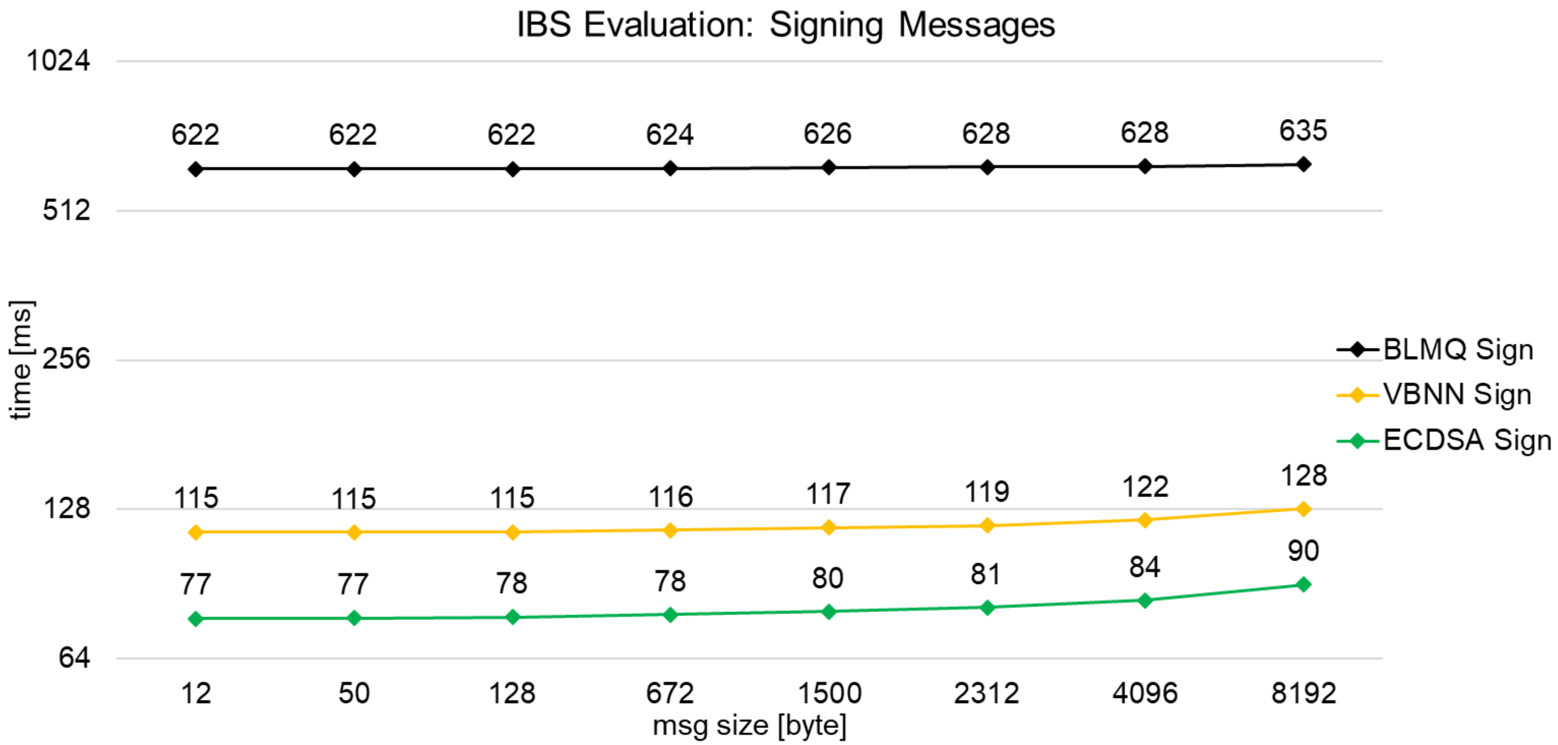
Tested for 2 IBS-schemes

- “VBNN” (Cao et al., 2008, based on Elliptic Curve Cryptography (ECC))
- “BLMQ” (Barreto et al., 2006, based on ECC with pairings)

Implementation

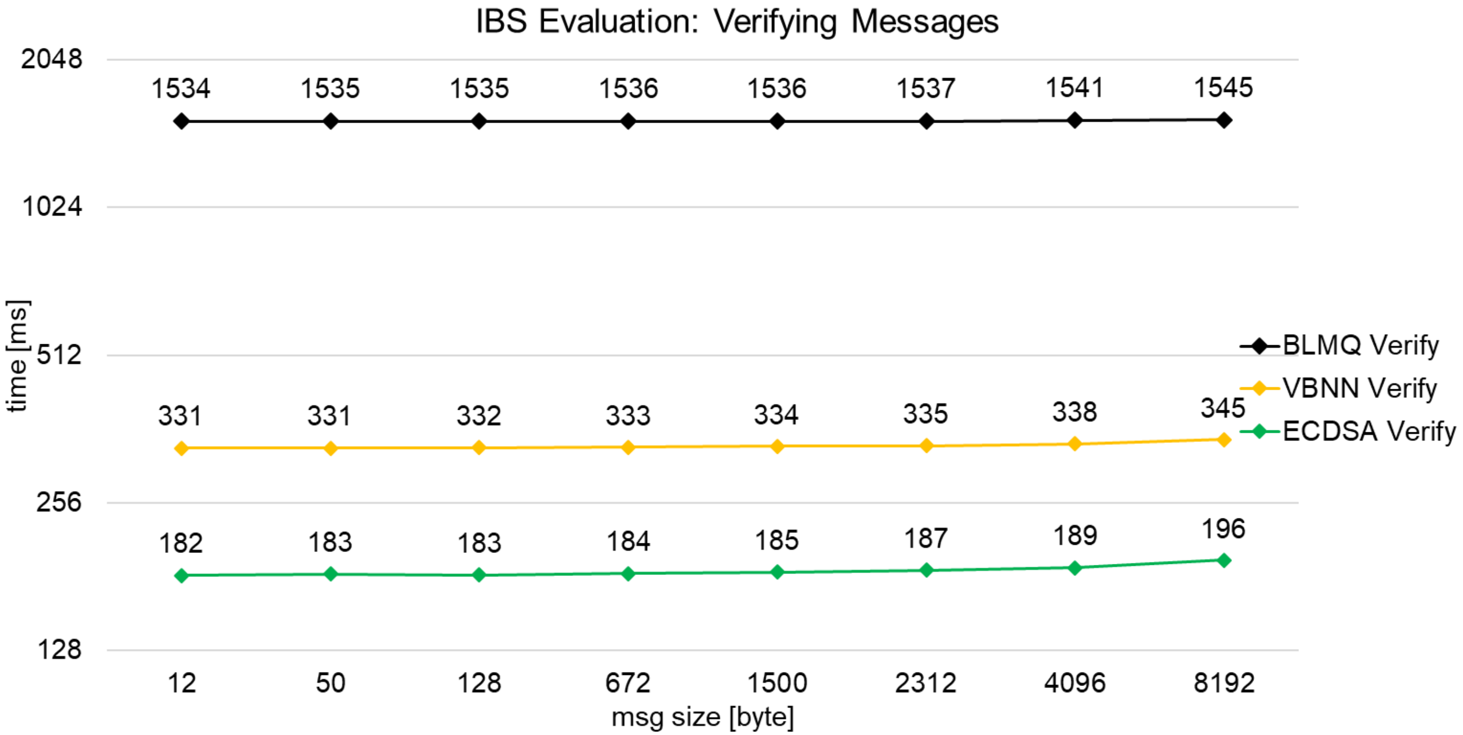
- Operating System: RIOT (https://riot-os.org)
- Cryptographic library: Relic (https://github.com/relic-toolkit/relic)

Testing IBS in constrained groups



Time consumption for signing one message

Testing IBS in constrained groups



Time consumption for verifying one message

Key management challenges

Key management for the group

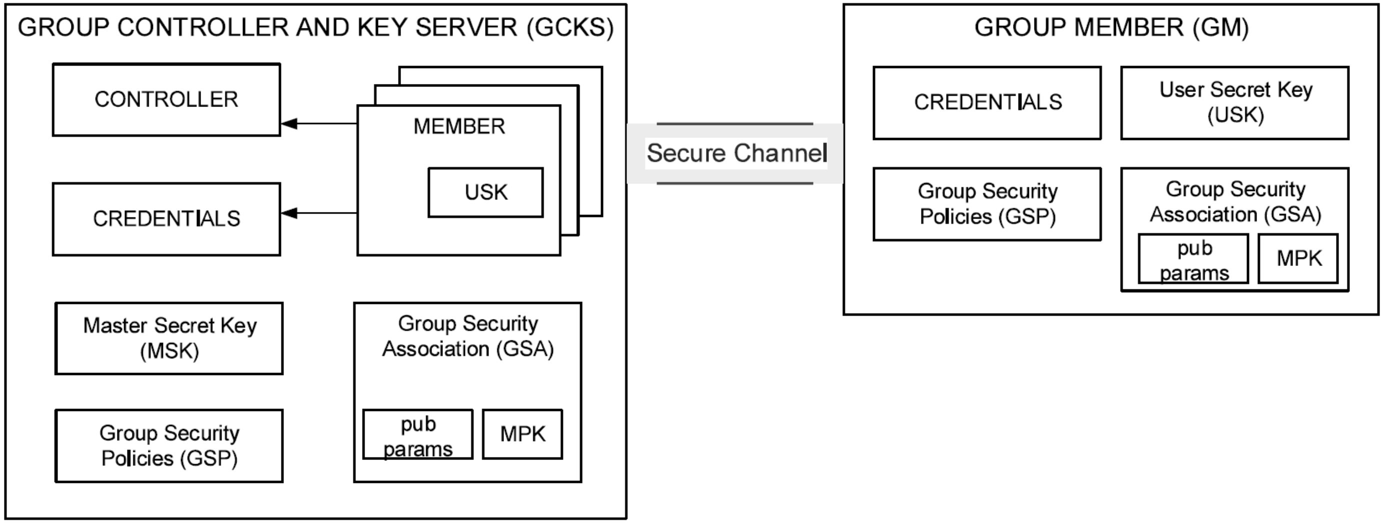
- Identification
- Authorization
- Key distribution

IBS in existing key management architectures

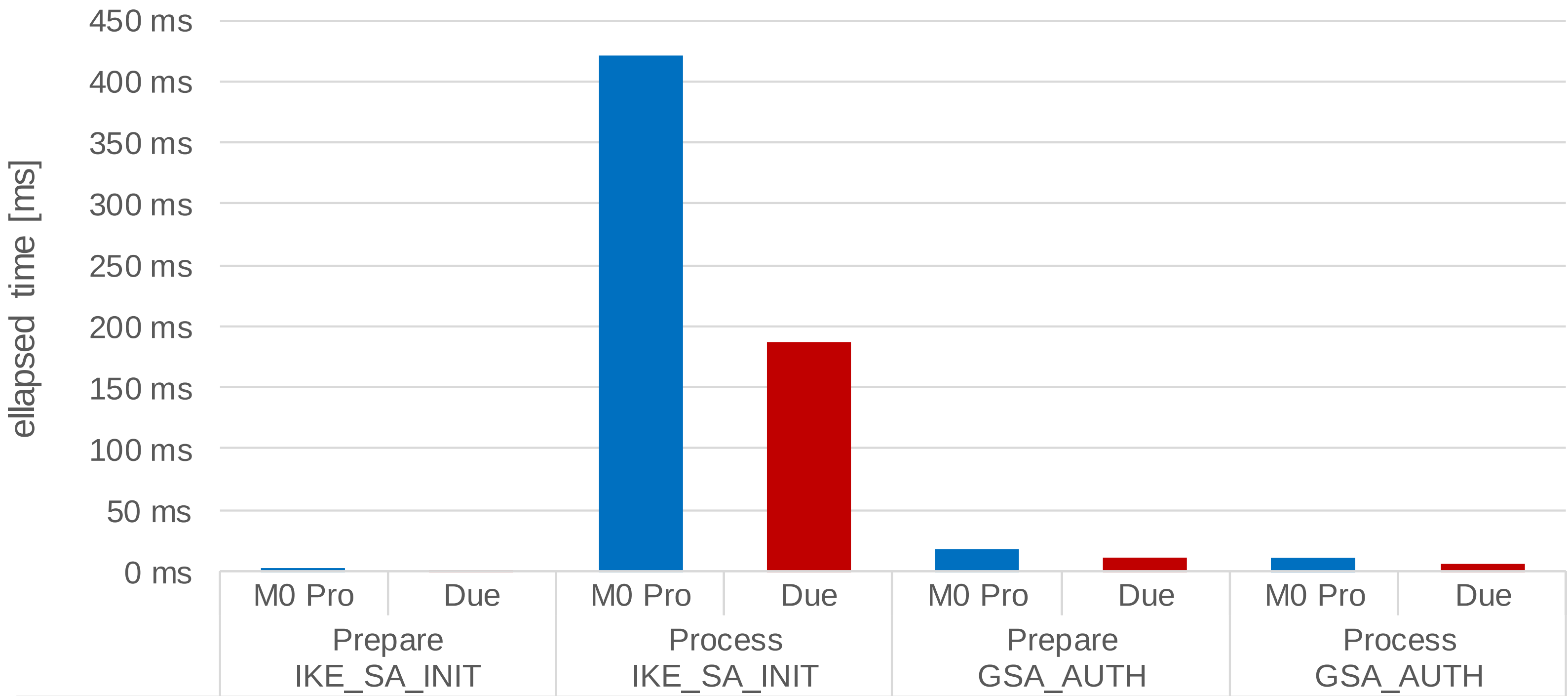
Key management for the group

- Identification
- Authorization
- Key distribution

➔ Use group key infrastructure as in RFC 4046


GROUP CONTROLLER AND KEY SERVER (GCKS)
CONTROLLER
MEMBER
USK
CREDENTIALS
Master Secret Key (MSK)
Group Security Association (GSA)
pub params
MPK
Group Security Policies (GSP)
Secure Channel
GROUP MEMBER (GM)
CREDENTIALS
User Secret Key (USK)
Group Security Policies (GSP)
Group Security Association (GSA)
pub params
MPK

IBS in existing key management architectures: Group IKEv2



	Prepare IKE_SA_INIT		Process IKE_SA_INIT		Prepare GSA_AUTH		Process GSA_AUTH	
	M0 Pro	Due	M0 Pro	Due	M0 Pro	Due	M0 Pro	Due
avg [ms]	2,62	1,62	421,94	187,92	17,41	10,29	10,53	6,32
std. dev. [ms]	0,00	0,00	0,13	0,11	0,00	0,00	0,00	0,40
min [ms]	2,62	1,62	421,71	187,72	17,41	10,29	10,52	6,15
max [ms]	2,62	1,62	422,18	188,11	17,41	10,29	10,53	7,26

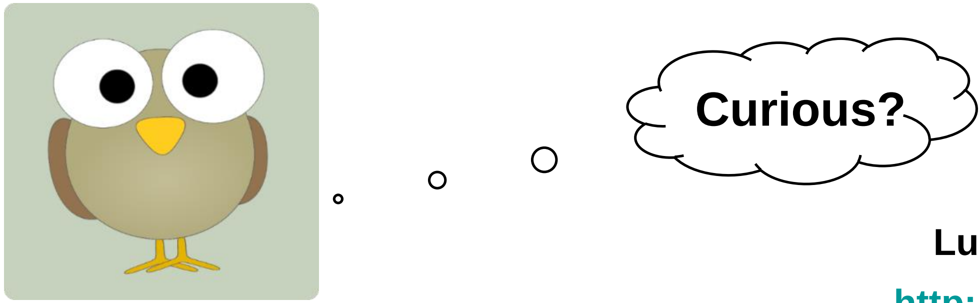
Source: gentschen Felde, N., Guggemos, T., Heider, T., Kranzlmüller, D., Secure Group Key Distribution in Constrained Environments with IKEv2, Proceedings of 2017th IEEE Conference on Dependable and Secure Computing, IEEE, Taipei , Taiwan , August, 2017.

Future work

- extended evaluation with additional devices
- experimental comparison to certificate-based approaches
- evaluate Hierarchical IBS
- more efficient re-keying in IBS

Summary

- discussion of IBS in groups
  - mathematically sound key revocation
  - integration in key management architectures
- taxonomy for scheme comparison
- testing and measurements of using IBS on constrained devices



Sophia Grundner-Culemann

MNM-Team

Ludwig-Maximilians-Universität München

http://www.mnm-team.org/projects/embedded