Freie Universität Berlin

# „Sicherheit im Internet der Dinge leicht gemacht“
# (- Security Made Easy in the IoT)

OMNUISECURE, Berlin 24.01.2018

Gerhard Wunder

FU-Berlin, Heisenberg CIT Group
Head of Group

# Goal of Talk

- Short introduction on Physical Layer Security technologies for securing the IoT
- Physical Layer Security: Establishing security in wireless system exploiting the physical (wireless) environment and other physical layer parameters

*Acknowledgement:*

*PROPHYLAXE (www.ict-prophylaxe.de, CO), the biggest German project on Physical Layer Security in the Internet of Things, nominated 2017 for Deutscher Zukunftspreis by the BMBF (GW, Dr. Andreas Müller BOSCH, Prof. Christoph Paar, RUB)*

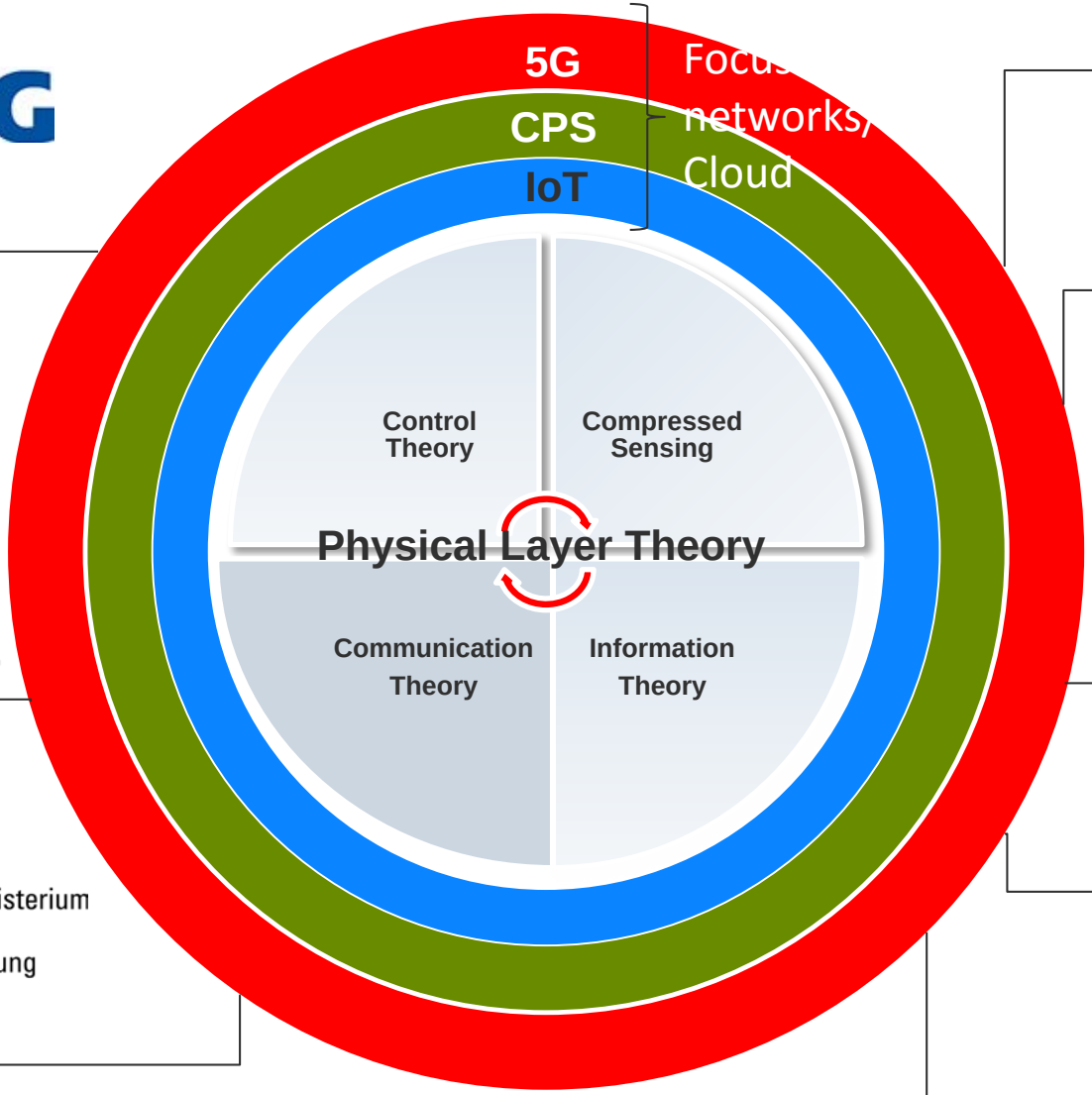
G. Wunder, A. Müller, C. Paar et al, Sicherheit im Internet der Dinge leicht gemacht, Nominierungsschrift für den dt. Zukunftspreis 2017, erscheint in Industrie 4. 0 Management, Januar 2018

# Core Competencies, Portfolio

Freie Universität Berlin

CPN
SPP 1914

DFG




ONE5G

H2020
~8 Mi €

PhasmaFood

H2020
~3 Mi €

H2020
AutoKEY

WiSHFUL

RACOON

S. Korea
ETRI

CoSIP
CSMIMO

DFG
SPP 1798

Bundesministerium
für Bildung
und Forschung

SecureFog

CoSIP
SecCS

DFG
SPP 1798

# IoT Security Attacks

Freie Universität Berlin

**Security is key to IoT market!**

- Recent attack (Oct. 2017) on 4-way handshake of the WPA2 protocol in WiFi
- DDoS attack on Dyn servers by manipulating embedded IoT devices such as IP cameras, printers, routers etc. to to create Mirai botnet (Oct. 2016)

| Username/Password | Manufacturer | Link to supporting evidence |
|---|---|---|
| | | |
| admin/123456 | ACTi IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/anko | ANKO Products DVR | http://www.cctvforum.com/viewtopic.php?f=3&t=44250 |
| root/pass | Axis IP Camera, et. al | http://www.cleancss.com/router-default/Axis/0543-001 |
| root/vizxv | Dahua Camera | http://www.cam-it.org/index.php?topic=5192.0 |
| root/888888 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/666666 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/7ujMko0vizxv | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| root/7ujMko0admin | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| 666666/666666 | Dahua IP Camera | http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C |
| root/dreambox | Dreambox TV receiver | https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/ |
| root/zlxx | EV ZLX Two-way Speaker? | ? |
| root/juantech | Guangzhou Juan Optical | https://news.ycombinator.com/item?id=11114012 |
| root/xc3511 | H.264 - Chinese DVR | http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15 |
| root/hi3518 | HiSilicon IP Camera | https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/ |
| root/klv123 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/klv1234 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/jvbzd | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/admin | IPX-DDK Network Camera | http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/ |
| root/system | IQinVision Cameras, et. al | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/meinsm | Mobotix Network Camera | http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/ |
| root/54321 | Packet8 VOIP Phone, et. al | http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411 |
| root/00000000 | Panasonic Printer | https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html |
| root/realtek | RealTek Routers | |
| admin/1111111 | Samsung IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/xmhdipc | Shenzhen Anran Security Camera | https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI |
| admin/smcadmin | SMC Routers | http://www.cleancss.com/router-default/SMC/ROUTER |
| root/ikwb | Toshiba Network Camera | http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en |
| ubnt/ubnt | Ubiquiti AirOS Router | http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm |
| supervisor/supervisor | VideoIQ | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/<none> | Vivotek IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/1111 | Xerox printers, et. al | https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/ |
| root/Zte521 | ZTE Router | http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html |

# IoT Security Challenges

Freie Universität Berlin

- Ideally, even the tiniest and cheapest platforms will provide standard security features such as data encryption, device authentication, and (some) protection against manipulation and denial-of-service attacks

Ressource-constrained devices, light-weight cryptography

No user interfaces, operate in background, “plug-and-secure” operation

Scalable and flexible node management, easy deployment and bootstrapping

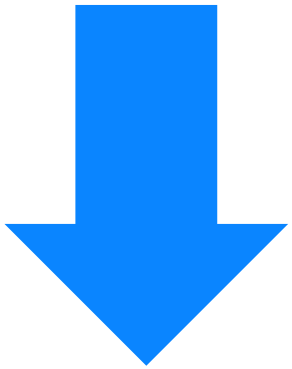
Fast cyphers, fast authentication, fast MitM detection

# IoT Security Challenges

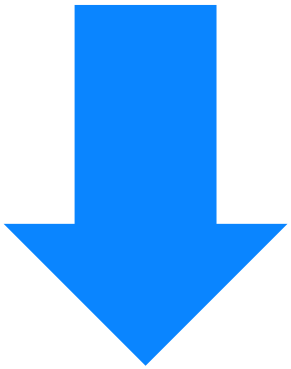
Freie Universität Berlin

Mutually exclusive requirements!

Physical Layer Security a remedy?

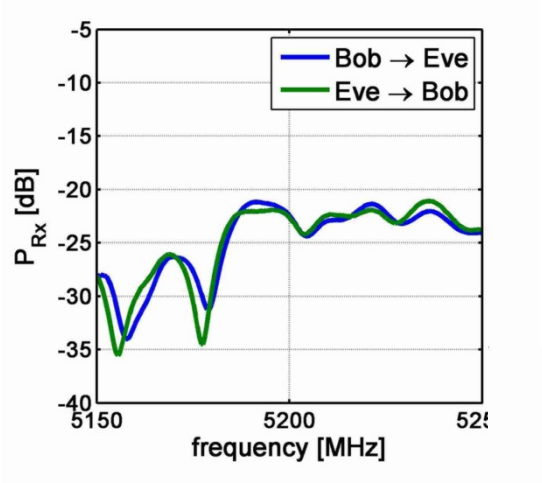


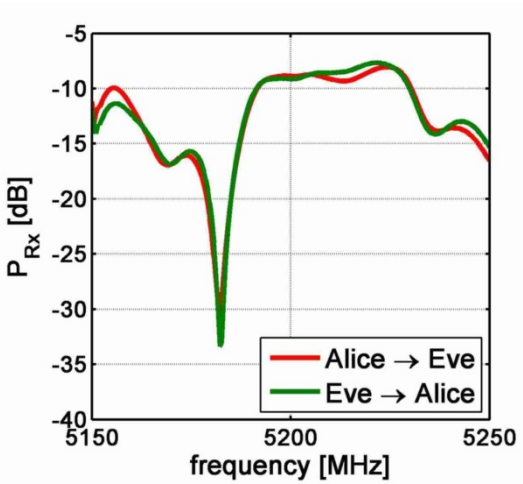
Wiretap Coding (Wyner 1975)



Wireless Channel based Key Generation (Hershey et al 1996)

# Physical Layer Security



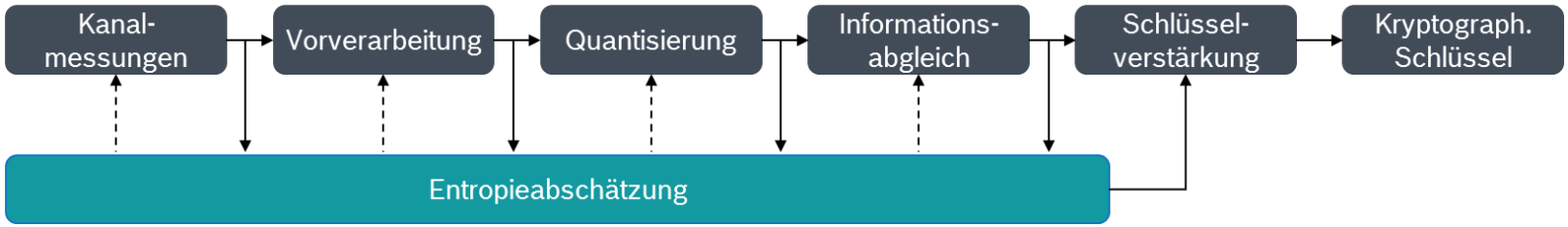



# Physical Layer Security

Freie Universität Berlin

Key messages from PROPHYLAXE:

- Correctness of technology:
  - Reliable IoT autonomous key management (with AES or 3DES) for off-the-shelf Wifi, ZigBee etc. simply by firmware updates



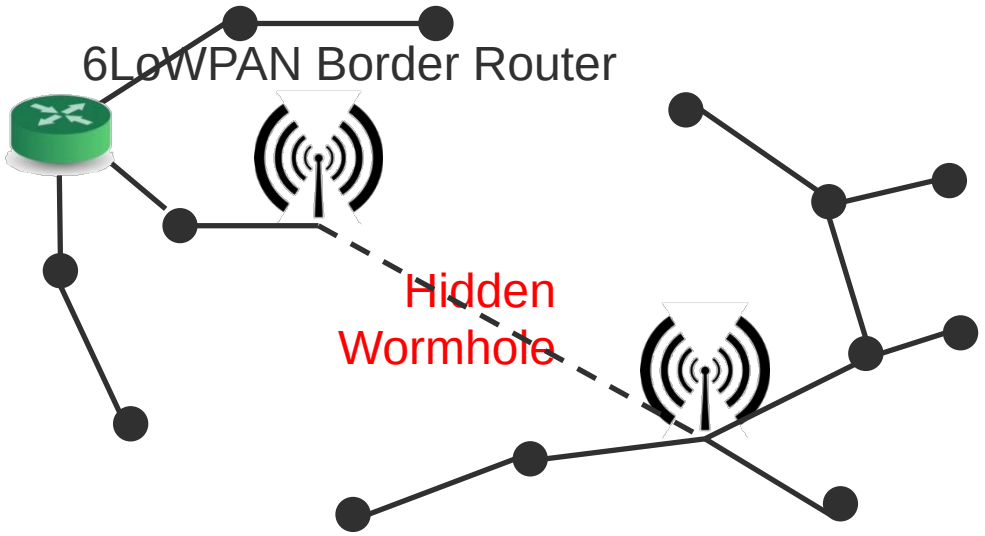

  - Key strengths and key generation rates often sufficient but depending on mobility scenarios
- Security of technology:
  - Keys typically not recoverable outside some critical distance
  - Interplay with AES and 3DES for secure IoT
  - Very favourable tradeoffs: linear vs kubic complexity

C. T. Zenger, M.-J. Chur, J.-F. Posielek, G. Wunder, C. Paar, A Novel Key Generating Architecture for Wireless Low-Resource Devices, International Workshop on Secure Internet of Things (SIoT), 2014

# SCREWED

## Fast MitM detection

- “SCREWED”- a complete solution for detecting wormholes/MitM in 6LoWPAN networks
- Very fast and efficent, uses only PHY command frames (detection within ms !)
- Implemented in Contiki Kernel
- Extended towards bootstrapping and preventing „spoofing“ (6doku protocol)



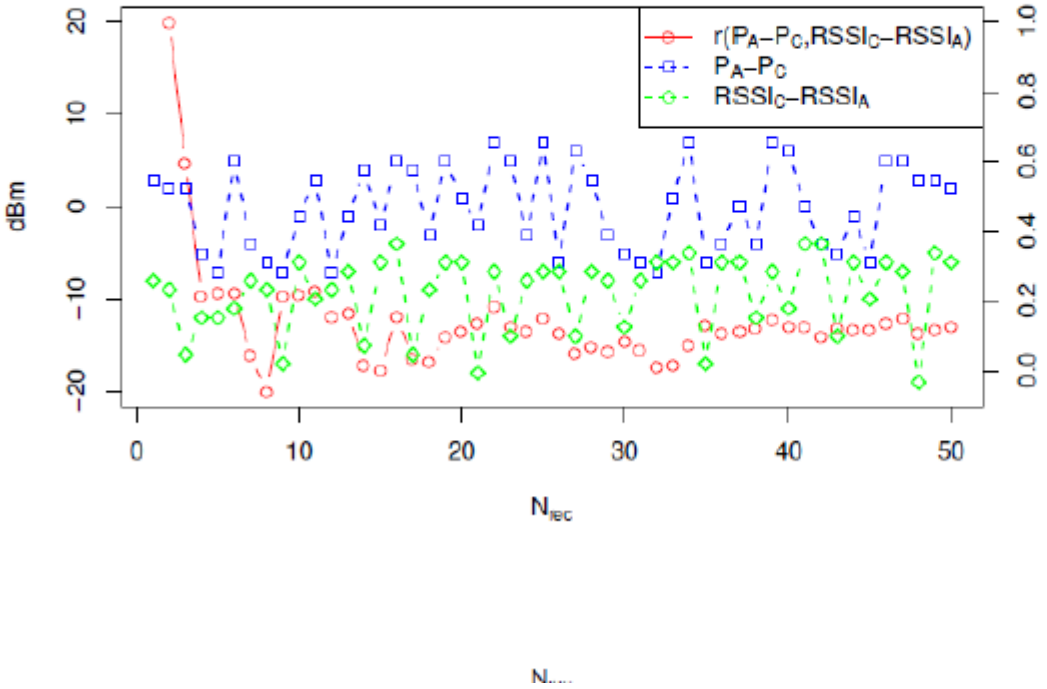


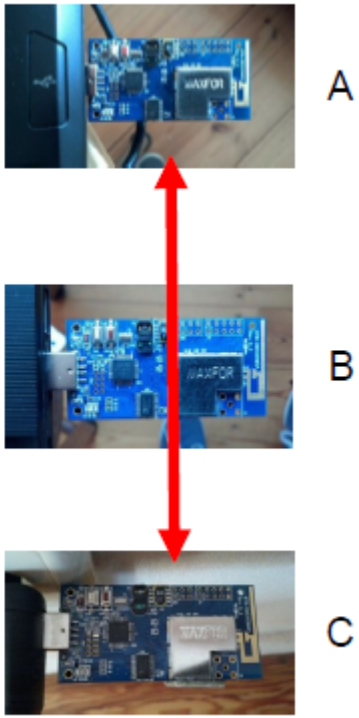
K. F. Krentz, G. Wunder, 6doku: Towards Secure Over-the-Air Preloading of 6LoWPAN Nodes using PHY Key Generation, Smart SysTech 2015: European Conference on Smart Objects, Systems and Technologies, Aachen, Germany, June 2015, published by IEEE

G. Wunder, R. Fritschek, and R. Khan, “RECiP: Wireless Channel Reciprocity Restoration Method for Varying Transmission Power”, IEEE Symposium on Personal and Indoor Mobile Radio Communications (PIMRC), 2016

K. Krentz and G. Wunder, 6LoWPAN Security: Avoiding Hidden Wormholes using Channel Reciprocity, ACM Int. Workshop on Trustworthy Embedded Devices, (TrustED 2014), Scottsdale (USA)

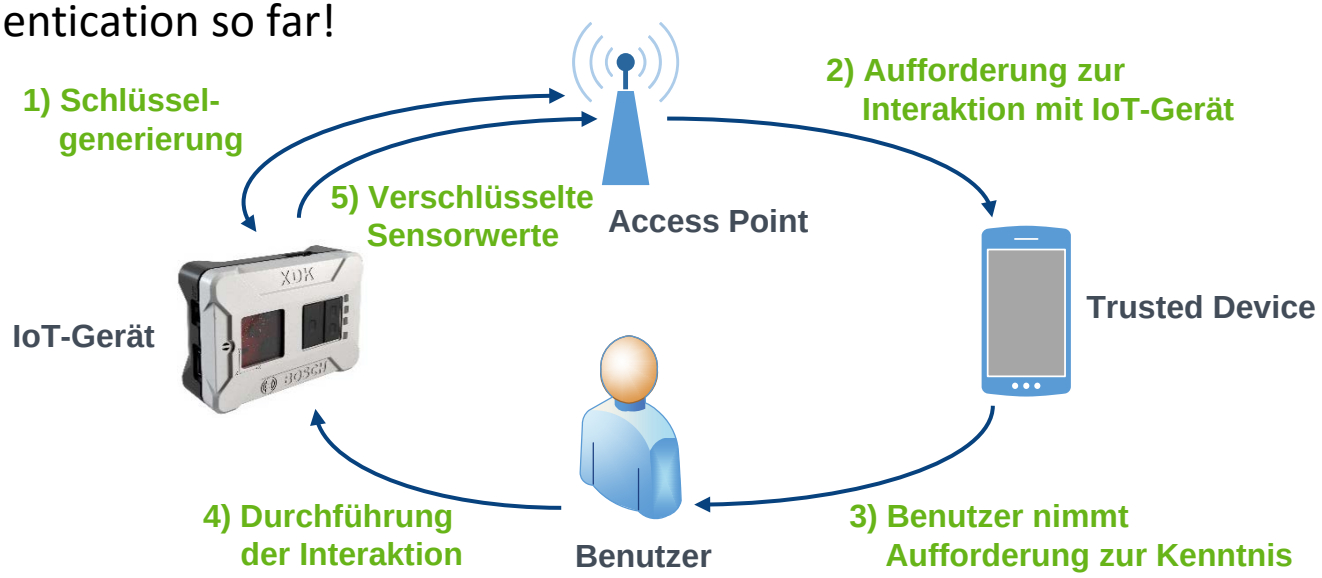
# Physical Layer Security



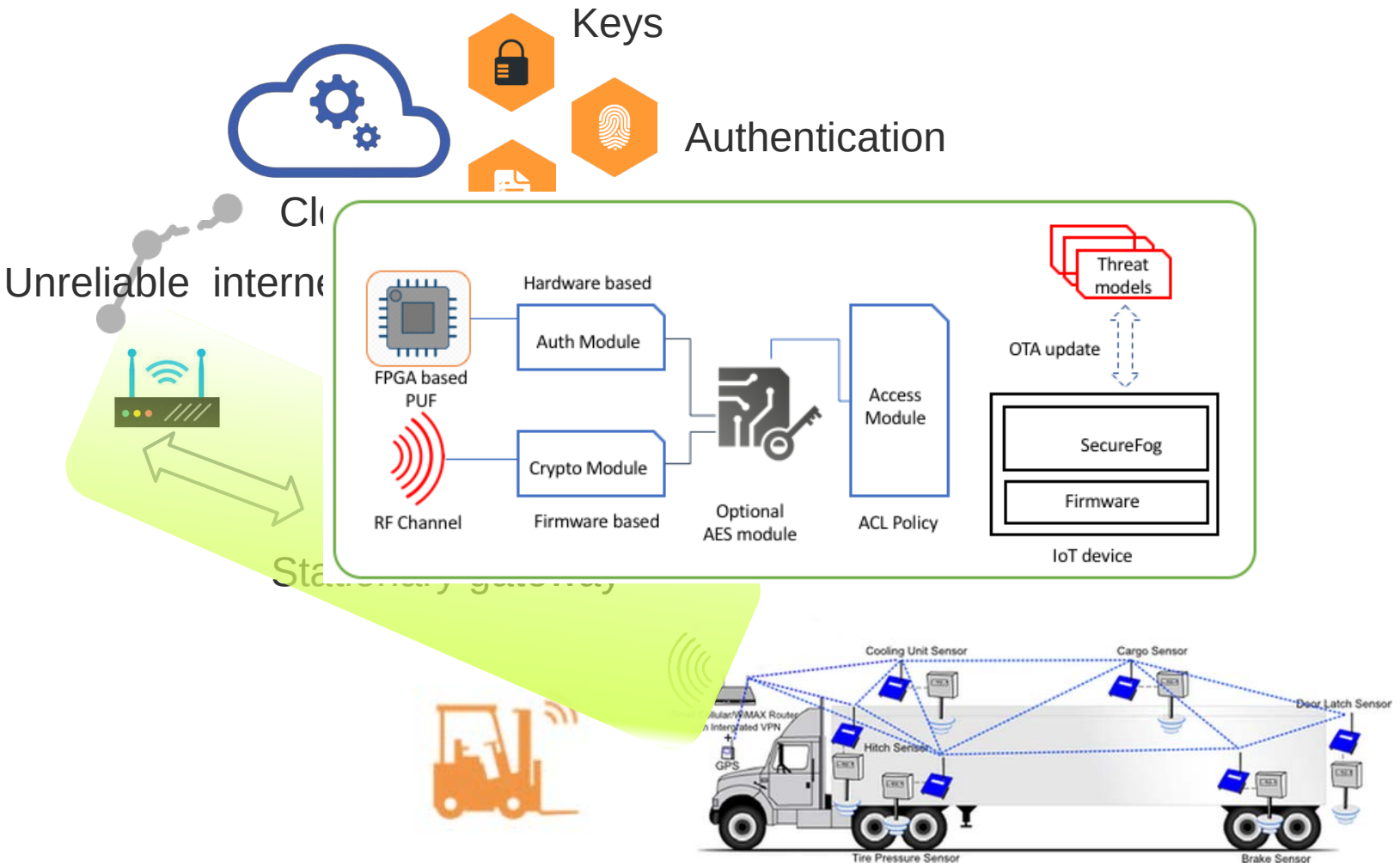
# Conclusions

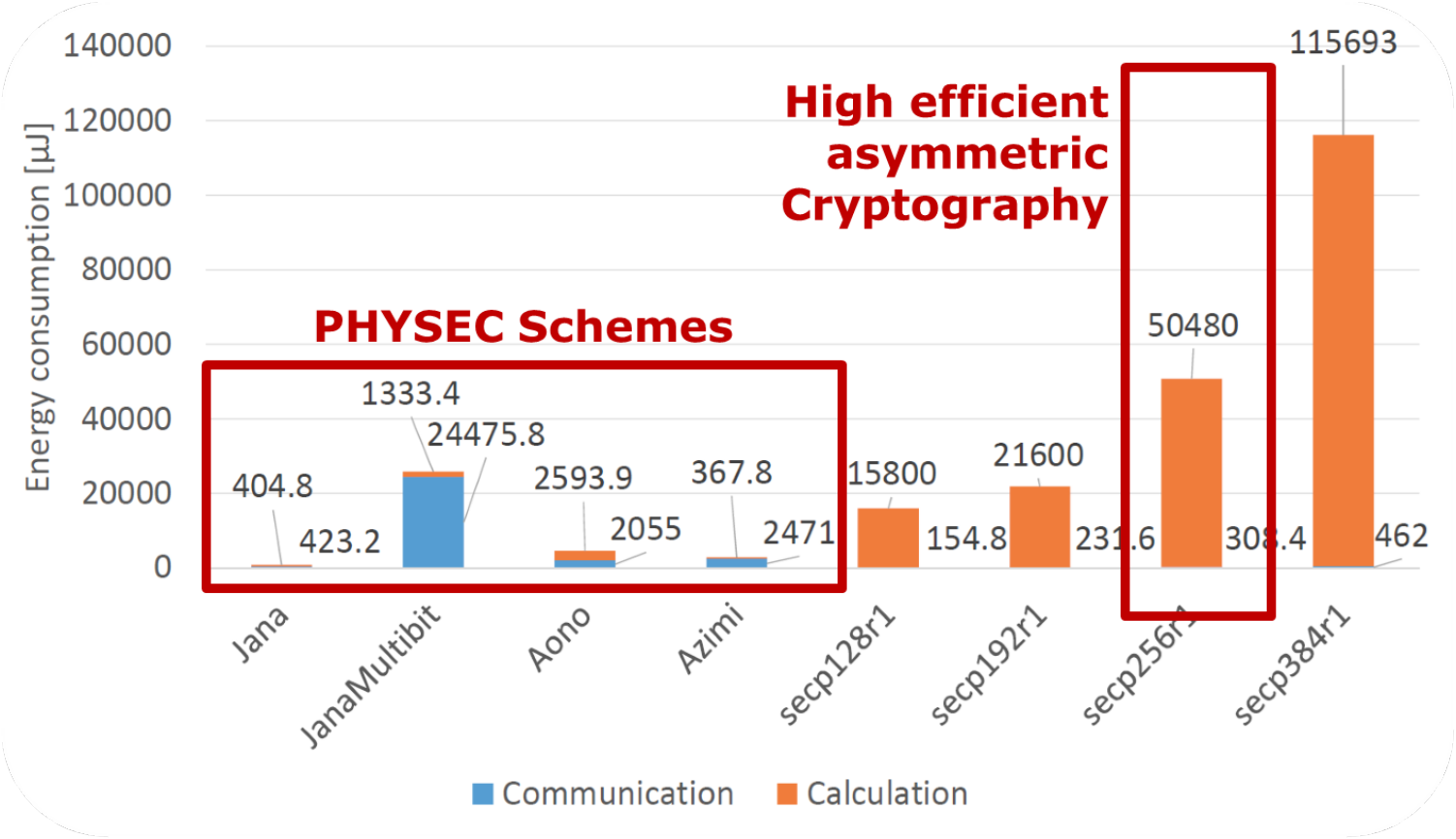
- PHYSEC provides a plethora of new ideas, challenges and opportunities!
- Major research to be done:
  - Modeling the physical environment
  - Combine HW- and SW-based security anchors (project SecureFog)
  - Bridging CRYPTO and PHYSEC (“our deterministic model”)
  - Leverage 5G++ PHYSEC
  - Nothing about authentication so far!



# SecureFog

## The Logistics Scenario

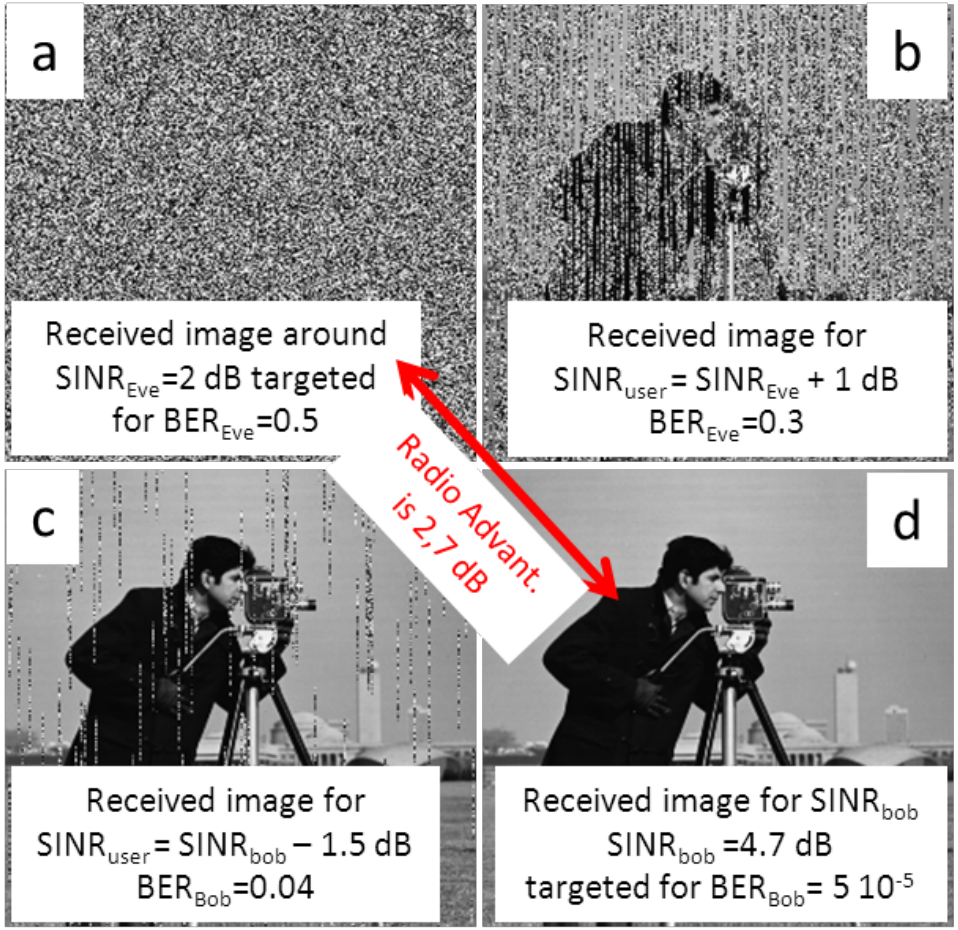




# Physical Layer Security

## Wiretap coding

- Good wiretap codes available
- **Problem**: How to gurantee the advantage of Bob over Eve? No clear threshold




F. Delaveau, A. Mueller, C. Kameni Ngassa, R. Guillaume, R. Molière, G. Wunder, Perspectives of Physical Layer Security (Physec) for the improvement of the subscriber privacy and communication confidentiality at the Air Interface, ETSI Workshop, 2016