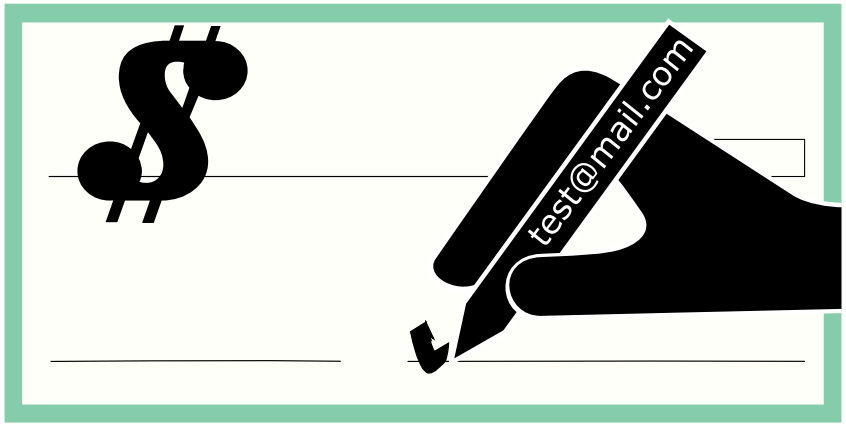
Tobias Guggemos
MNM-Team
Ludwig-Maximilians-Universität München

An architecture for dynamic key management in embedded systems

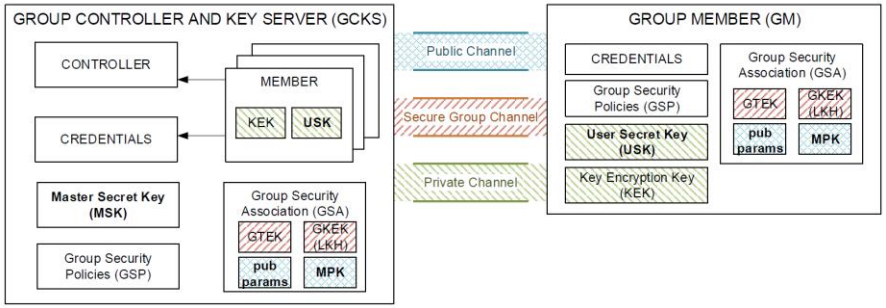
CGW Workshop ´18

Lets start at the end...

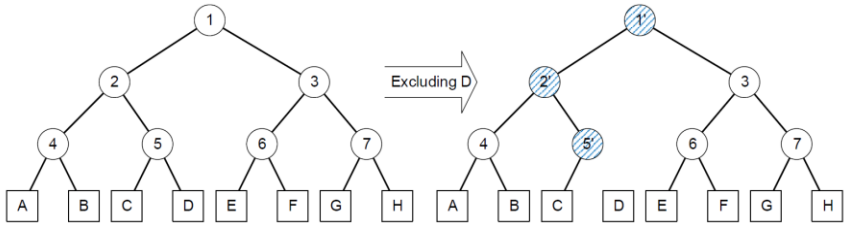
Identity Based Signatures



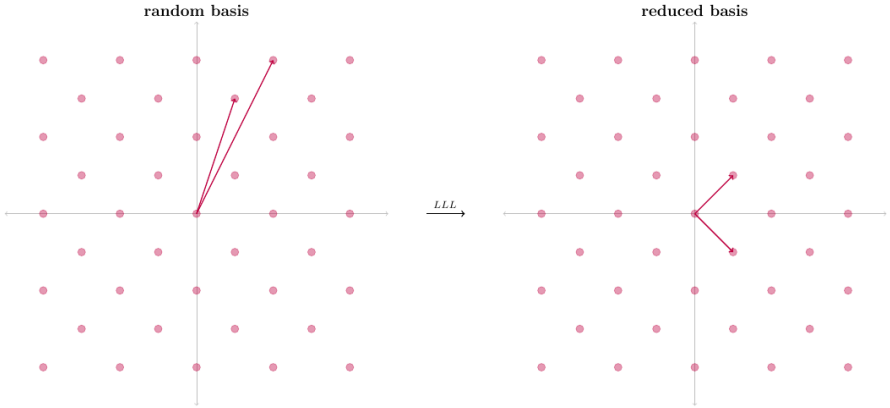
Group Key Security Architecture



Group Key Security Protocols

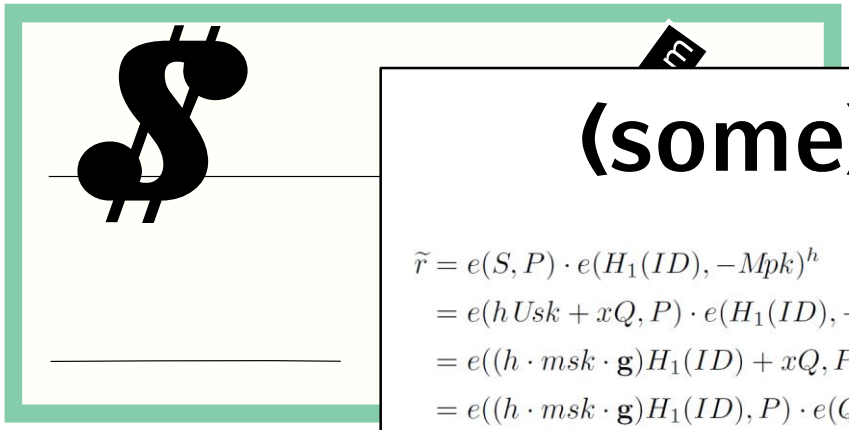


(PostQuantum) Cryptography

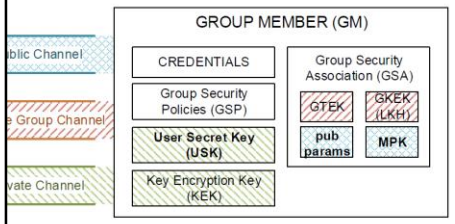


Lets start at the end...

Identity Based Signatures



Group Key Security Architecture

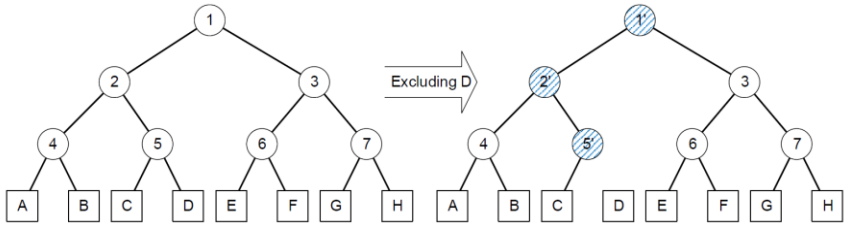


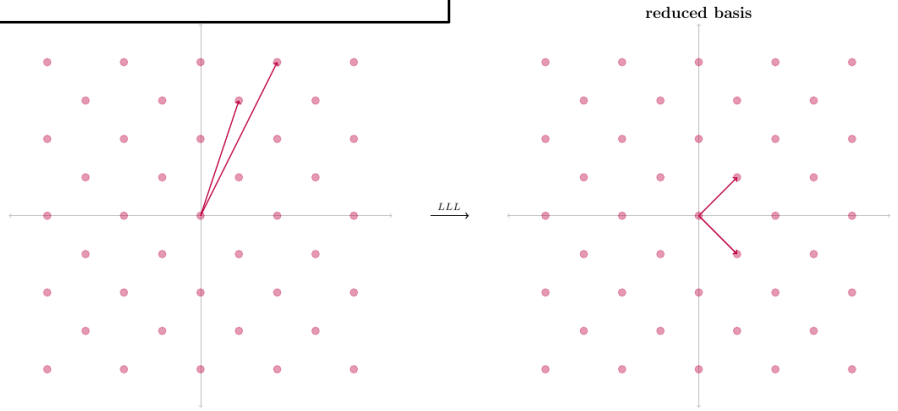
(some) maths

$$
\begin{aligned}
\widetilde{r} &= e(S,P)\cdot e(H_1(ID),-Mpk)^h && = \\
&= e(h\,Usk + xQ, P)\cdot e(H_1(ID),-Mpk)^h && = \\
&= e((h\cdot msk\cdot \mathbf{g})H_1(ID) + xQ, P)\cdot e(H_1(ID),-(msk\cdot \mathbf{g})P)^h && = \\
&= e((h\cdot msk\cdot \mathbf{g})H_1(ID), P)\cdot e(Q,P)^x \cdot e(H_1(ID),-(msk\cdot \mathbf{g})P)^h && = \\
&= e(H_1(ID),P)^{h\cdot msk\cdot \mathbf{g}}\cdot e(Q,P)^x \cdot e(H_1(ID),P)^{-h\cdot msk\cdot \mathbf{g}} && = \\
&= e(Q,P)^x
\end{aligned}
$$

Group Key Se

) Cryptography

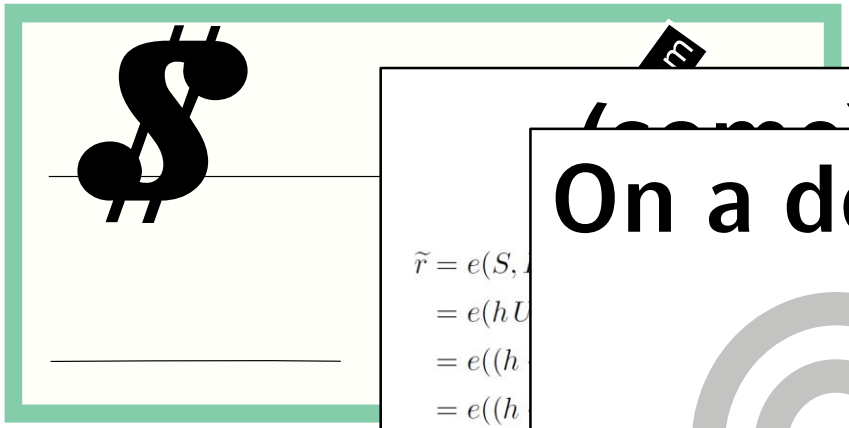


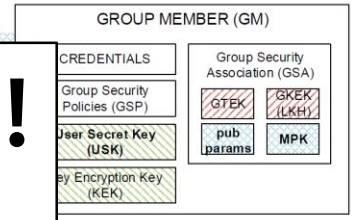


Lets start at the end…

Identity Based Signatures

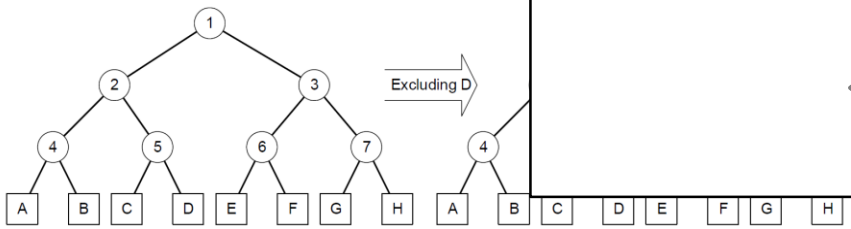
Group Key Security Architecture

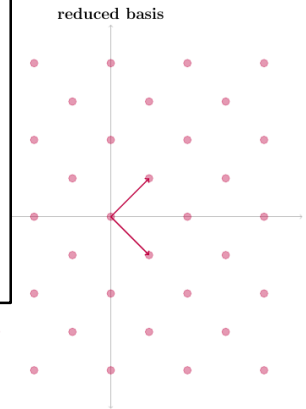




Group Key Se

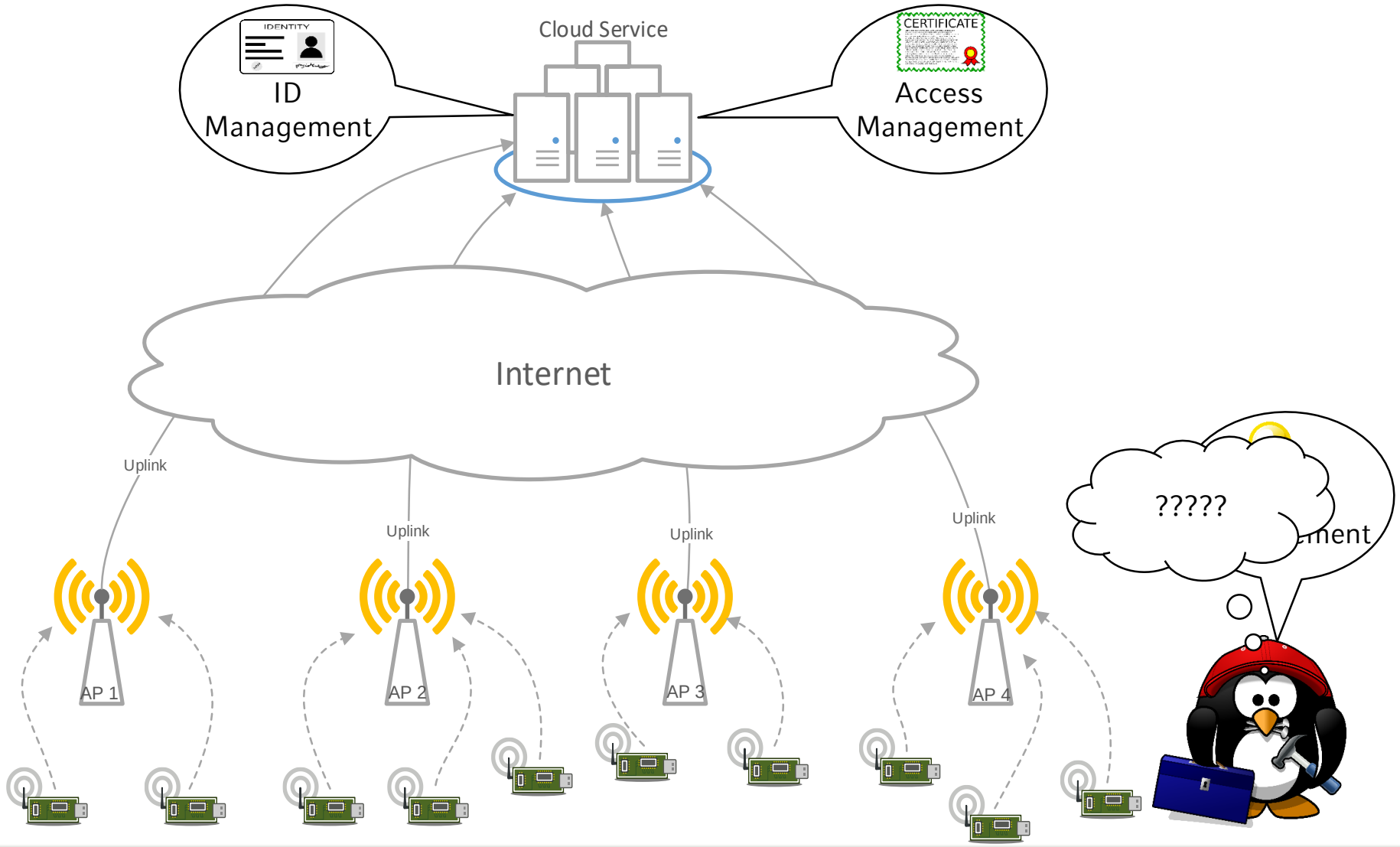
otography





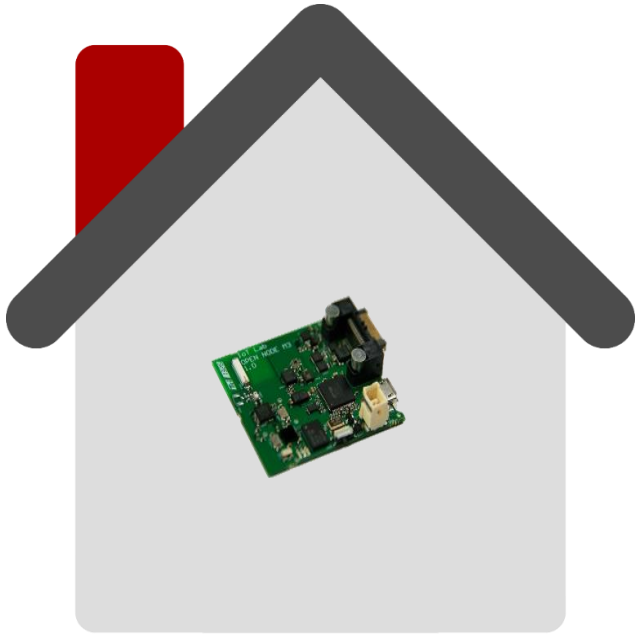
On a device like that!

Typical IoT Management Architecture



Classic Key Management

build trust
Exchange keys



communicate
- encrypt
- integrity check
- authenticate

set up
Key Generation

Key Revocation

What happens if the scenarios get dynamic?

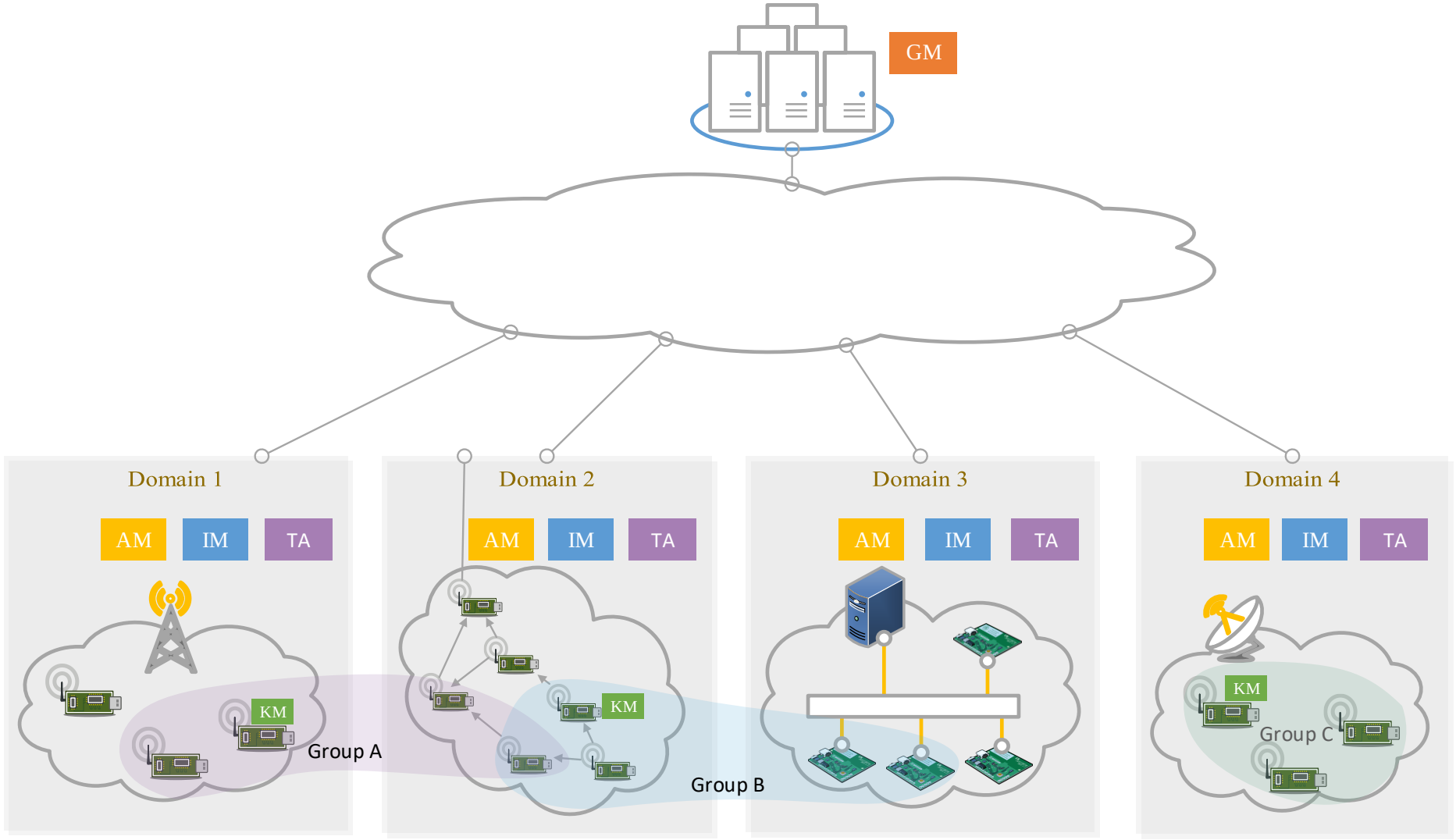
build trust
Exchange keys

communicate
- encrypt
- integrity check
- authenticate

set up
Key Generation

Key Revocation

Proposed Architecture

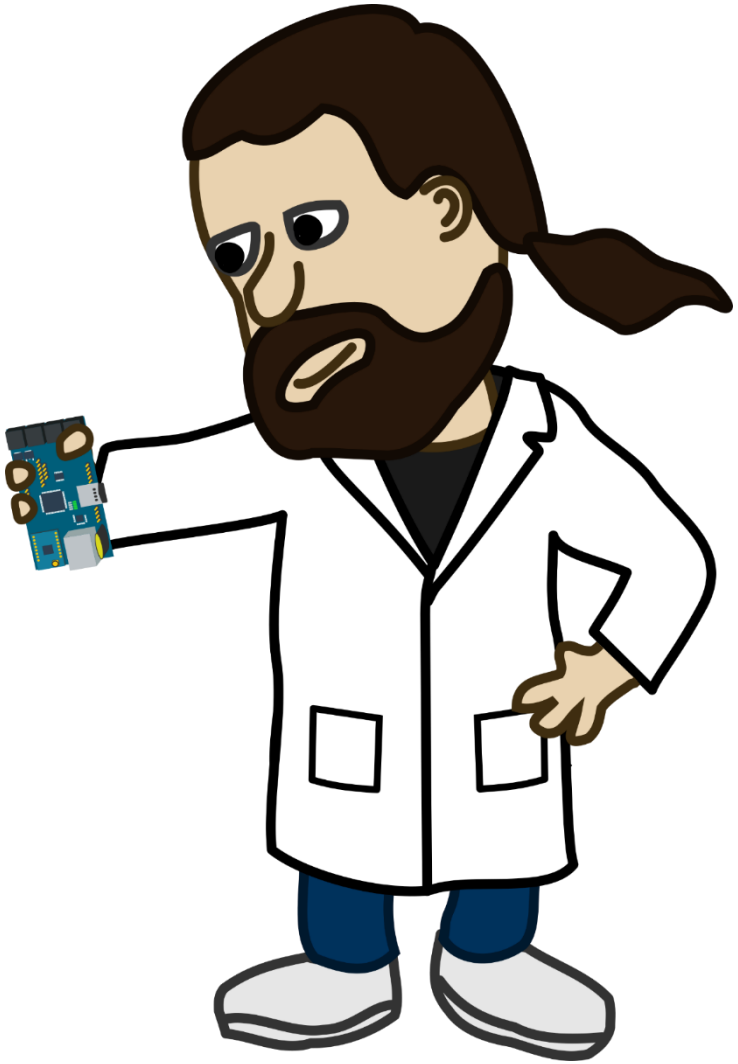


Goals and Challenges

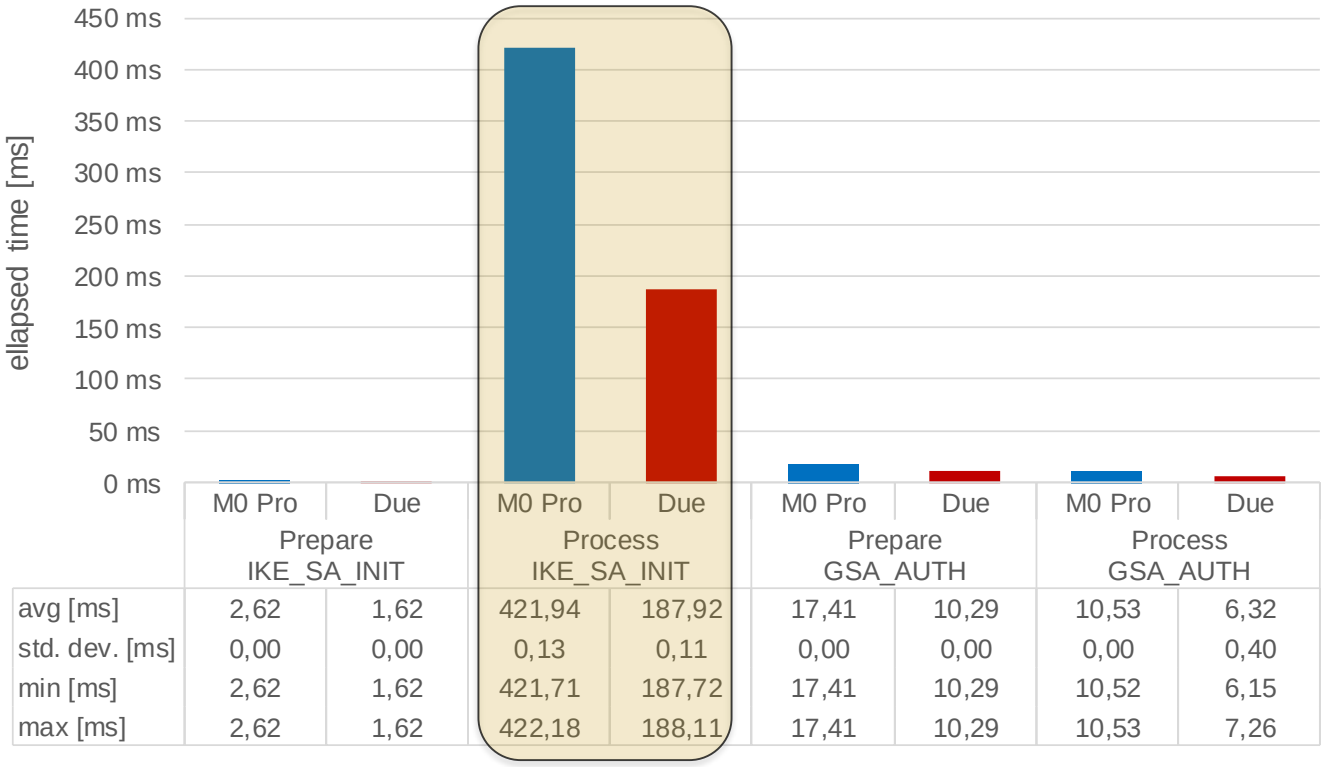
- Making transport protocols ready for embedded devices
  - IPsec/ESP
- Making key management architecture suitable for embedded devices
  - IKEv2, G-IKEv2
- Finding promissing cryptographic primitives and improve their keys management
  - Identity Based Signatures
  - Hash-Based Signatures

➔ Only few (open source) implementations available

A few results



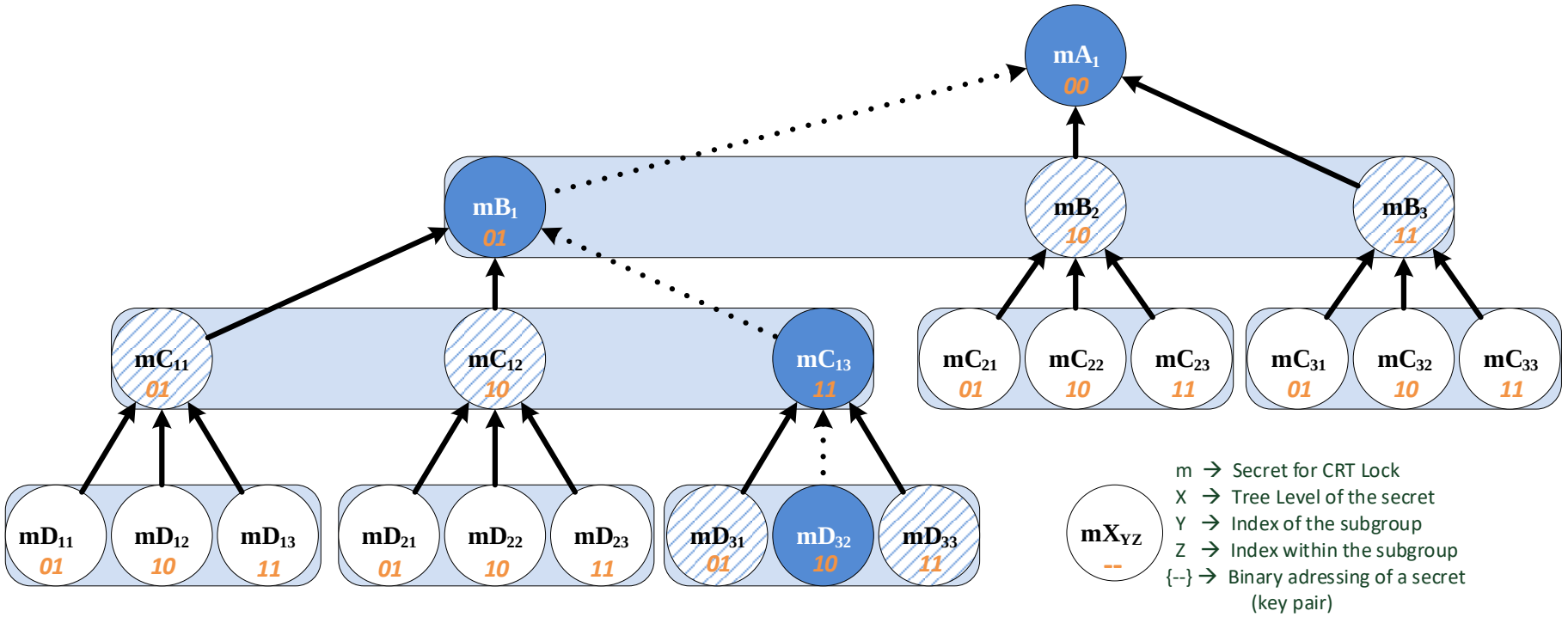
Key Management – 1



	M0 Pro	Due	M0 Pro	Due	M0 Pro	Due	M0 Pro	Due
	Prepare IKE_SA_INIT		Process IKE_SA_INIT		Prepare GSA_AUTH		Process GSA_AUTH	
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

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.

Key Management – 2



Guggemos, T., Streit, K., Knüpfer, M., gentschen Felde, N., Hillmann, P., No Cookies, just CAKE: CRT based Key Hierarchy for Efficient Key Management in Dynamic Groups, In *to appear in: 13th International Conference for Internet Technology and Secured Transactions (ICITST–2018)* , 2018, 13, IEEE, Dezember, 2018.

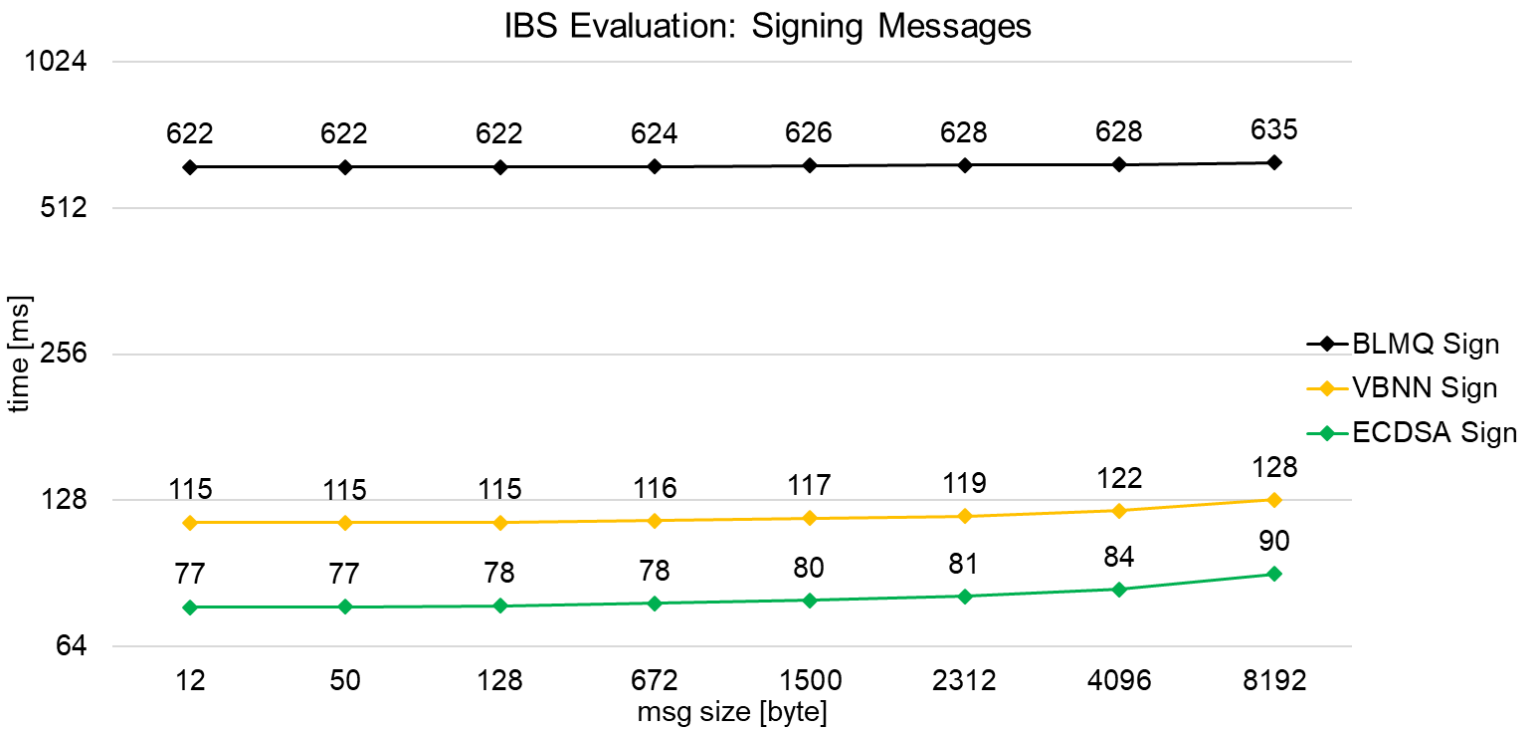
Identity Based Signatures (IBS)

	Hess	BLMQ
Setup	$msk \leftarrow \mathbb{Z}_p^*$ $Mpk = msk\ P$	$msk \leftarrow \mathbb{Z}_p^*$ $Mpk = msk\ P$
Extract	$Usk = msk\ H_1(ID)$	$Usk = \frac{1}{msk+h_1(ID)}P$
Re-Key (TTP)	$msk \leftarrow \mathbb{Z}_p^*$ $Mpk = msk\ P$ $Usk = msk\ H_1(ID)$	$msk \leftarrow \mathbb{Z}_p^*$ $Mpk = msk\ P$ $Usk = \frac{1}{msk+h_1(ID)}P$
Sign	1. $x \leftarrow \mathbb{Z}_p^*$, $Q \leftarrow \mathbb{G}^*$ 2. $r = e(Q,P)^x$ 3. $h = h_2(M,r)$ 4. $S = h\,Usk + xQ$ $sig = (h,S)$	1. $x \leftarrow \mathbb{Z}_p^*$ 2. $r = e(P,P)^x$ 3. $h = h_2(M,r)$ 4. $S = (x+h)\,Usk$ $sig = (h,S)$
Verify	$\widetilde{r} = e(S,P) \cdot e(H_1(ID), -Mpk)^h$ $h \stackrel{?}{=} h_2(M,\widetilde{r})$	$\widetilde{r} = e(S,(h_1(ID))P + Mpk) \cdot e(P,P)^{-h}$ $h \stackrel{?}{=} h_2(M,\widetilde{r})$

^{p} prime number ^{P} generator of an ell. curve group $^{\mathbb{G}}$ cyclic group generated by P
$^{\mathbb{Z}_p^*}$ $\mathbb{Z}_p$ without identity ($\mathbb{1}$) element $^{h_i()}$ hash function in $\mathbb{Z}_p$ $^{H_i()}$ hash function in $\mathbb{G}$
^{M} message ^{sig} signature

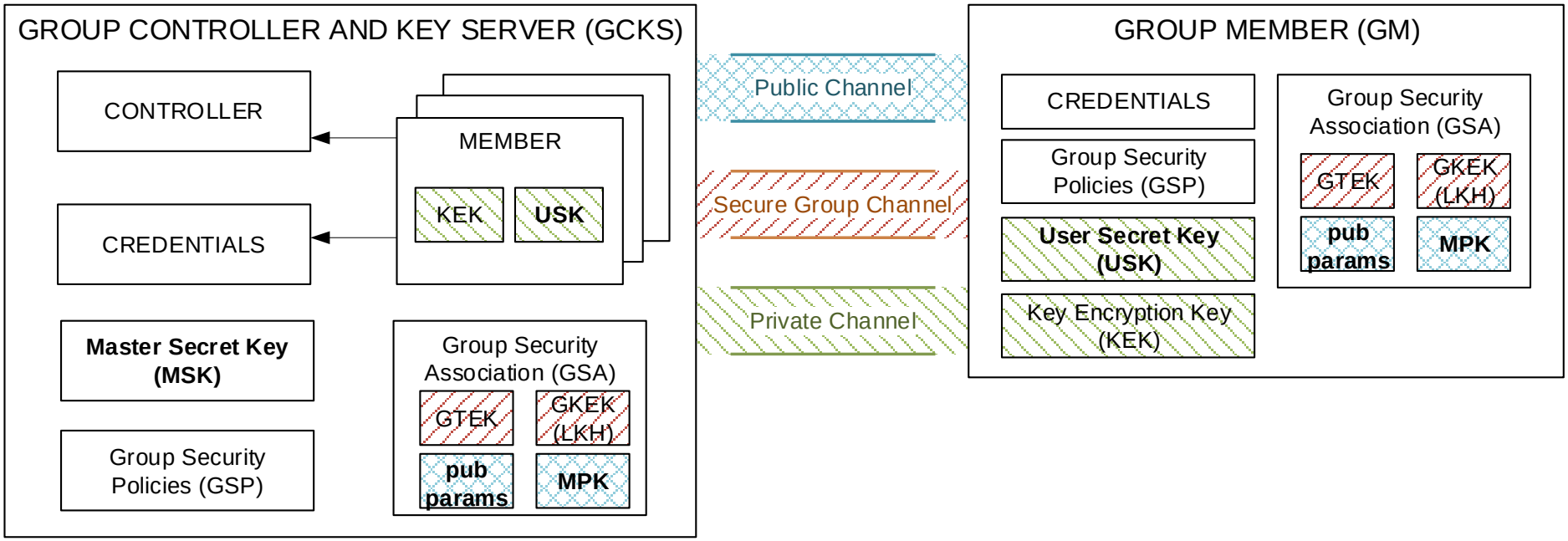
- F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings, in Selected Areas in Cryptography: 9th Annual International Workshop, SAC 2002. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 310–324.
- P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Advances in Cryptology- Asiacrypt 2005.

IBS on constrained devices



gentschen Felde, N., Grundner–Culemann, S., Guggemos, T., Using identity–based signatures for authenticated group communication, In *to appear in: 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (WiMob 2018)*, 2018, Limassol, Cyprus, Oktober, 2018.

Bridging the gap



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.

gentschen Felde, N., Grundner–Culemann, S., Guggemos, T., Using identity–based signatures for authenticated group communication, In *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (WiMob 2018)*, 2018, Limassol, Cyprus, Oktober, 2018.

What about Quantum Computers?

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

Where does this matter?

build trust
Exchange keys

set up
Key Generation

communicate
- encrypt
- integrity check
- authenticate

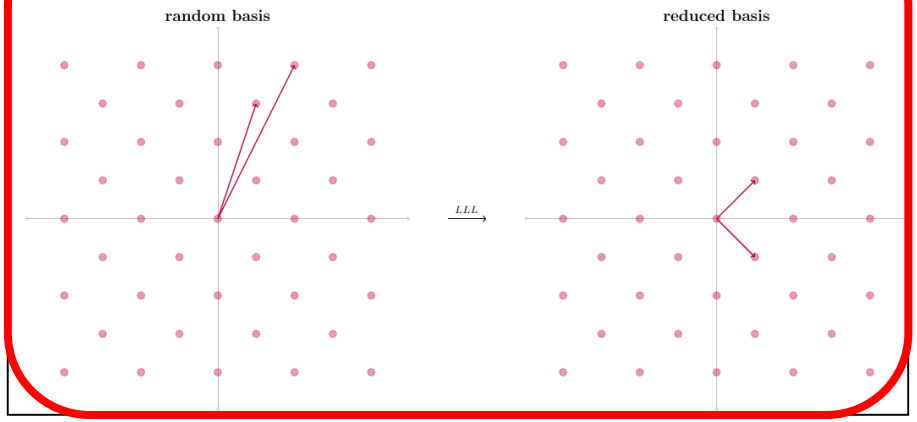
Key Revocation

New Cryptographic Primitives

Code Based Cryptography

- McEliece
- Goppa Codes
- …

Lattices



Multivariate Systems

$$x_0x_3 + x_2x_3 + x_0 + 1 = 0$$

$$x_0x_1 + x_2x_3 + x_2 + 1 = 0$$

$$x_0x_1 + x_0x_3 + x_0 + x_1 + 1 = 0$$

$$x_1x_2 + x_2x_3 + x_3 = 0$$

Others

- Isogenies on supersingular elliptic curves
- Braids (broken)
- …

Lattices on embedded devices?

- Offers encryption, signatures and key exchange
- Offers more advanced cryptographic techniques, such as IBS, IBE or ABE
- Key Sizes are in the range of RSA (which might already be a problem)

➔Ongoing research

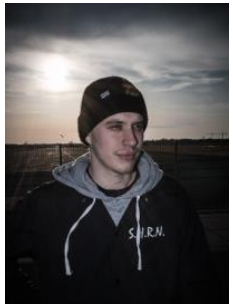
Who we are

Dr. N. gentschen Felde

T. Guggemos

S. Grundner-Culemann

M. Höb



J. Schmidt

MNM-Team

Ludwig-Maximilians-Universität München

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