A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO

Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, Jose Luis Torre-Arce

Philips Research, The Netherlands

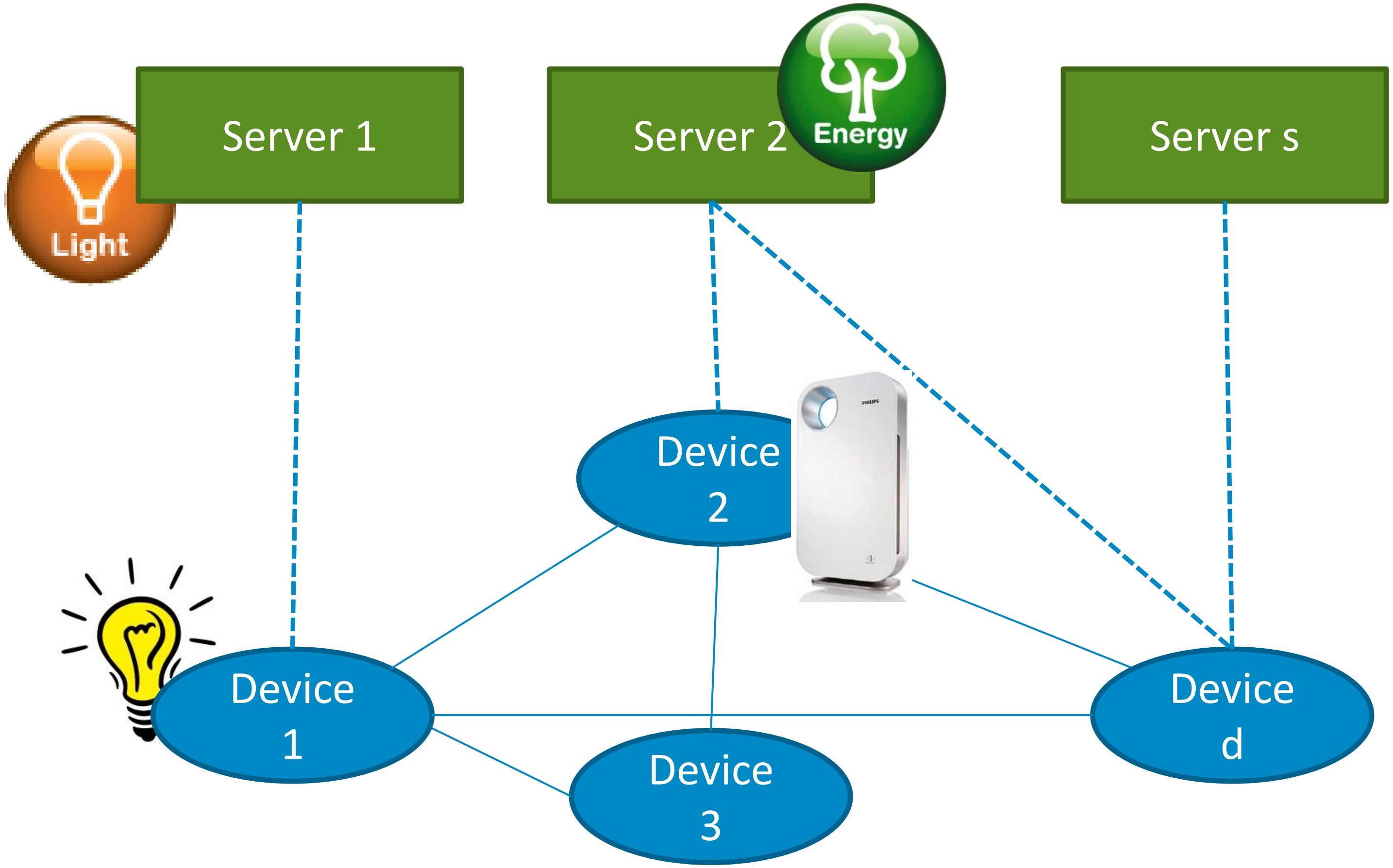
Lightweight Cryptography Workshop, NIST, July 21st 2015

innovation you

PHILIPS

Motivation

Securing the Internet (of Things)

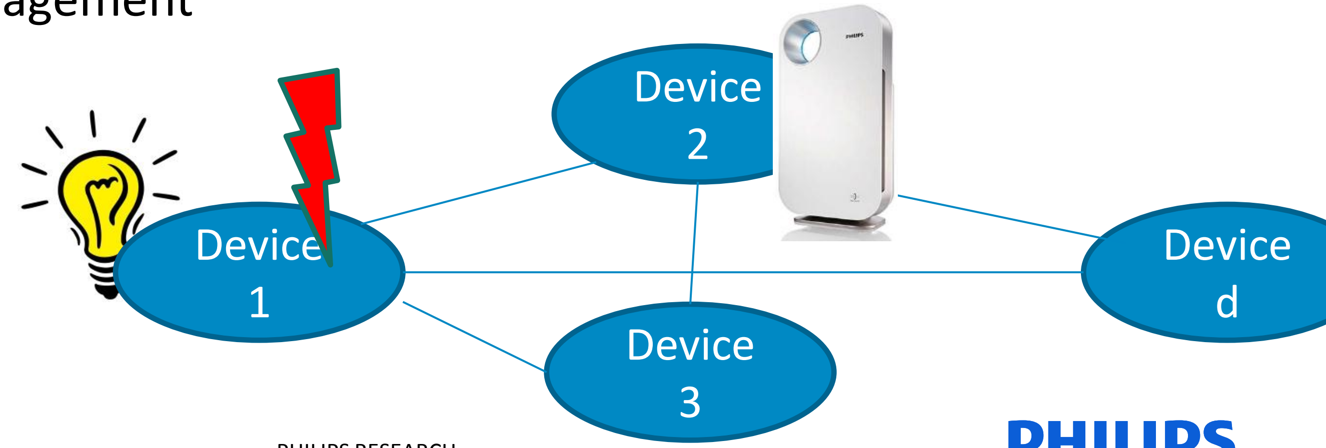


PHILIPS

Motivation

Secure device-to-device communication

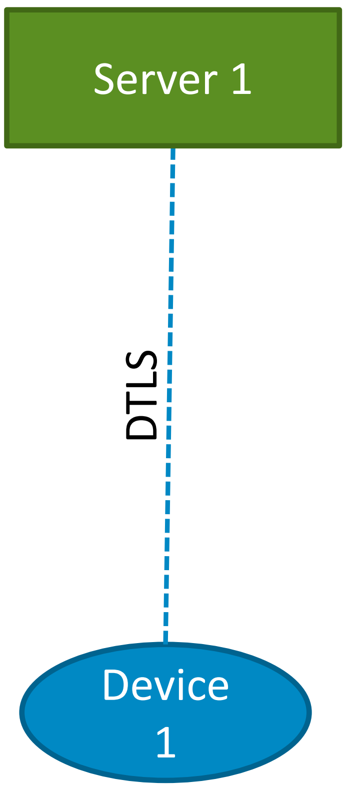
- IEEE 802.15.4 : PHY and MAC layers for Personal Area Networks, e.g., ZigBee and IPv6/6LoWPAN
  - Message protection with AES-CCM
  - Key management is left open
- Problems
  - Many current solutions rely on global secrets: the whole system/network is compromised if a single device is captured
  - Credential management



PHILIPS

Motivation

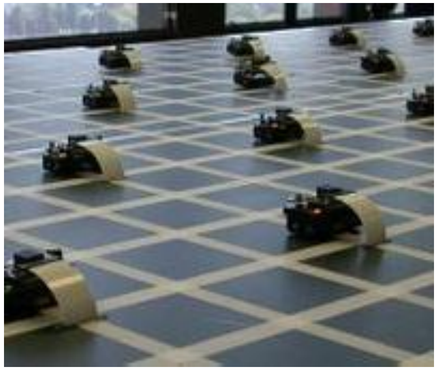
Securely connecting to the Internet



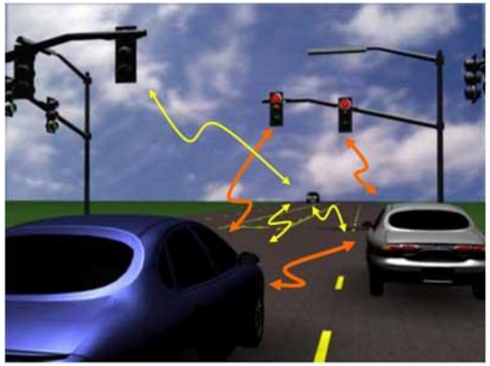
- DTLS is the datagram version of TLS and is used to protect the Internet of Things
- Problems:
  - Non-PSK modes are resource-hungry
  - PSK does not scale
  - All cipher suites in (D)TLS (except PSK) will be broken if a quantum computer is built
  - Certification authority compromised → huge problem

Some security & operational goals

Energy efficient



Real-time



Fits lifecycle

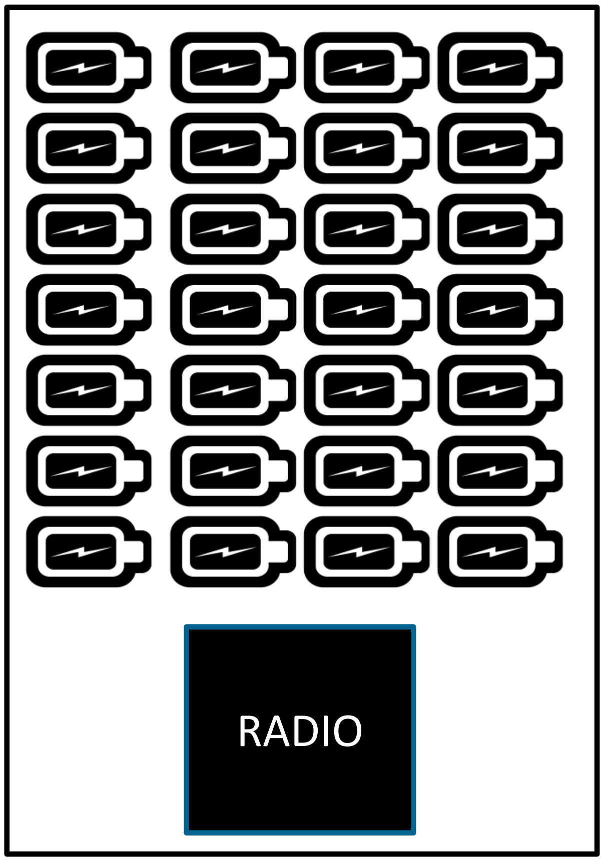
Simple operation

(**Quantum**) Secure

Goal: Efficient and scalable management of keys/credentials of devices?

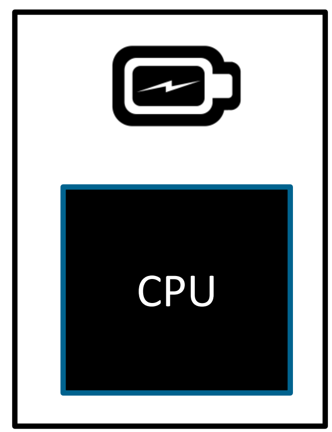
Some security & operational goals

Related to energy efficiency



- Sending 1 bit ~ 190 instructions
- Sending 1 KB over 100 m ~ 3 million instructions

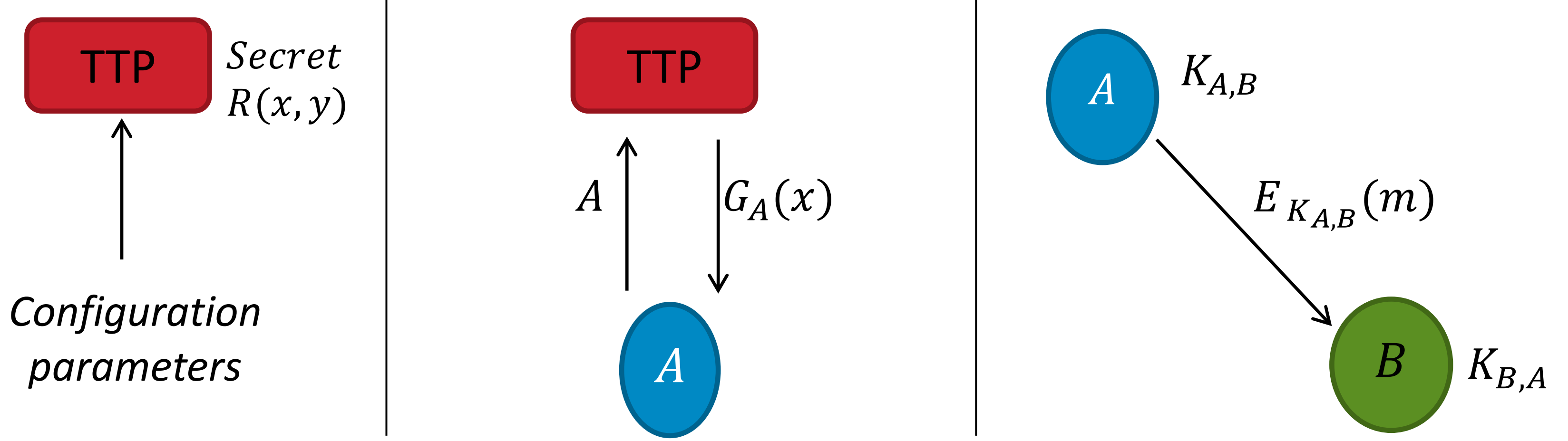
*From **Protocols and Architectures for Wireless Sensor Networks** By Holger Karl, Andreas Willig*



HIMMO

HIMMO is a key pre-distribution scheme

1) *Setup*	2) *Keying material extraction*	3) *Key establishment protocol*



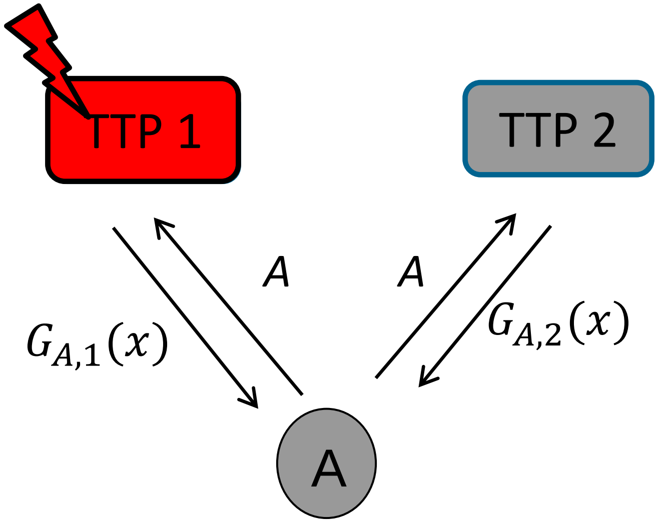
1) Trusted Third Party (TTP) creates a master-secret function $R(x,y)$
2) Each device A gets a secret key share, function $G_A(x)$ from the TTP
3) $K_{A,B} = \langle\langle G_A(\eta)\rangle_N\rangle_{2^b}$ and $K_{A,B} \sim K_{B,A}$. Thus, devices A, B can directly compute a common key using their identities

→ **A can directly send an encrypted and authenticated message to B!!!**

HIMMO

Some extensions

- **Certification and verification of credentials**
  - Efficient! Only one additional hash evaluation needed and implicit certificates
  - Implicit verification of credentials feasible since HIMMO is based on identities
- **Support of multiple TTPs:** device A can compute its combined $G_A(x)$ from the inputs of multiple TTPs
  - No increased computational or communication resources
  - Resilient against TTP compromise
  - Single TTP does not have access to all keys



HIMMO

Construction based on two interpolation problems

- **Hiding Information (HI) problem [2]: Let $f \in Z[x]$ of degree at most α, $x_i \in Z$ and $y_i = \langle\langle f(x_i)\rangle_N\rangle_r$ for $0 \leq i \leq c$. Given $\alpha, N, r, (x_1, y_1), \ldots (x_c, y_c)$ and x_0, find y_0 .**

  Equivalent to a close lattice vector problem in a lattice of dimension $\alpha + 1 + c$. For HIMMO parameters $r = 2^b$ and $N \approx 2^{(\alpha+1)B+b}$, c must be $\gtrsim (\alpha + 1)(\frac{\alpha B}{2b} + 1)$ to find a unique y_0.

- **Mixing Modular Operations (MMO) problem [3]: Let $m \geq 2$ and $g_1, \ldots, g_m \in Z[x]$, all of degree at most α, let $x_i \in Z$ and $y_i = \sum_{j=1}^{m} \langle g_j(x_i)\rangle_{q_j}$ for $0 \leq i \leq c$. Given $\alpha, m(x_1, y_1), \ldots, (x_c, y_c)$ and x_0, find y_0 .**

  If q_j known: lattice problem in dimension $m(\alpha + 1 + c)$, and c must be $\geq m(\alpha + 1)$ to find a unique y_0. No efficient way to reconstruct the q_i, problem considered infeasible.

---

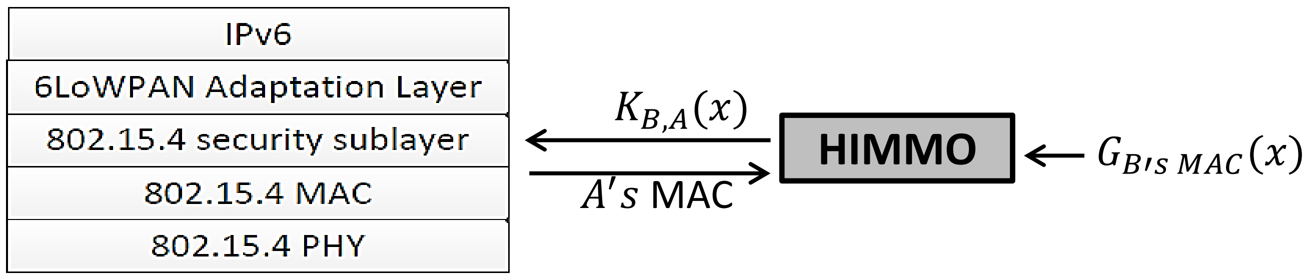
[2] O. Garcia Morchon, Ronald Rietman, Igor E. Shparlinski, and Ludo Tolhuizen. Interpolation and approximation of polynomials in finite fields over a short interval from noisy values. Experimental mathematics, 23:241–260, 2014.

[3] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez, R. Rietman, and L. Tolhuizen. The MMO problem. In Proc. ISSAC'14, pages 186–193. ACM, 2014.

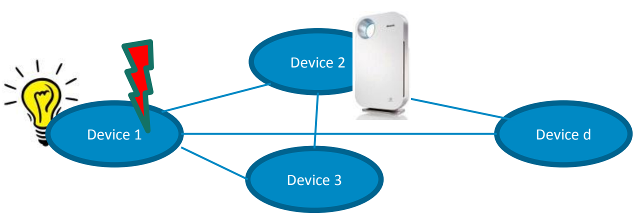
Secure device to device communication

IEEE 802.15.4

- HIMMO key shares instead of a common secret
  1. Configuration of each device with a secret key share linked to its MAC
  2. Pairwise keys during operation



- Advantages:
  - Collusion resistance
  - No message overhead
  - Easy protocol integration
  - Compromised devices can be blacklisted
  - Out-of-the-box secure by factory configuration



Performance

Table 1: HIMMO performance for $B = b = 128$ as a function of α.

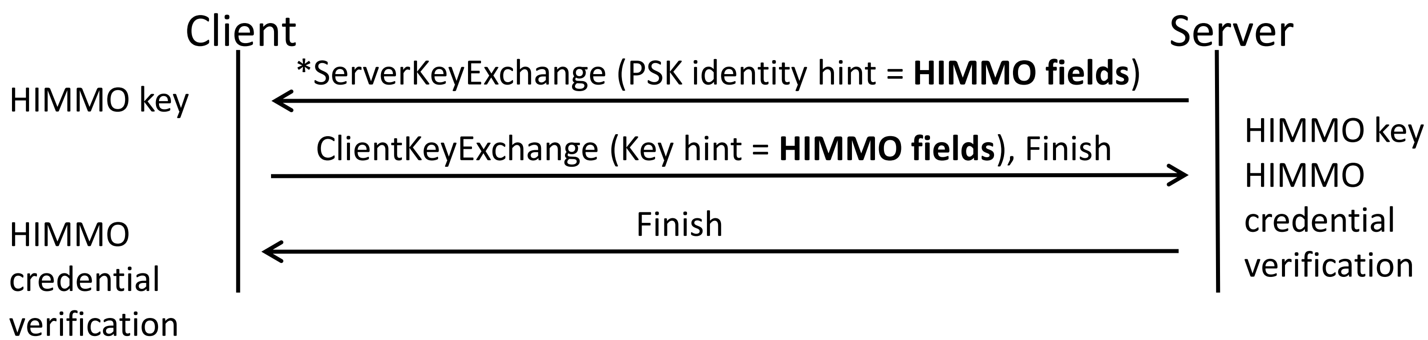
α		34	40	50
Keying material size (KB)		11.18	15.07	22.83
CPU time (msec)	ATMEGA128L (8-bit @ 8 MHz)	367	497	743
	NXP LPC1769 (32-bit @ 120 MHz)	30.59	41.77	64.25
	Intel i3 3120M (64-bit @ 2.5 GHz)	0.109	0.147	0.225

- Implementation on ATMEGA128L optimized in assembler
- Values for NXP and Intel based on flexible c library and TTP
  - Keying material structure can be optimized for the word size (8, 16, 32, 64) of the target CPU

Securely connecting to the Internet

DTLS-HIMMO

- HIMMO can be easily integrated into (D)TLS
- How? By exchanging HIMMO fields in two parameters of DTLS-PSK

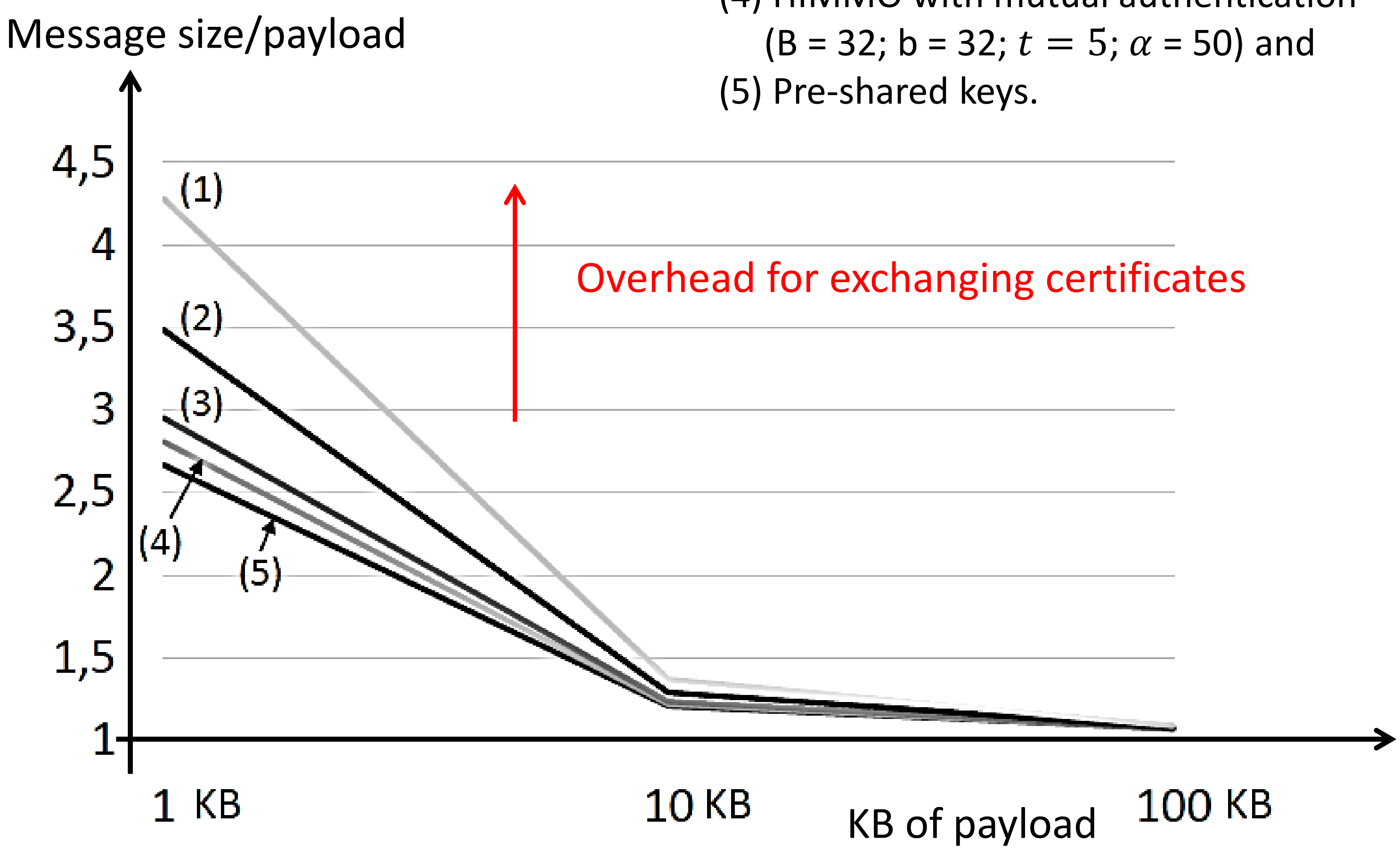


- HIMMO fields: identity, credentials, TTP identifiers
- Advantages? Next slides

DTLS-HIMMO

Bandwidth performance

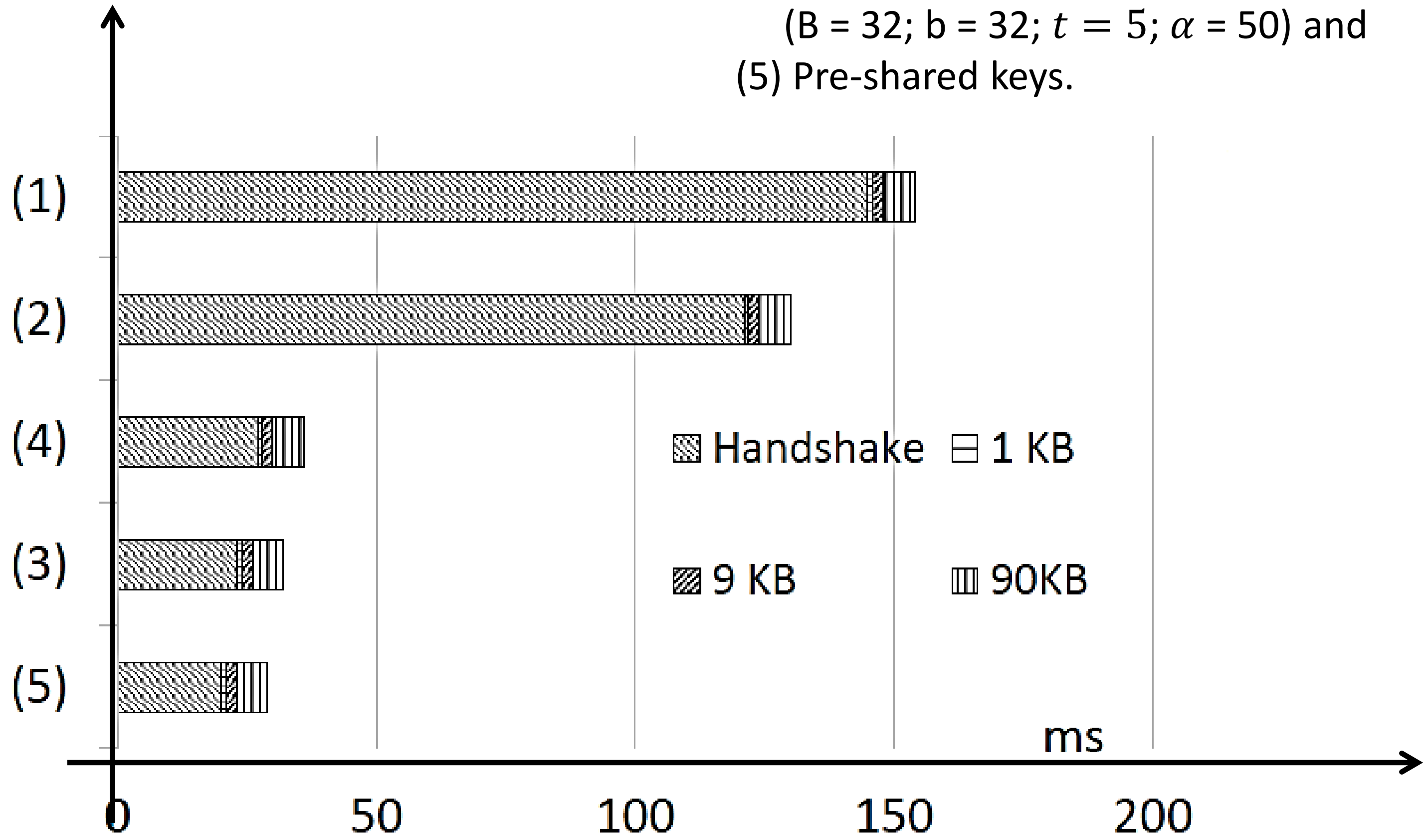
(1) ECDH-ECDSA with mutual authentication,
(2) ECDH-ECDSA with server authentication,
(3) HIMMO with mutual verification of client's and server's credentials (B = 256; b = 32; t=5, α = 50),
(4) HIMMO with mutual authentication (B = 32; b = 32; $t = 5$; α = 50) and
(5) Pre-shared keys.



DTLS-HIMMO

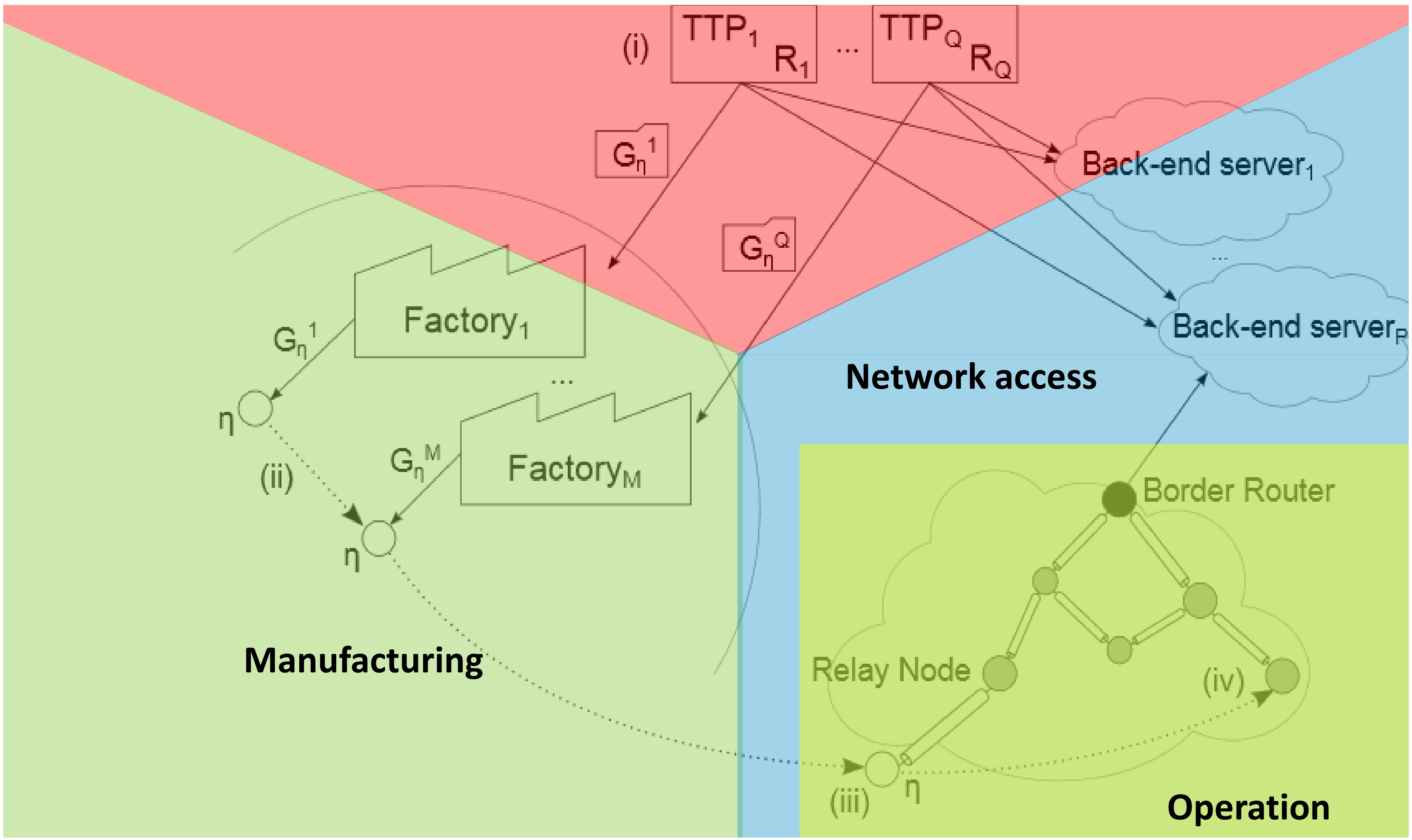
Timing performance

(1) ECDH-ECDSA with mutual authentication,
(2) ECDH-ECDSA with server authentication,
(3) HIMMO with mutual verification of client's and server's credentials (B = 256; b = 32; t=5, α = 50),
(4) HIMMO with mutual authentication (B = 32; b = 32; $t = 5$; α = 50) and
(5) Pre-shared keys.

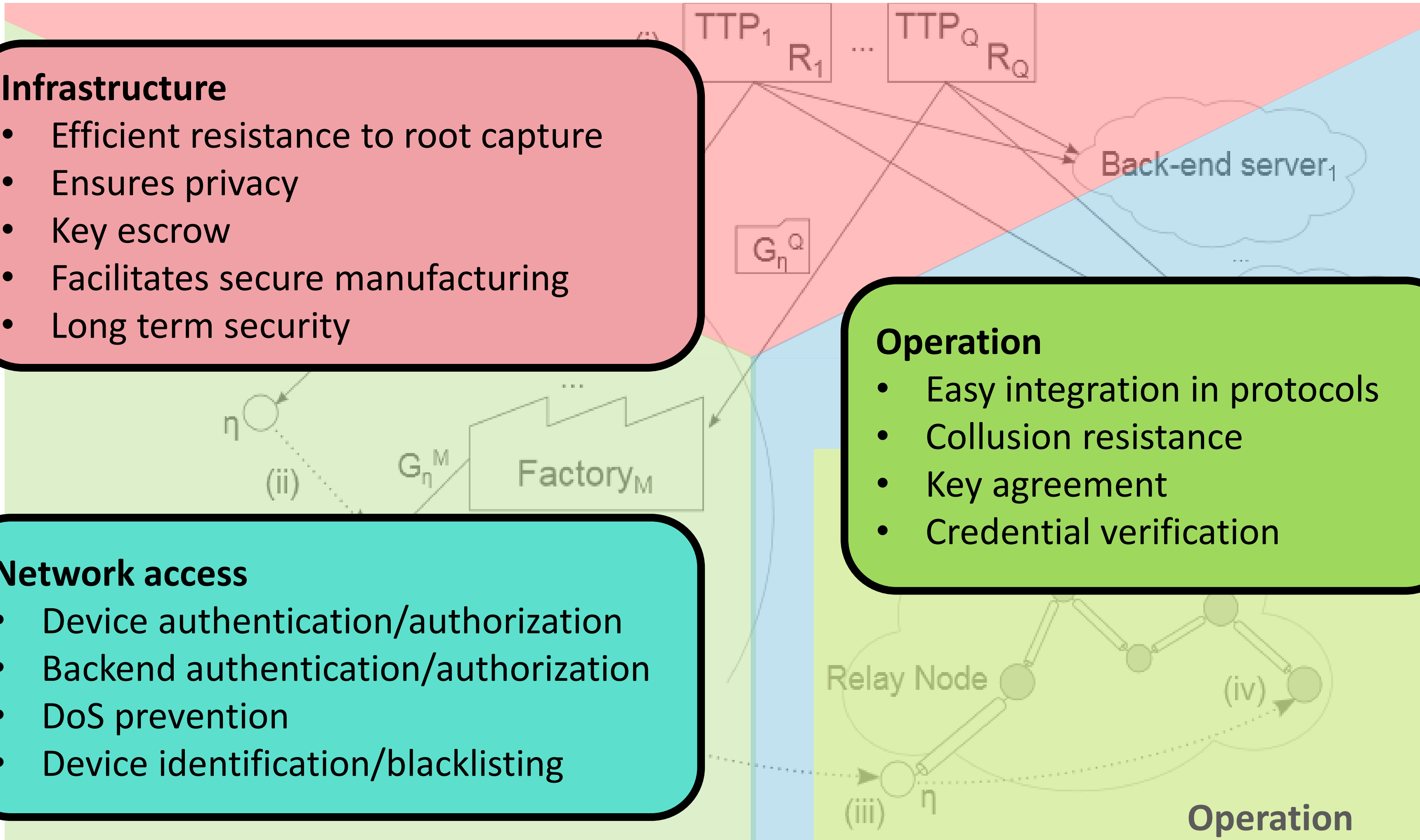


PHILIPS

Security architecture



Some features



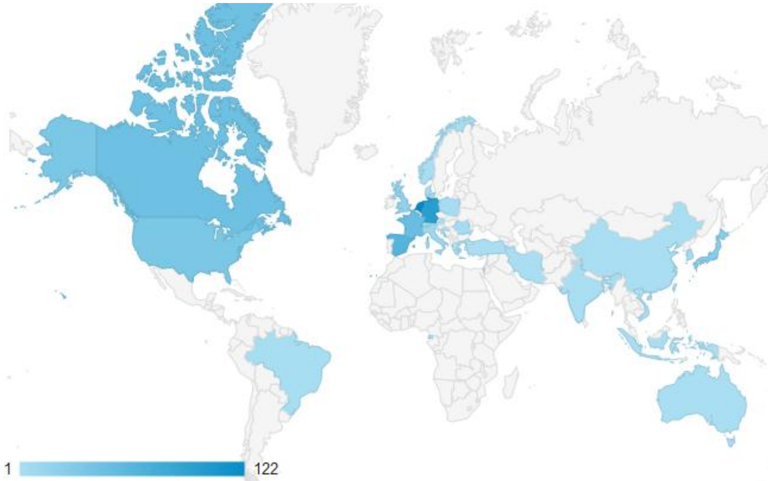
Infrastructure
- Efficient resistance to root capture
- Ensures privacy
- Key escrow
- Facilitates secure manufacturing
- Long term security

Operation
- Easy integration in protocols
- Collusion resistance
- Key agreement
- Credential verification

Network access
- Device authentication/authorization
- Backend authentication/authorization
- DoS prevention
- Device identification/blacklisting

HIMMO contest

www.himmo-scheme.com



	Country	Sessions	% New Sessions	New Users	Pages / Session	Avg. Session Duration
		841 % of Total: 100.00% (841)	43.28% Avg for View: 43.16% (0.28%)	364 % of Total: 100.28% (363)	3.07 Avg for View: 3.07 (0.00%)	00:02:52 Avg for View: 00:02:52 (0.00%)
1.	Netherlands	216 (25.68%)	34.72%	75 (20.60%)	4.90	00:04:19
2.	Germany	151 (17.95%)	52.98%	80 (21.98%)	2.42	00:01:32
3.	Spain	99 (11.77%)	46.46%	46 (12.64%)	2.52	00:02:44
4.	South Korea	75 (8.92%)	9.33%	7 (1.92%)	3.53	00:03:28
5.	France	49 (5.83%)	83.67%	41 (11.26%)	2.20	00:01:29
6.	United States	47 (5.59%)	76.60%	36 (9.89%)	1.79	00:01:13
7.	Canada	45 (5.35%)	22.22%	10 (2.75%)	1.31	00:02:29
8.	Japan	37 (4.40%)	37.84%	14 (3.85%)	2.97	00:04:48
9.	Romania	30 (3.57%)	13.33%	4 (1.10%)	2.63	00:03:17
10.	United Kingdom	20 (2.38%)	55.00%	11 (3.02%)	2.25	00:01:38

HIMMO Contest HIMMO Features and Applications Resources The Contest Status Submit your solution

Can you break it?

We are challenging you to attempt to break the HIMMO scheme as well as the mathematical problems it is built upon.

Enter the contest »

HIMMO challenges

	Challenge #	alpha	Lattice dimension	Data (B)	Time(ms)
Key agreement (b= B = 32)	*HIMMO1*	*5*	*27*	-	-
	HIMMO3	*20*	*252*	-	-
	HIMMO5	25	377	*4*	5.33
	HIMMO7	30	527	*4*	6.9
	HIMMO9	35	702	*4*	8.68
	HIMMO11	40	902	*4*	10.65
	HIMMO13	50	1377	*4*	15.1
	HIMMO15	100	5252	*4*	48.48

	Challenge #	alpha	Lattice dimension	Data (B)	Time(ms)
Key agreement + data verification (b= 32 – B = 256)	*HIMMO2*	*2*	*51*	-	-
	HIMMO4	*7*	*296*	-	-
	HIMMO6	9	450	*32+data*	18.21
	HIMMO8	10	539	*32+data*	21.64
	HIMMO10	12	741	*32+data*	29.32
	HIMMO12	14	975	*32+data*	38.12
	HIMMO14	17	1386	*32+data*	53.4
	HIMMO16	35	5364	*32+data*	197.68

- Started: 5/26/15
- Very active
- First phase till: 8/15/15
- Winner of first phase to be announced at rump session Crypto (waiting for final confirmation)
- Second phase till 12/31/15

PHILIPS

Conclusions

- Solution that is lightweight (time and energy) and scalable and fits lifecycle is required to protect the Internet of Things
- HIMMO-based security architecture enables for:
  – Pairwise key agreement + implicit credential certification & verification
  – Support of multiple TTP

  while being
  – Lightweight
  – Scalable
  – Collusion resistant and potentially quantum secure
- HIMMO's identity-based security easily integrates with existing protocols (DTLS, IEEE 802.15.4,…) bringing many advantages
- HIMMO algorithm can be reused for other primitives, e.g., stream cipher
- Open source implementation of HIMMO available for research purposes (oscar dot garcia at philips dot com).

Acknowledging the contributions to the HIMMO scheme of:

Domingo Gomez and Jaime Gutierrez (Univ. of Cantabria, Spain)
Igor Shparlinski (University of New South Wales, Australia)
Berry Schoenmakers (TU/e, The Netherlands)

HIMMO

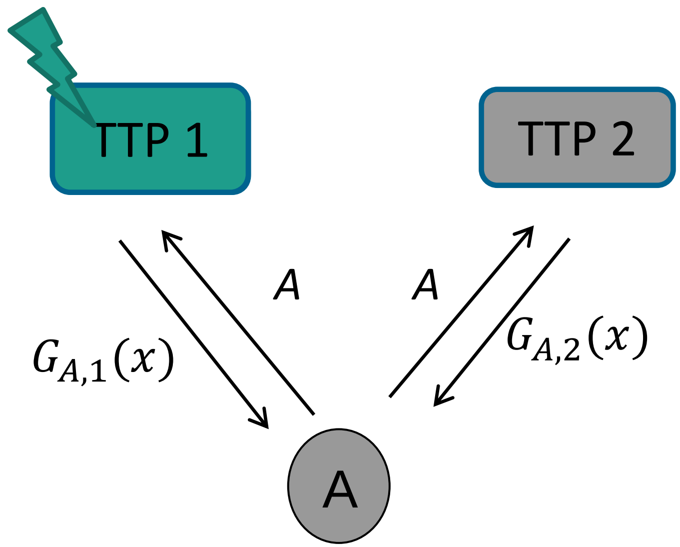
In a post-quantum world

- HIMMO itself is not lattice-based, but its security analysis [2][3][4] leads in a natural way to lattice problems
- Analysis [4] shows that HIMMO can achieve fully collusion resistance for adequate parameters
- HIMMO can be post-quantum secure since there is no known quantum algorithm to find a reduced basis of a lattice providing a significant performance improvement compared with non-quantum algorithms.

---

[4] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez , R. Rietman, B. Schoenmakers, and L. Tolhuizen,. HIMMO - A Lightweight, Fully Collusion Resistant Key-Pre-distribution Scheme. Cryptology ePrint Archive, Report 2014/698, 2014. http://eprint.iacr.org/.

HIMMO's multiple TTP scheme defends against hacked root authorities



$$G_A(x) = G_{A,1}(x) + G_{A,2}(x)$$

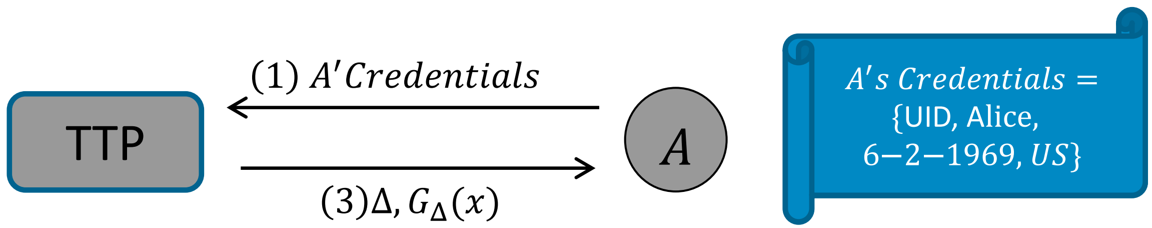
- **No single party has all the keys to the entire Internet of Things**: the network is secure as long as at least one TTP is not compromised
- **Efficient mixing:** same operational performance as a single TTP scheme

PHILIPS RESEARCH

Using HIMMO to certify and verify credentials

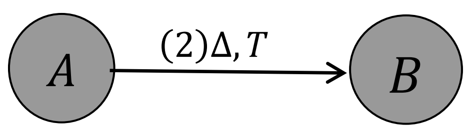
Step 1: Certification

$(2)\Delta = hash\ (Credentials)$



Step 2: Implicit verification

(1) $\mathrm{T} = Credentials\ protected$
$with\ \ K_{\Delta,B} = G_\Delta(B)$



$(3)\ Decrypt\ T\ to\ get\ Credentials$
$with\ K_{B,\Delta} = G_B(\Delta)$

$(4)\ Check\ if\ \Delta = hash(A's\ Credentials)$

- **Credential certification/verification** was only feasible with PKC till today
- **Efficient verification:** only involves an additional hash computation, much more efficient than PKC

HIMMO Literature

[1] O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez. Towards full collusion resistant ID-based establishment of pairwise keys. In Extended abstracts of the third Workshop on Mathematical Cryptology (WMC 2012) and the third international conference on Symbolic Computation and Cryptography (SCC 2012). Pages 30-36, **2012**.
[2] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez, R. Rietman, and L. Tolhuizen. The MMO problem. In Proc. ISSAC'14, pages 186–193. ACM, **2014**.
[3] O. Garcia Morchon, Ronald Rietman, Igor E. Shparlinski, and Ludo Tolhuizen. Interpolation and approximation of polynomials in finite fields over a short interval from noisy values. Experimental mathematics, 23:241–260, **2014**.
[4] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez , R. Rietman, B. Schoenmakers, and L. Tolhuizen,. HIMMO - A Lightweight, Fully Collusion Resistant Key-Pre-distribution Scheme. Cryptology ePrint Archive, Report 2014/698, **2014**. http://eprint.iacr.org/.
[5] O. Garca-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, J.L., Torre-Arce. DTLS-HIMMO Efficiently Securing a Post-Quantum World with a Fully-Collusion Resistant KPS. Cryptology ePrint Archive, Report 2014/1008, **2014**. http://eprint.iacr.org/.
[6] O. Garca-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, J.L., Torre-Arce. A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO. Cryptology ePrint Archive, Report 2015/454, **2015**. http://eprint.iacr.org/.