DTLS-HIMMO: Efficiently Securing a PQ world with a fully-collusion resistant KPS

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

Philips Research, The Netherlands

Workshop on PQ Cryptography, NIST, April 3rd 2015

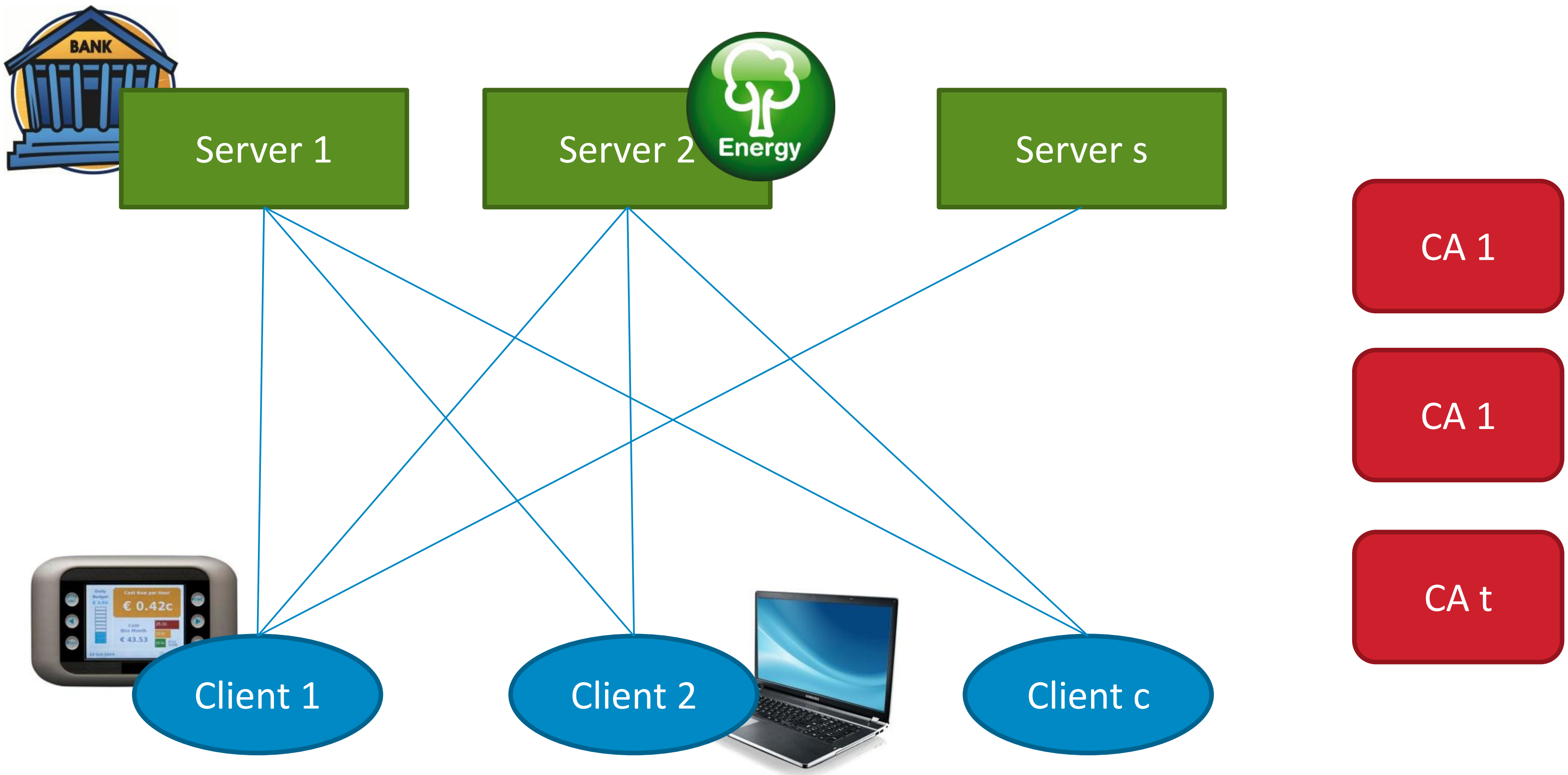
PHILIPS

Agenda

- Motivation
- HIMMO
- DTLS-HIMMO
- Conclusion

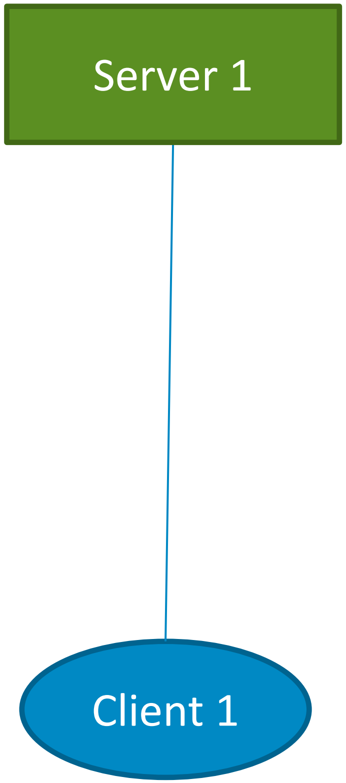
Motivation

Securing the Internet (of Things)



Motivation

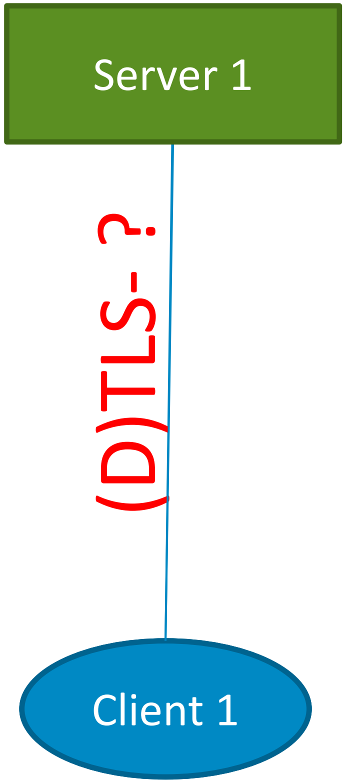
(D)TLS



- Used to secure Internet connection between client and server. DTLS to protect the Internet of Things
- Cipher-suites
  – Based on ECC, RSA,…
  – Only server authentication or both
  – Pre-shared key (PSK) is the most efficient one
- Problems:
  – All cipher suites in (D)TLS (except PSK) will be broken if a quantum computer is built
  – Non-PSK modes are resource-hungry for Internet of Things
  – PSK does not scale

Motivation

Goals



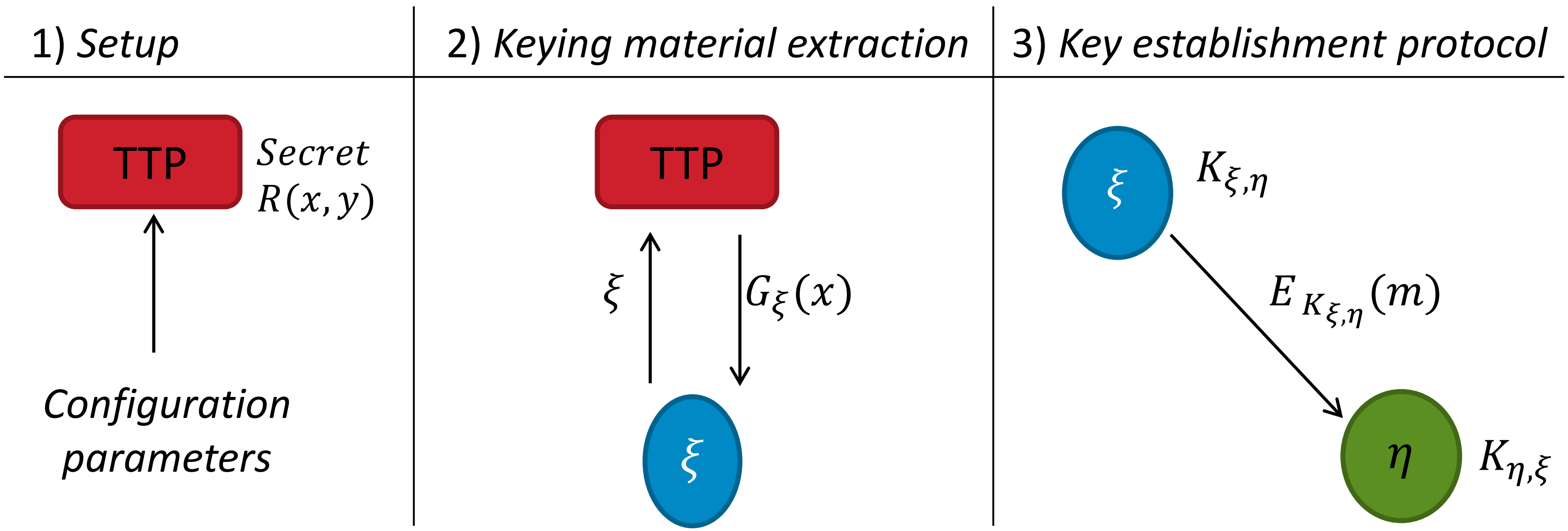
We would like to have a scheme that:

- is resilient to quantum computers,
- has the low operational cost of DTLS-PSK,
- enables mutual authentication and credential verification as with certificate-based schemes,
- and is scalable like solutions based on public-key cryptography and infrastructure.

PHILIPS

HIMMO

HIMMO is a key pre-distribution scheme



1) Trusted Third Party (TTP) creates a master-secret function $R(x,y)$
2) Each device ξ gets a secret key share, function $G_\xi(x)$ from the TTP
3) $K_{\xi,\eta} = \left\langle \left\langle G_\xi(\eta) \right\rangle_N \right\rangle_{2^b}$ and $K_{\xi,\eta} \sim K_{\eta,\xi}$. Thus, devices ξ, η can compute a common key using their identities without communication overhead

HIMMO

Some extensions

- **Implicit certification and verification:** HIMMO is based on identities and identities are implicitly verified if key agreement succeeds. Therefore, we can achieve implicit verification of credentials if the identity generated as

$$\xi = hash(\xi' s\ credentials)$$

- **Support of multiple TTPs:** device ξ can compute its combined $G_\xi(x)$ from the inputs of multiple TTPs

$$G_\xi(x) = \left\langle G_\xi^{TTP_1}(x) + \cdots + G_\xi^{TTP_t}(x) \right\rangle_N$$

  The advantages are that (i) this approach is resilient against TTP compromise without increasing communication or computational needs and (ii) single TTP does not have access to pairwise keys, but all TTPs together can (key escrow)

HIMMO

Efficient implementation and performance

- Key generation accounts for the evaluation of a polynomial $K_{\xi,\eta} = \left\langle \left\langle G_{\xi}(\eta) \right\rangle_N \right\rangle_{2^b}$
- Performance (without multiplication optimization)

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

		α			
		26	34	40	50
Keying material size (KB)		6.90	11.18	15.07	22.83
Lattice dimension		405	665	902	1377
CPU time (msec)	ATMEGA128L (8-bit @ 8 MHz)	223	367	497	743
	NXP LPC1769 (32-bit @ 120 MHz)	18.38	30.59	41.77	64.25
	Intel i3 3120M (64-bit @ 2.5 GHz)	0.067	0.109	0.147	0.225

Table 2. HIMMO performance for $\alpha = 26$ as a function of $b = B$.

		$b = B$			
		64	128	192	256
Keying material size (KB)		3.45	6.90	10.34	13.79
CPU time (msec)	ATMEGA128L (8-bit @ 8 MHz)	63	223	393	632
	NXP LPC1769 (32-bit @ 120 MHz)	5.55	18.39	40.34	71.41
	Intel i3 3120M (64-bit @ 2.5 GHz)	0.023	0.067	0.134	0.224

  - **b** is the size of the generated key, **B** is the identifier size and $\boldsymbol{\alpha}$ is the polynomial degree

- Code size on ATMEGA 128L: 428 Bytes

PHILIPS

HIMMO

Implementation

Algorithm 1 Optimized key generation

INPUT: $B, b, \alpha, \eta, G_{\xi,j}$ with $j \in \{0, \dots, \alpha\}$
OUTPUT: key
$key \leftarrow \langle G_{\xi,\alpha} \rangle_{2^b}$
$temp \leftarrow \lfloor \frac{G_{\xi,\alpha}}{2^b} \rfloor$
for $j = \alpha - 1$ **to** 0 **do**
  $temp \leftarrow temp \times \eta + \lfloor \frac{G_{\xi,j}}{2^{(\alpha-1-j)B+b}} \rfloor$
  $key \leftarrow \langle key \times \eta \rangle_{2^b} + \langle G_{\xi,j} \rangle_{2^b}$
  $key \leftarrow \langle key + \lfloor \frac{temp}{2^{(j+2)B}} \rfloor \rangle_{2^b}$
  $temp \leftarrow \lfloor \frac{\langle temp \rangle_{2^{(j+2)B}}}{2^B} \rfloor$
end for
return key

HIMMO

Construction based on two interpolation problems

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

  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. For $\alpha > 20$, all known lattice techniques fail to give a correct answer.

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

  If q_j known: lattice problem in dimension $m(\alpha + 1 + c)$, and c must be $\ge m(\alpha + 1)$ 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.

HIMMO

In a PQ 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
- We believe that 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.

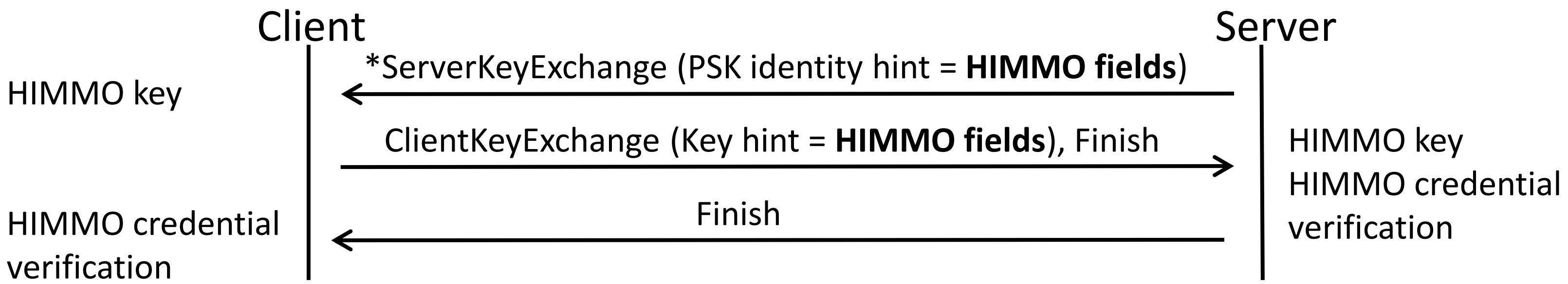
---

[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/.

DTLS-HIMMO

What is it?

- Recall, (D)TLS includes:
  - Handshake: (mutual) authentication and session key agreement
  - Record layer: secure exchange of data
- How? By exchanging HIMMO fields in two parameters of DTLS-PSK



- HIMMO fields

	HIMMO flag	Message Type	Number of TTPs	TTP ID	Identifier	HIMMO Credentials length	HIMMO Credentials	Reconci-lliation data
Length(Bytes)	2	1	1	1/ # TTP	B	1	$0 \ldots (122 - B)$	1
Mandatory (M)/ Optional (O)	M	M	M	M	M	O	O	O

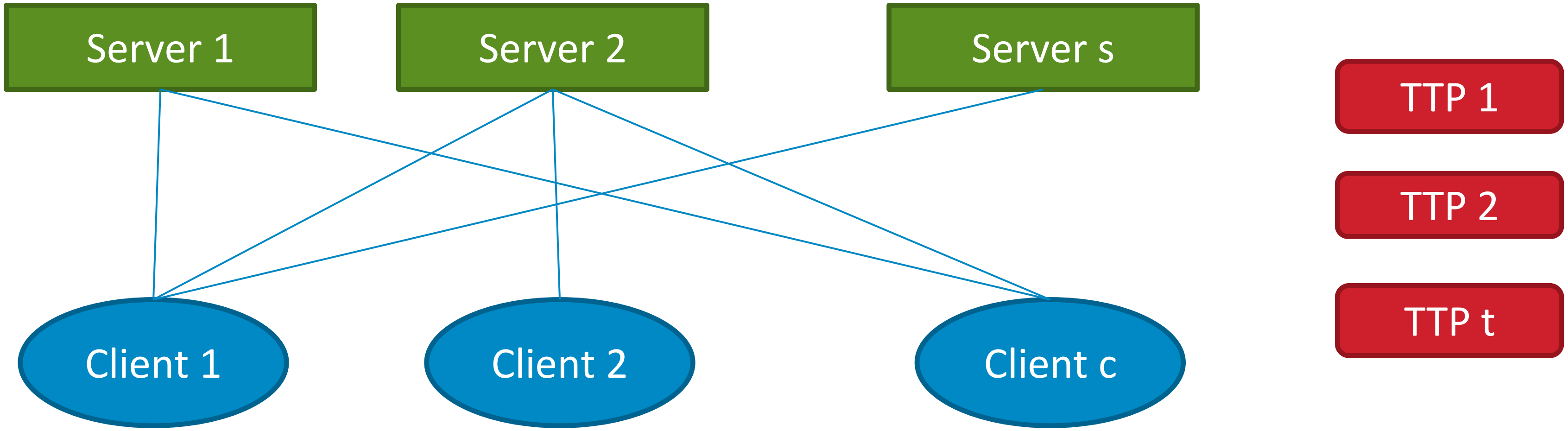
DTLS-HIMMO

Configurations

	Client sends HIMMO's ID	Client sends HIMMO's credentials
Server sends HIMMO's ID	**Messages exchanged**	
	ClientKeyExchange: Client ID and Reconciliation data ServerKeyExchange: Server ID	ClientKeyExchange: Clients credentials and Reconciliation data ServerKeyExchange: Server ID
	Computations	
	Two HIMMO evaluations in total	Two HIMMO evaluations in total One hash evaluation
	Properties	
	Mutual authentication	Mutual authentication Verification of client's credentials
Server sends HIMMO's credentials	**Messages exchanged**	
	ClientKeyExchange: Client ID and Reconciliation data ServerKeyExchange: Servers credentials	ClientKeyExchange: Clients credentials and Reconciliation data ServerKeyExchange: Servers credentials
	Computations	
	Two HIMMO evaluations in total One hash evaluation	Two HIMMO evaluations in total Two hash evaluations
	Properties	
	Mutual authentication Verification of server's credentials	Mutual authentication Verification of the credentials of client and server

DTLS-HIMMO

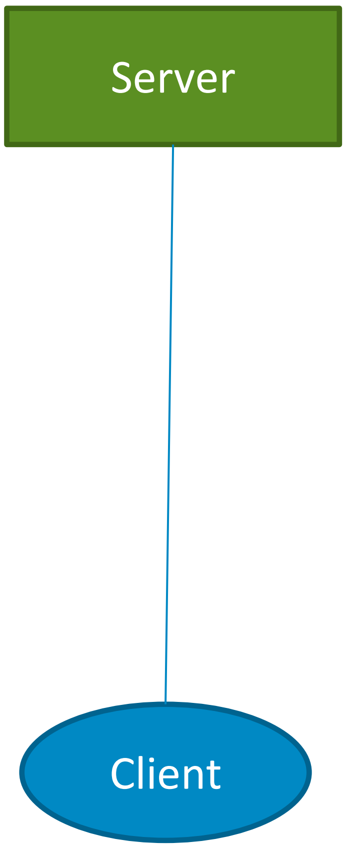
TTP infrastructure in a PQ world?



- Public key infrastructure → TTP infrastructure
- Single TTP compromise does not break down the system
- Single TTP does not have access to communication links, but cooperation of TTPs enables **key escrow**
- Protocol **performance** between client and server **independent of t**

DTLS-HIMMO

Setup

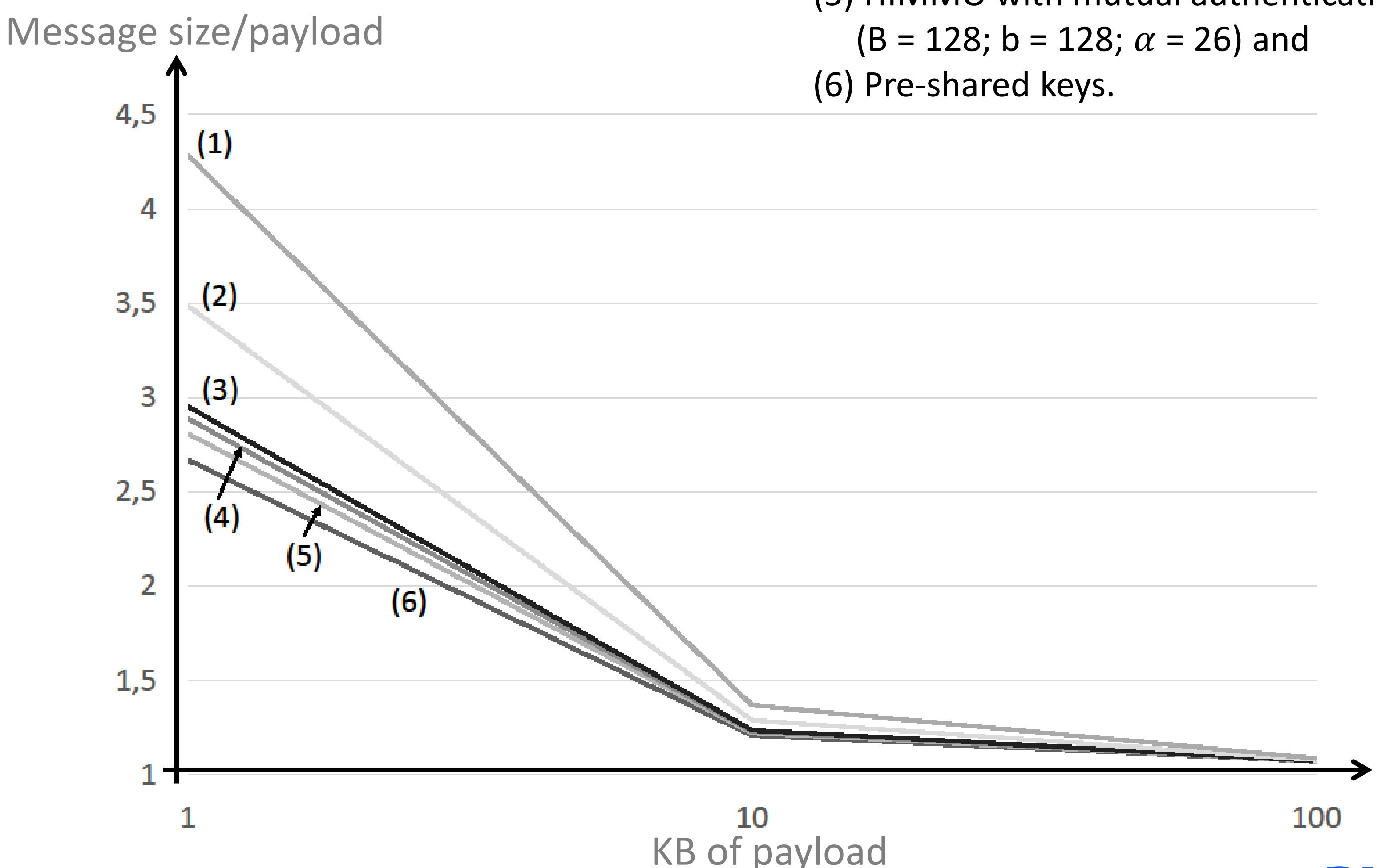


- Server and client: Intel Core i5-3437U @ 1.90 GHz with Windows 7 Enterprise
- DTLS in different modes:
  - Pre-shared key
  - ECDHE and ECDSA on NIST secp256r1 curve with server authentication and mutual authentication
  - HIMMO (mutual authentication and verification of credentials)
- Wireshark sniffer between client and server

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 = 128; α = 50),
(4) HIMMO with mutual verification of client's and server's credentials (B = 256; b = 128; α = 26),
(5) HIMMO with mutual authentication (B = 128; b = 128; α = 26) and
(6) Pre-shared keys.

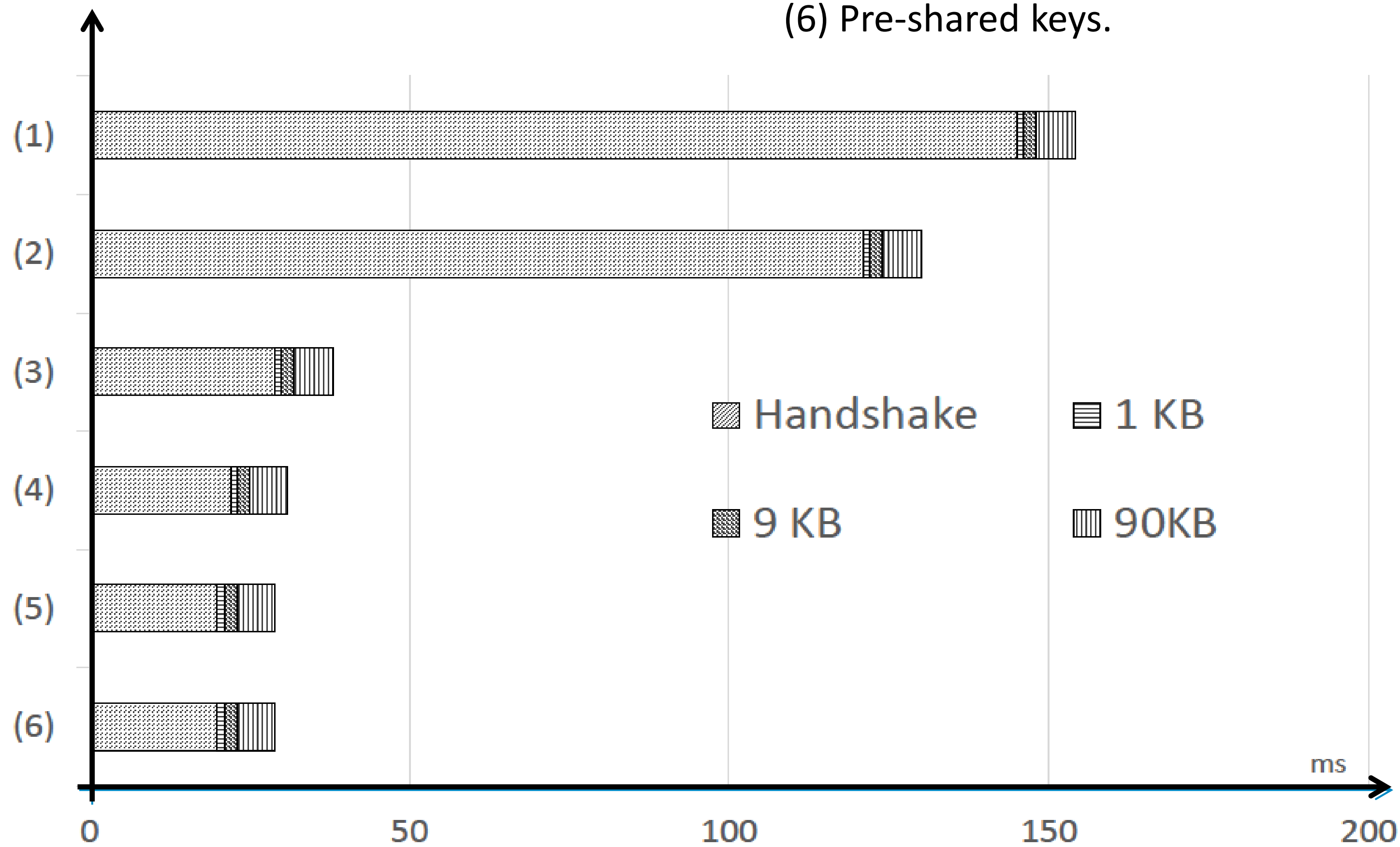


PHILIPS

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 = 128; α = 50),
(4) HIMMO with mutual verification of client's and server's credentials (B = 256; b = 128; α = 26),
(5) HIMMO with mutual authentication (B = 128; b = 128; α = 26) and
(6) Pre-shared keys.



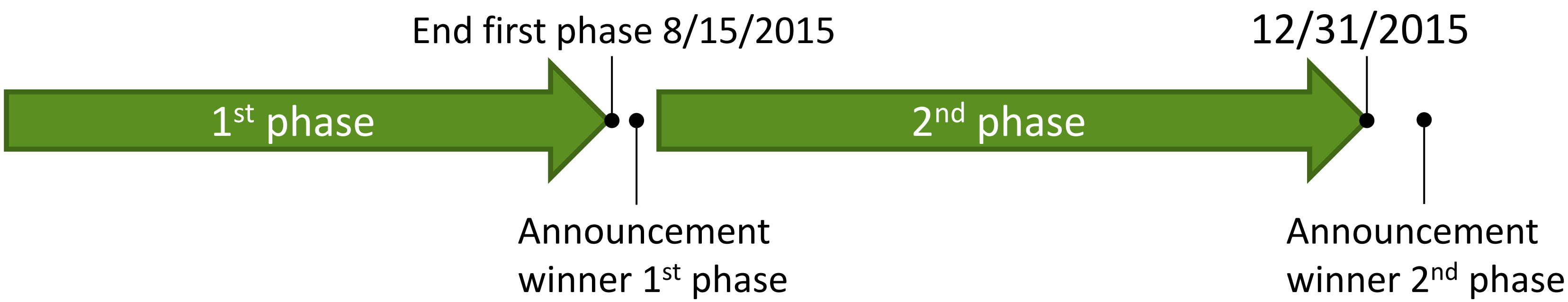
Conclusions

- Solution that is quantum secure, lightweight and scalable is required to protect the Internet (of Things)
- HIMMO enables for:
  – Pairwise key agreement + implicit credential certification & verification
  – Support of multiple TTP

  while being
  – Lightweight
  – Scalable
  – Collusion resistant and potentially quantum secure
- (D)TLS-HIMMO improves performance of existing cipher-suites and is potentially quantum secure.
- Open source implementation of HIMMO available for research purposes.

HIMMO Challenge

Increasing confidence



- Challenges: from small to large parameters with little price for each of them
- Two phases with two winners
  - Who wins? challenge with largest parameters at that point of time.
  - Winner to be announced during well-known crypto conferences
- Where: www.himmo-scheme.com
- More announcements and details in the next weeks through mailing lists
- If you are interested, send me an email: oscar.garcia@philips.com

PHILIPS

HIMMO Literature

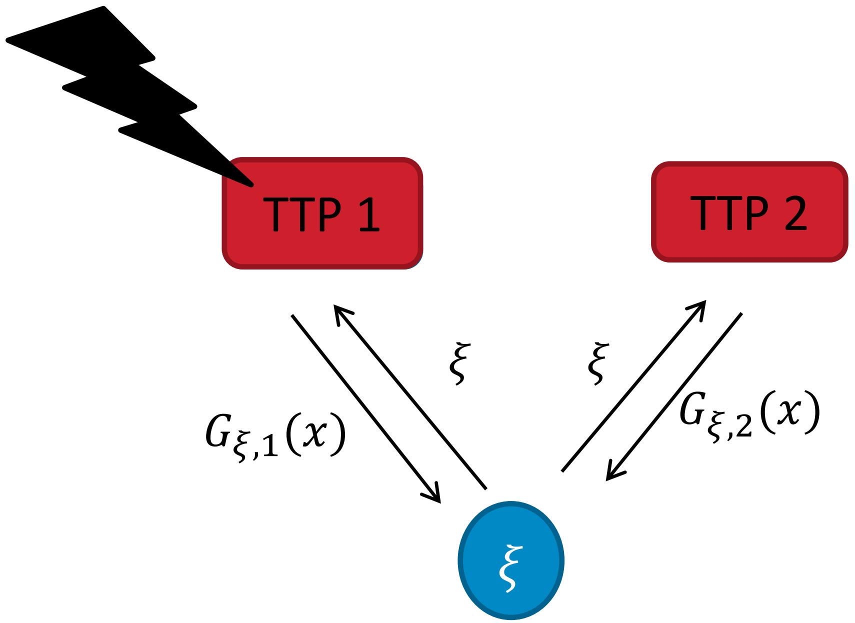
[1] O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez. Towards full collusion resistant ID-based establishment of pairwise keys. In Extended abstracts of the third Workshop on Mathematical Cryptology (WMC 2012) and the third international conference on Symbolic Computation and Cryptography (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/**???**, **2015**. http://eprint.iacr.org/.

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)

Multiple TTP scheme



$$G_{\xi}(x) = G_{\xi,1}(x) + G_{\xi,2}(x)$$

- **Protection** against hacked roots of trust
- **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

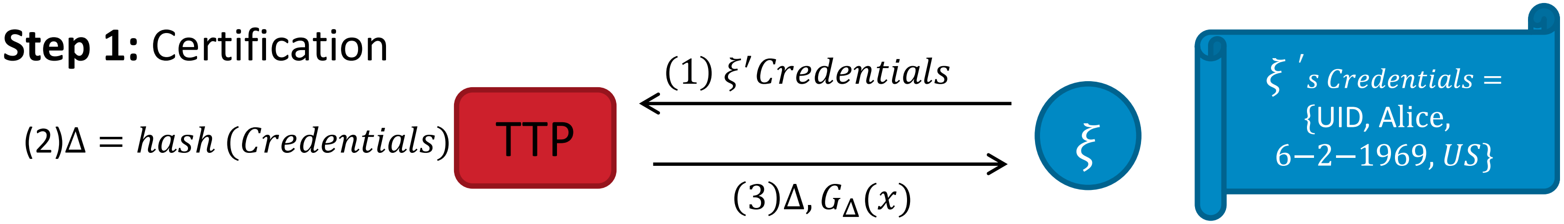
Certification and verification of credentials

$\xi\ 's\ Credentials =$
$\{\mathrm{UID},\ \mathrm{Alice},$
$6\!-\!2\!-\!1969,\ US\}$

- **Credential certification/verification** was only feasible with PKC

Certification and verification of credentials

Step 1: Certification

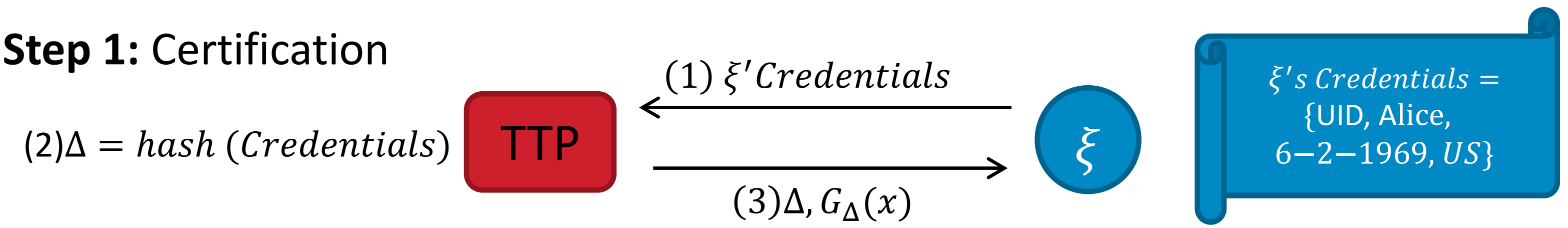


- **Credential certification/verification** was only feasible with PKC

PHILIPS

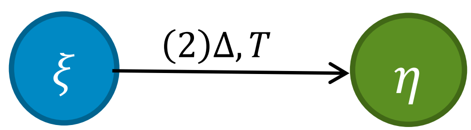
Certification and verification of credentials

Step 1: Certification



Step 2: Implicit verification

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



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

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

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