The HIMMO Contest

Oscar Garcia-Morchon
Philips Research, The Netherlands

August 18th 2015

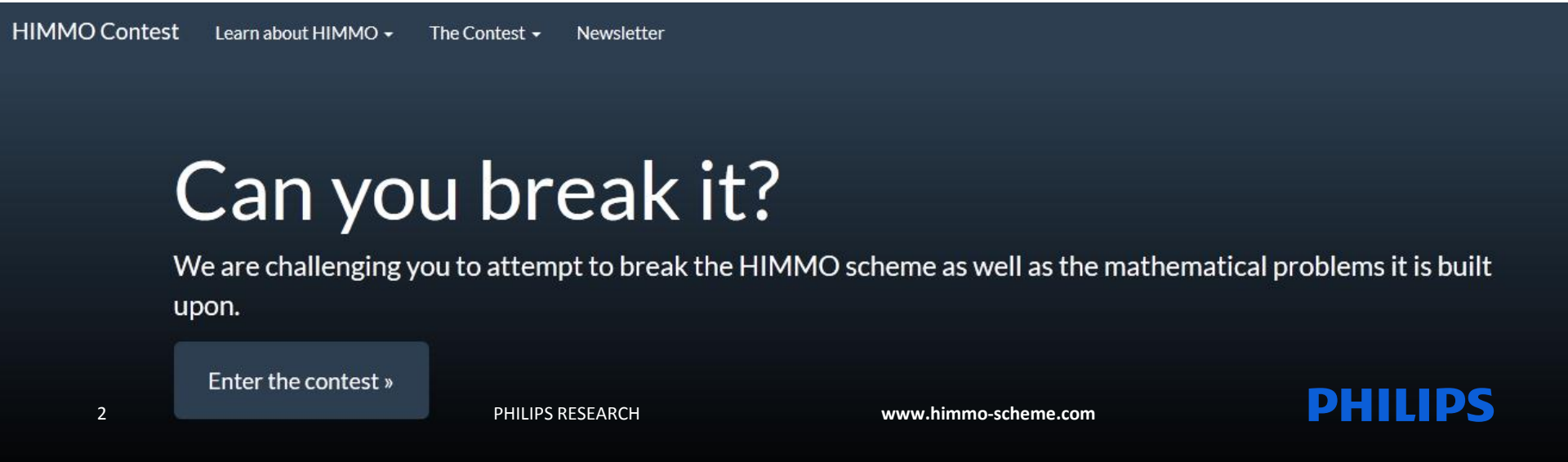
innovation + you

PHILIPS

Invitation to participate

In the open verification of the practical and efficient HIMMO scheme

www.himmo-scheme.com



What's the HIMMO Contest about?

Lattice problems

Cryptanalysis

Polynomials

Lattices

KPS

NIKE

Key establishment

Lightweight "certificates"

Practical scheme

Some information

	Challenge #	Lattice dim.	
Key agreement	*HIMMO1*	*27*	
	HIMMO3	*252*	
	HIMMO5	377	$
	HIMMO7	527	$
	HIMMO9	702	$
	HIMMO11	902	$
	HIMMO13	1377	$
	HIMMO15	5252	$

	Challenge #	Lattice dim.	
Key agreement + data verification	*HIMMO2*	*51*	
	HIMMO4	*296*	$
	HIMMO6	450	$
	HIMMO8	539	$
	HIMMO10	741	$
	HIMMO12	975	$
	HIMMO14	1386	$
	HIMMO16	5364	$

2/April/15
Announced NIST PQ workshop

26/May/15
Website online

26/June/15
First solution for an easy challenge

15/August/15
End of first phase

$$$

31/12/15
End of second phase

$$$

And the winner is…

	Challenge #	Lattice dim.	
Key agreement	*HIMMO1*	*27*	
	HIMMO3	*252*	
	HIMMO5	377	$
	HIMMO7	527	$
	HIMMO9	702	$
	HIMMO11	902	$
	HIMMO13	1377	$
	HIMMO15	5252	$

	Challenge #	Lattice dim.	
Key agreement + data verification	*HIMMO2*	*51*	
	HIMMO4	*296*	$
	HIMMO6	450	$
	HIMMO8	539	$
	HIMMO10	741	$
	HIMMO12	975	$
	HIMMO14	1386	$
	HIMMO16	5364	$

2/April/15
Announced NIST PQ workshop

26/May/15
Website online

26/June/15
First solution for an easy challenge

15/August/15
End of first phase

Moon Sung Lee;
Seoul National University.

$$$

31/12/15
End of second phase

Might be you!

$$$

Participation so far….

Challenges downloaded ~ 20 times

Country	Sessions	% New Sessions	New Users	Pages / Session	Avg. Session Duration
	1,024 % of Total: 100.00% (1,024)	39.16% Avg for View: 39.06% (0.25%)	401 % of Total: 100.25% (400)	3.05 Avg for View: 3.05 (0.00%)	00:02:45 Avg for View: 00:02:45 (0.00%)
1. Netherlands	252 (24.61%)	32.94%	83 (20.70%)	4.69	00:04:05
2. Germany	220 (21.48%)	39.09%	86 (21.45%)	2.72	00:01:57
3. Spain	106 (10.35%)	45.28%	48 (11.97%)	2.47	00:02:34
4. South Korea	90 (8.79%)	7.78%	7 (1.75%)	3.37	00:03:23
5. United States	62 (6.05%)	74.19%	46 (11.47%)	1.77	00:01:15
6. Canada	55 (5.37%)	25.45%	14 (3.49%)	1.75	00:02:23
7. France	49 (4.79%)	83.67%	41 (10.22%)	2.20	00:01:29
8. Japan	37 (3.61%)	37.84%	14 (3.49%)	2.97	00:04:48
9. Romania	34 (3.32%)	11.76%	4 (1.00%)	2.44	00:02:53
10. United Kingdom	28 (2.73%)	46.43%	13 (3.24%)	2.11	00:01:19

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 .**

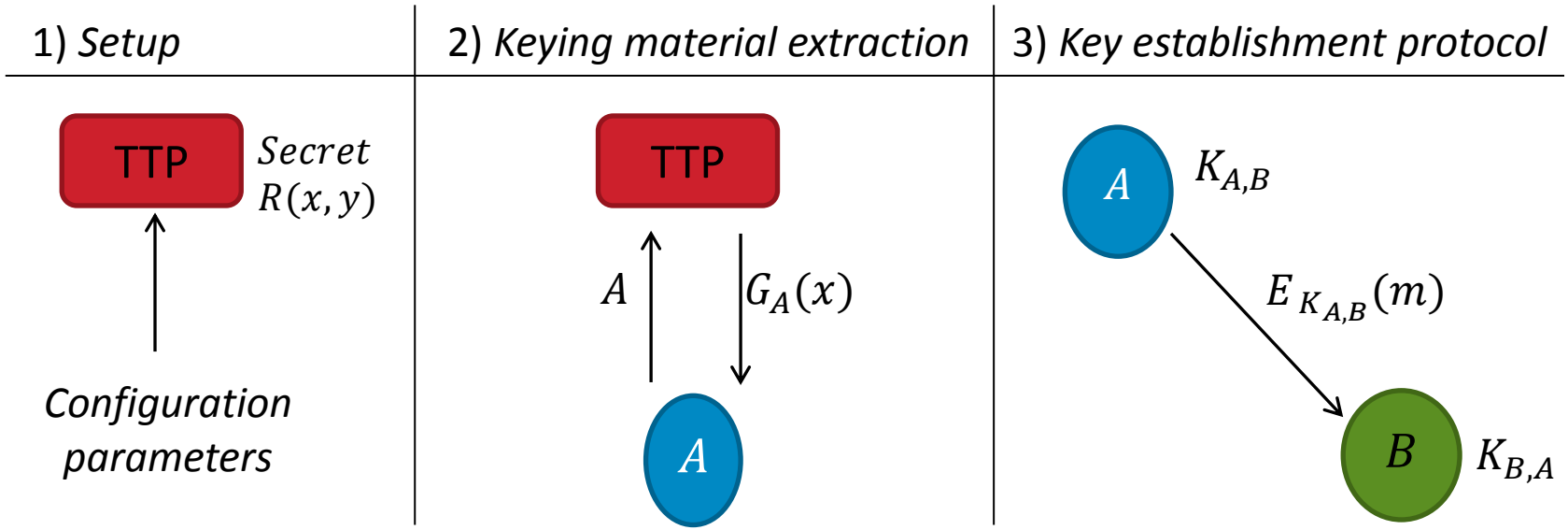
  Equivalent to a close lattice vector problem in a lattice of dimension $\alpha + 1 + c$. For HIMMO parameters $r = 2^b$ and $N \approx 2^{(\alpha+1)B+b}$, c must be $\gtrsim (\alpha + 1)(\frac{\alpha B}{2b} + 1)$ to find a unique y_0.

- **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.

HIMMO

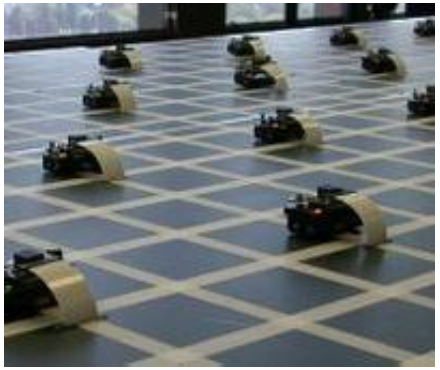
Efficient and collusion-resistant key pre-distribution scheme



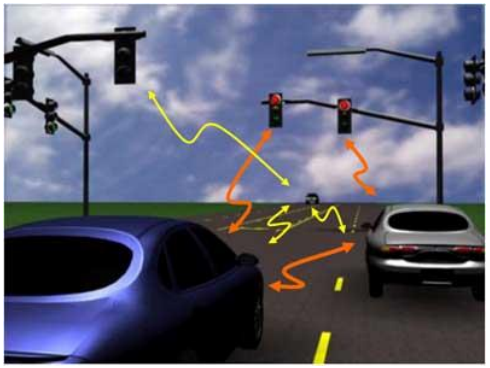
- Many practical applications in industry
- Important to have open verification of the scheme

Some security & operational goals & features

Energy efficient



Real-time



Fits device lifecycle

Simple operation

(**Quantum**) Secure


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, 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**.
[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. In ESORICS 2015; also presented at NIST workshop on Cybersecurity in a Post-Quantum World, 2015.
[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. In ALGOSENSORS 2015; also presented at NIST Lightweight Cryptography Workshop, 2015.