Rump Session 2016

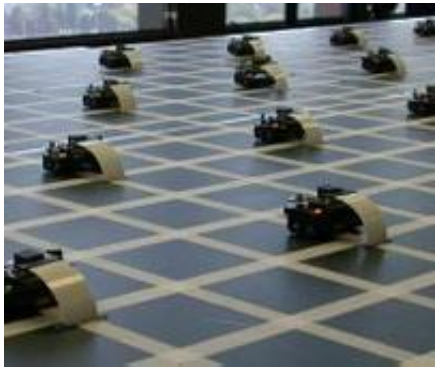
The HIMMO Scheme and its Contest

Oscar Garcia-Morchon; Ronald Rietman; Ludo Tolhuizen; Jose Luis Torre-Arce; Moon Sung Lee; Domingo Gomez; Jaime Guiterrez; Berry Schoenmakers

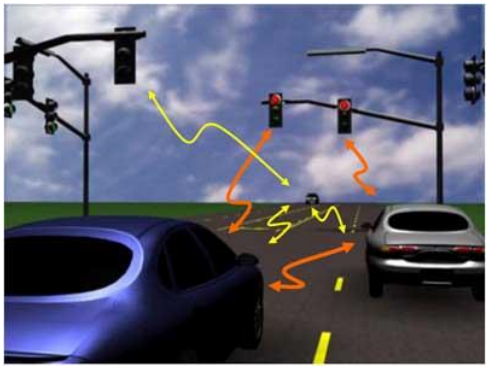
Philips Research; University of Luxembourg; University of Cantabria; University of Cantabria; TU/e

Nice features to have

Energy efficient



Small messages and real-time



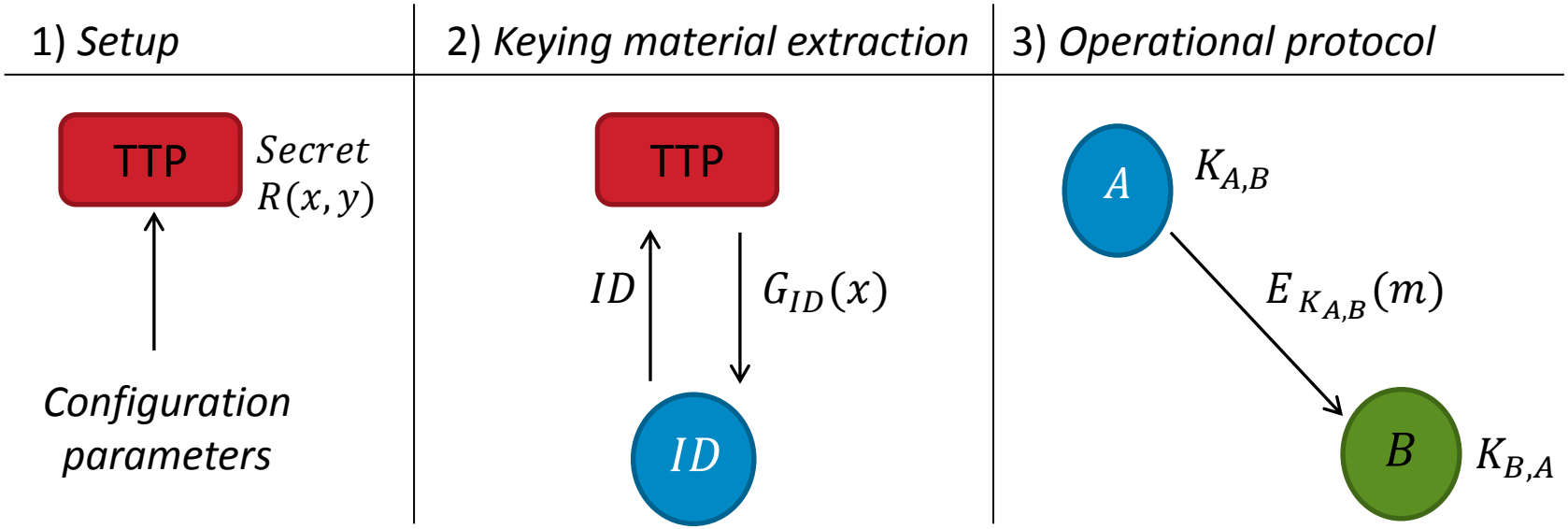
Fits device lifecycle

Simple operation

Quantum Secure

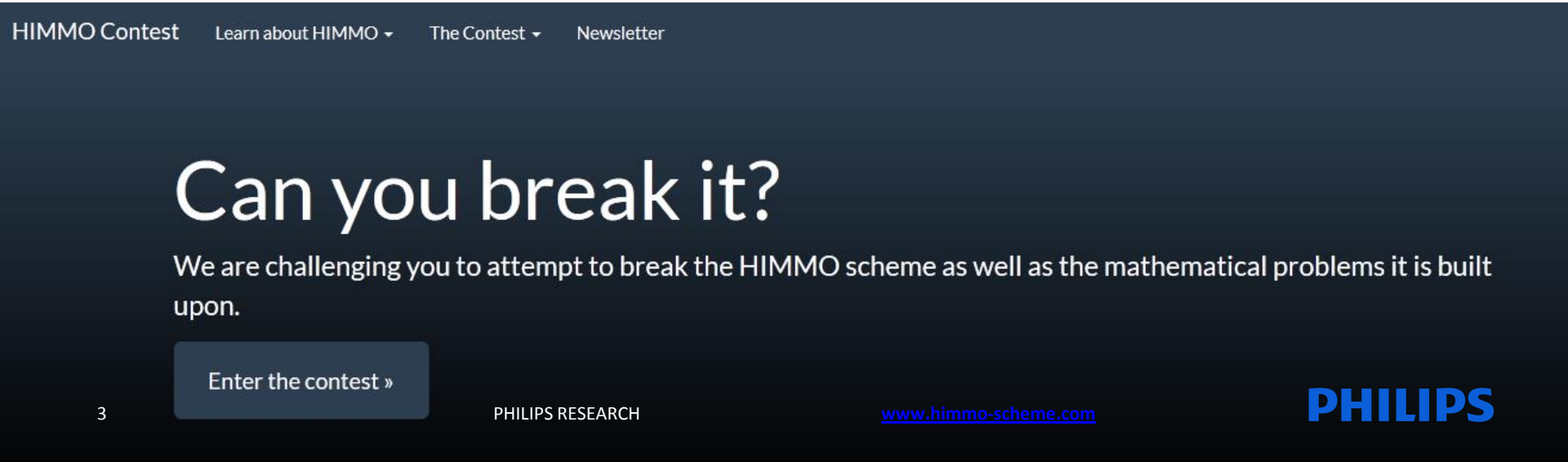
HIMMO

***Efficient* quantum- and collusion-resistant key pre-distribution scheme**



Contest 2015

www.himmo-scheme.com



Results from 2015 Contest

Attacks and parameter choices in HIMMO

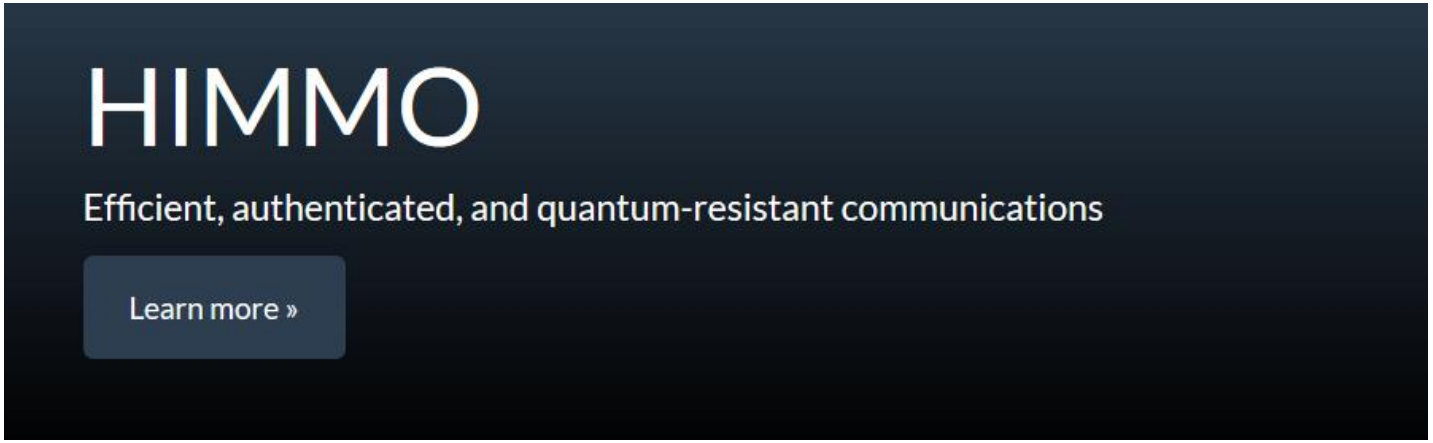
Oscar García-Morchón[1], Ronald Rietman[1], Ludo Tolhuizen[1], Jose-Luis Torre-Arce[1], Moon Sung Lee[2], Domingo Gómez-Pérez[3], Jaime Gutiérrez[3], and Berry Schoenmakers[4]

[1] Philips Research, Eindhoven, The Netherlands
[2] University of Luxembourg
[3] University of Cantabria, Santander, Spain
[4] TU Eindhoven, The Netherlands

https://eprint.iacr.org/2016/152.pdf

New Phase for the HIMMO Contest

www.himmo-scheme.com



About the HIMMO Contest

- No time limit for five challenges,
- 1000 Euros per solved challenge

#	α
HIMMO1	2000
HIMMO2	4000
HIMMO3	8000
HIMMO4	16000
HIMMO5	32000

About the HIMMO Contest

- No time limit for five challenges,
- 1000 Euros per solved challenge

#	α	For the best known attack
-	700	Can be attacked with LLL
HIMMO1	2000	Root Hermite factor of 1.011
HIMMO2	4000	Root Hermite factor of 1.005
HIMMO3	8000	
HIMMO4	16000	
HIMMO5	32000	

Parameter choice

- Very conservative, still practical and best performance:
  - one-way key exchange and verification of parameters with 107 B and 0.68 ms on standard PC for HIMMO2

- More details at www.himmo-scheme.com or on Friday

RUB

ECRYPT CSA


PHILIPS