The HIMMO Scheme and its Contest

Oscar Garcia-Morchon, Ronald Rietman, and Ludo Tolhuizen
Philips Research, The Netherlands

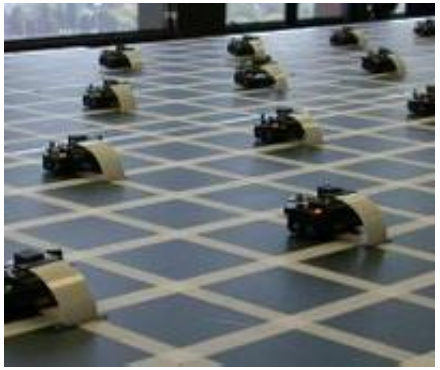
February 26th 2016

innovation + you

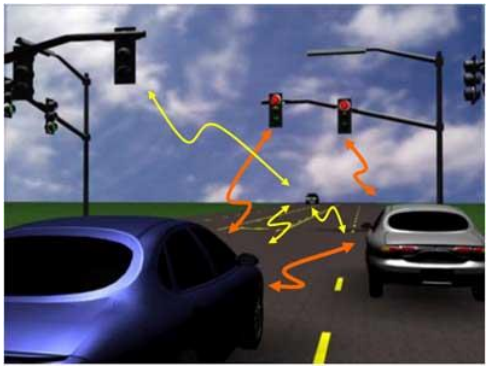
PHILIPS

Nice features to have

Energy efficient



Small messages and real-time



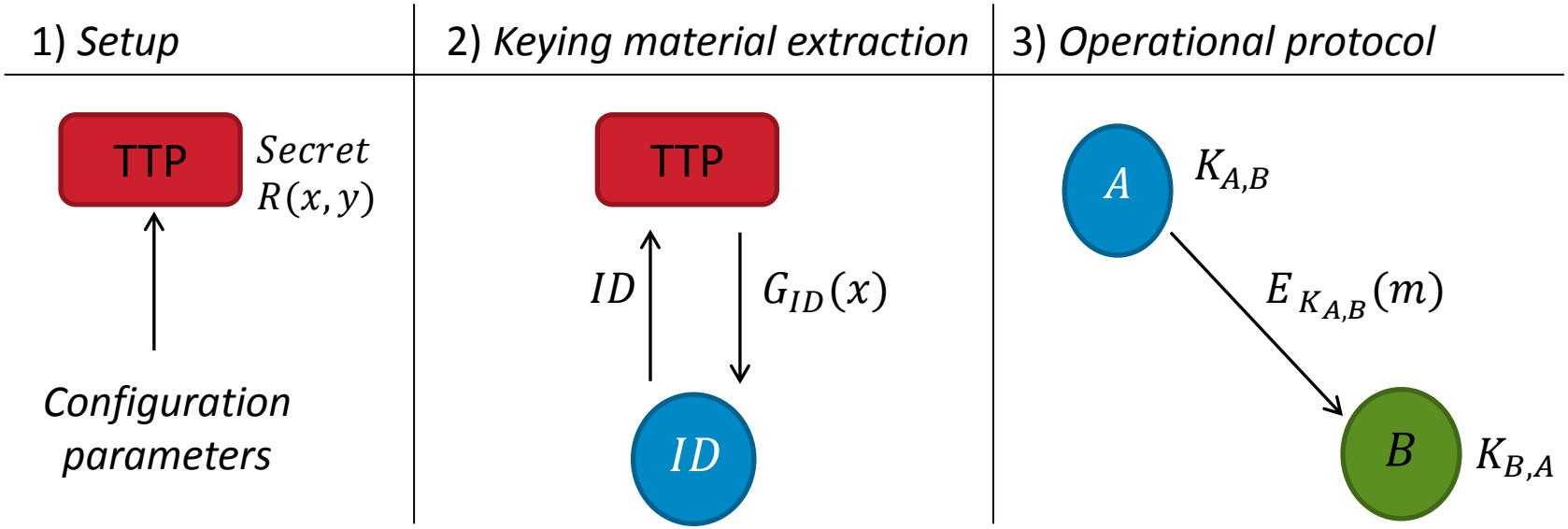
Fits device lifecycle

Simple operation

Quantum Secure

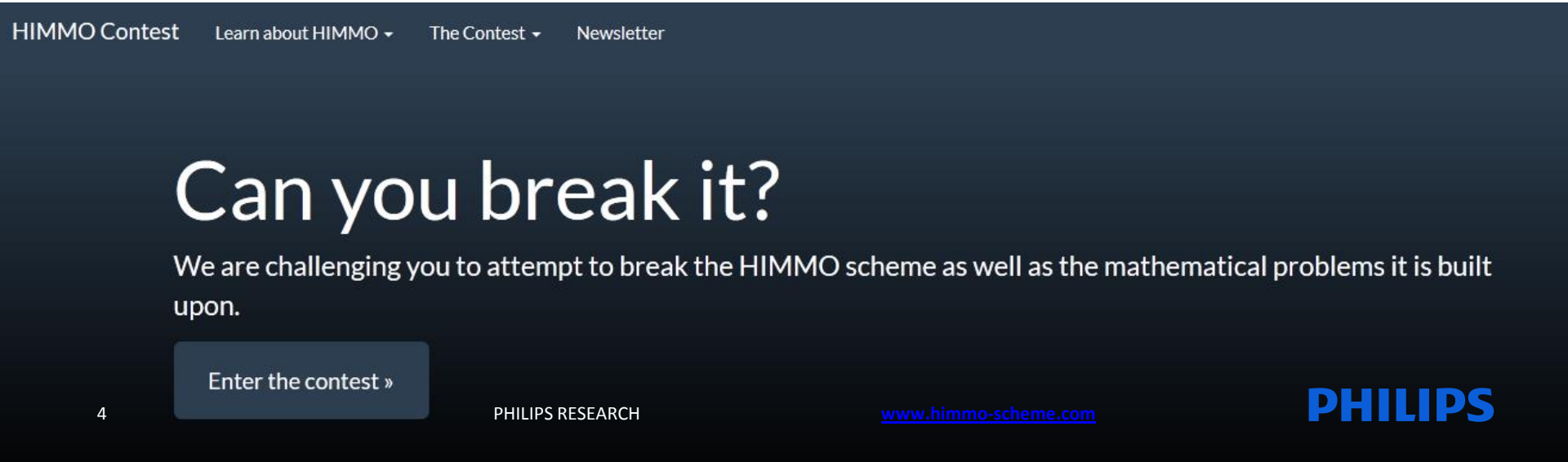
HIMMO

Efficient and collusion-resistant key pre-distribution scheme



Open verification 2015

www.himmo-scheme.com



Results

- Challenges downloaded ~ 30 times.
- Small instances of the **HI** and **MMO** Challenges solved
- As for the **HIMMO** Challenge:
  - Goal: guess the key shared between a pair of devices.
  - All challenges solved, except HIMMO15 with $\alpha = 100$

Who and how?

- Moon Sung Lee (University of Luxemburg) developed a method based on Orthogonal Lattices to attack a single node by finding an approximate solution to the MMO problem.

- This method:
  - does not solve MMO challenges
  - but solves HIMMO challenges of low alpha value.

Updated parameters

- The choice of:

  N independent of α.

- Improves HIMMO performance a factor α so that the security parameter α can be increased to the range of thousands or even tens of thousands.

- For this range:
  - HIMMO remains very efficient
  - existing attacks involve reducing a very large lattice

Details can be found online

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


PHILIPS