Lightweight Cryptographic Techniques for IoT

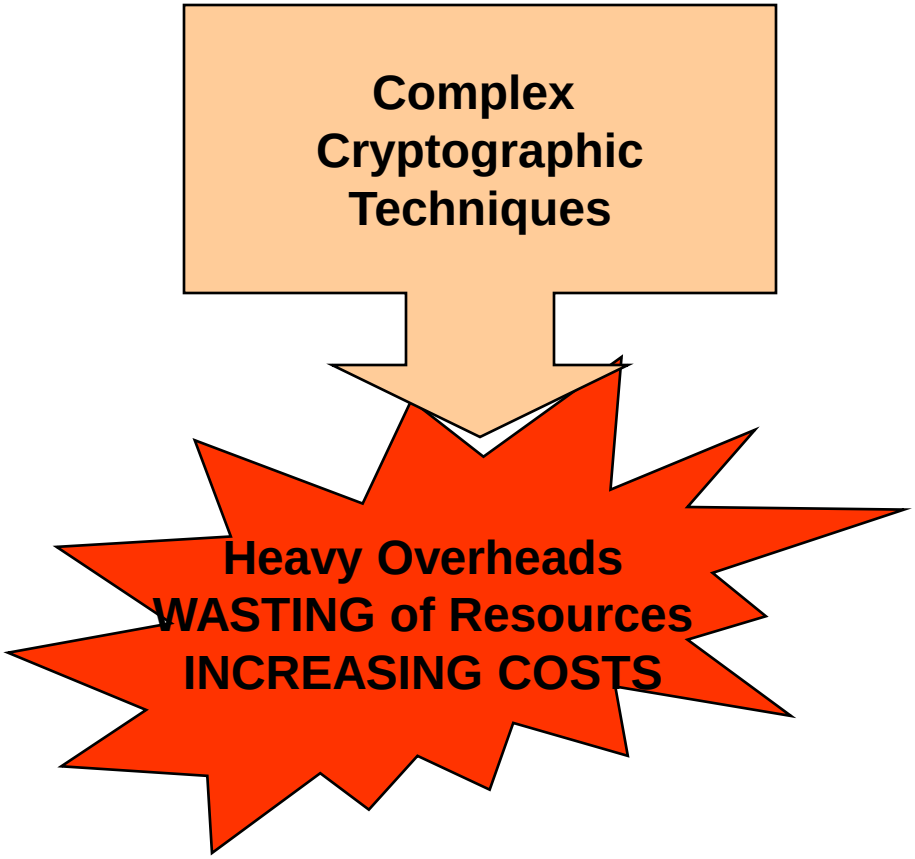
Miodrag Mihaljevic
Mathematical Institute
Serbian Academy of Sciences and Arts

Iot Week – Panel:

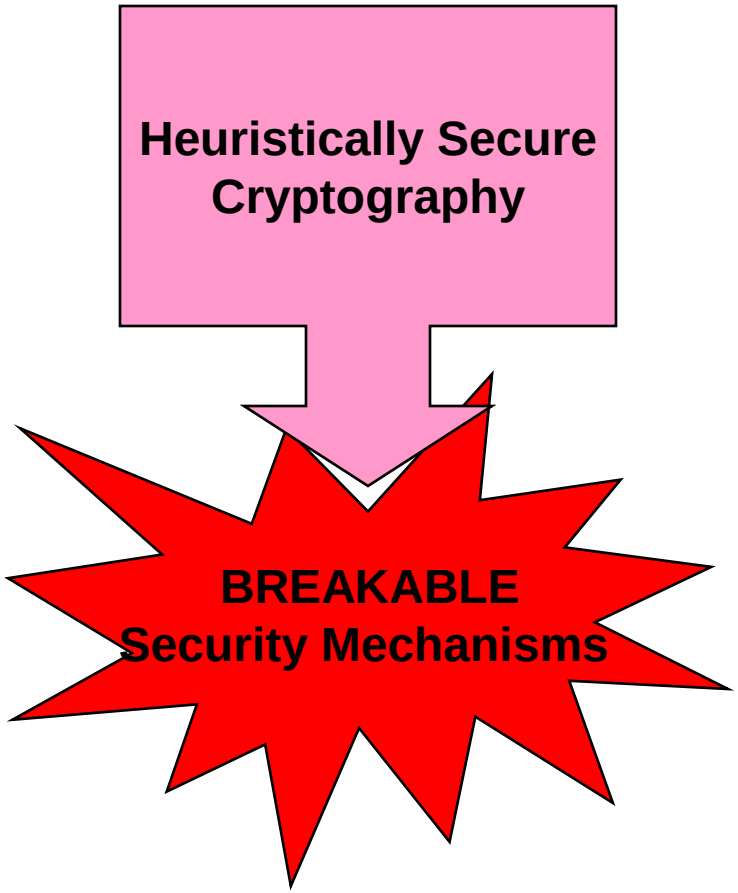
Privacy protection in IoT world: challenges and potential approaches

Belgrade, 2nd of June, 2016

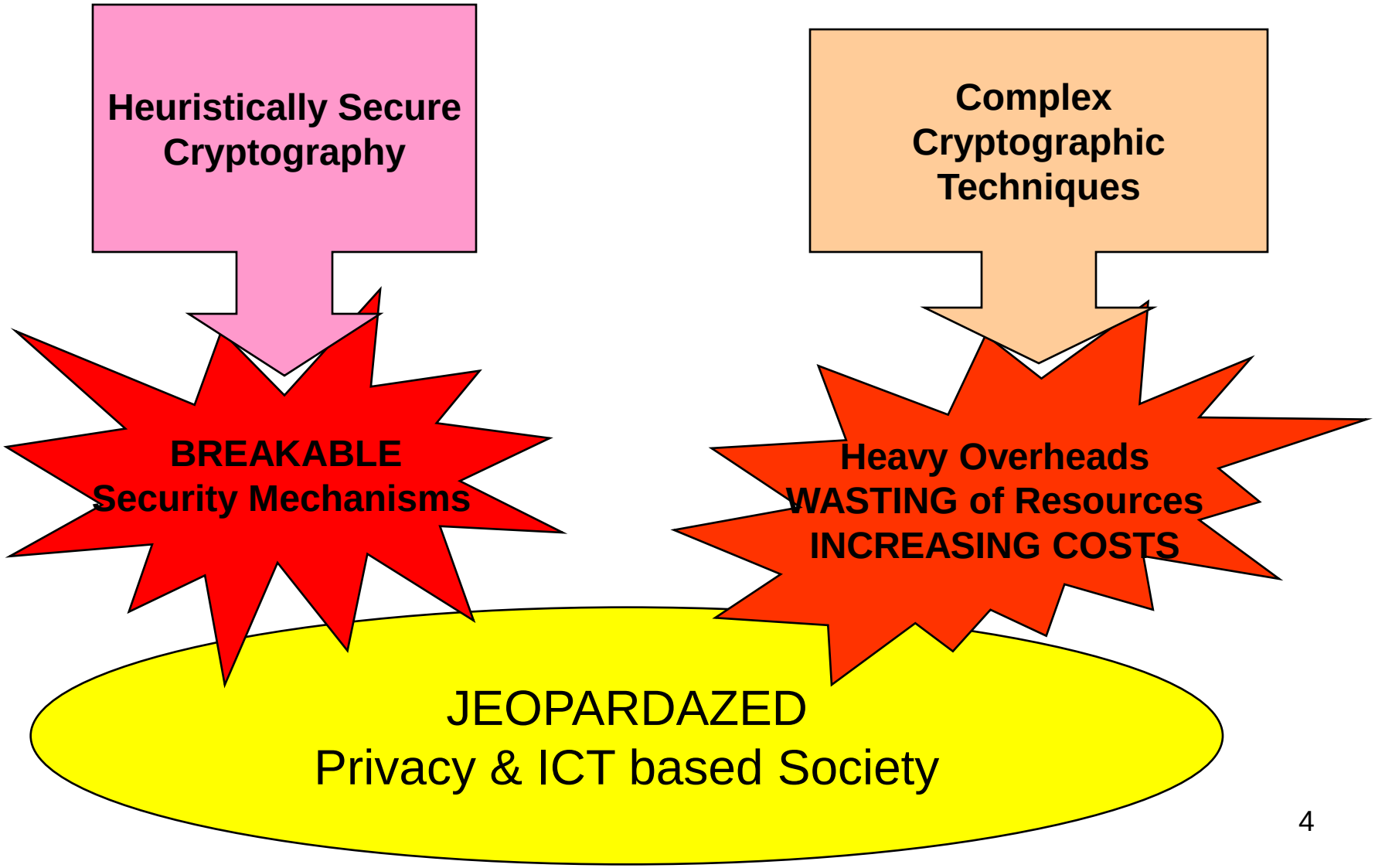
Privacy Related Technical Issues
Potential Disastrous Impacts (1)



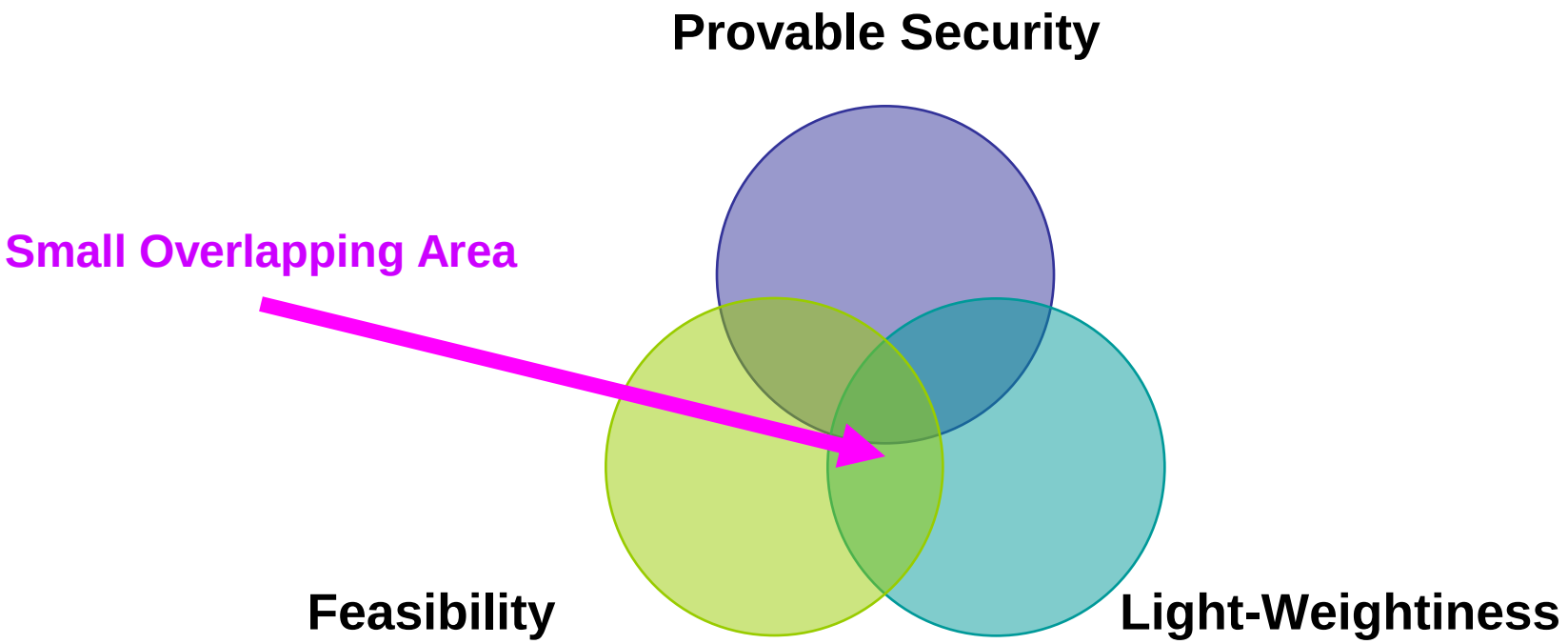
Privacy Related Technical Issues
Potential Disastrous Impacts (2)



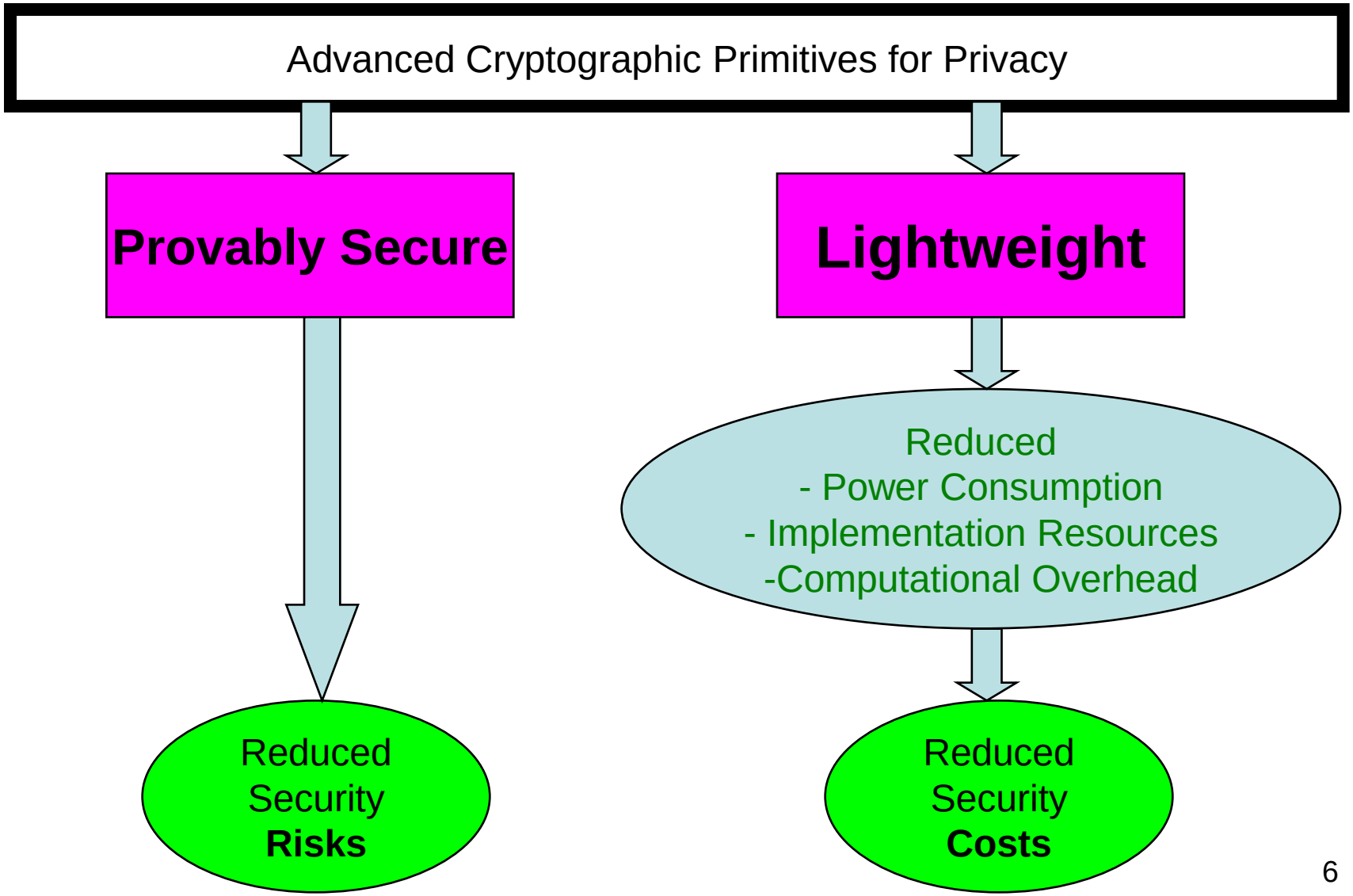
Privacy Related Technical Issues
Potential Disastrous Impacts (3)



Cryptographic Challenges within Cryptographic Primitives



Goals of the Advanced Construction



Minimization of the Overheads Implied by Security Mechanisms

- minimization of the implementation overheads
- minimization of the computational overheads (and particularly: minimization of the key management, authentication and encryption overheads)
- minimization of the communications overheads
- **minimization of power-consumption**

Significance of Lightweight Cryptographic Techniques has been well recognized

ETSI, ENISA (EU), NIST (US), CRYPTREC (JP),
EU Horizon 2020, EU COST,
ISO 29192, ISO18033,
documents of oneM2M, Clod Security Alliance

Organization of CRYPTREC（2013-）

(Chair: H. Imai)

Advisory Board for Cryptographic Technology
(Secretariat: MIC & METI)

NISC (National Information Security Center)

ISPC (Information Security Policy Council)

(Chair: H. Imai)

Cryptographic Technology Evaluation Committee (Secretariat: NICT, IPA)

① Monitoring and evaluation of the security and implementation properties of the cryptographic technology
② Research on new-generation cryptographic technology
③ Research on secure utilization of cryptographic technology

- Cryptanalysis Evaluation WG
- **Lightweight Cryptography WG**

(Chair: T. Matsumoto)

Cryptographic Technology Promotion Committee (Secretariat: IPA, NICT)

① Research on the promotion of cryptographic technologies and the strengthening of ICT security industries
② Research on the utilization status of cryptographic technologies and research of their promotion strategy
③ Research on the strategy of cryptographic policy from mid-and-long term viewpoints

- Standardization Promotion WG
- Operational Guideline WG

Reference of Math. Inst. Serbian Acadamy of Sci & Arts Relevant for Security Evaluation and Design of Lightweight Cryptography

- Over **60** results reported in top-level publications as **journal papers or book chapters**
- Over **70** results reported in the **Proceedings of International Meetings**
- **6 Granted Patents (Japan, US, China)**
- Over **2000 citations** of the reported results
- Participation in **over 10 international Projects**
- **The Most Prestigious Serbian National Award for 10-Years Scientific Achievements 2003-2012**
- **Member of Academia Europaea, elected in July 2014**

Main Messages

- Cryptograhic techniques plays **one of the main roles** for providing the privacy (they are a necessary technical component but not enough)
- An **open challenge** is design of advanced cryptographic techniques which provide are resistant against possible attacks and provide reduction of the overheads (**privacy is a top level issues but not the main functionality**)

Thank You Very Much for the Attention,

and

QUESTIONS Please!