Tutorial: The Energy Cost of Privacy and Security

Ayse Kivilcim Coskun[1], Paolo Palmieri[2], Francesco Regazzoni[3,4]
[1]Boston University, USA, *acoskun@bu.edu*
[2]University College Cork, Ireland, *p.palmieri@cs.ucc.ie*
[3]University of Amsterdam, Amsterdam The Netherlands, *f.regazzoni@uva.nl*
[4]Università della Svizzera italiana, Lugano, Swizterland, *francesco.regazzoni@usi.ch*

Security and privacy are key enablers (and often also a legal requirement) for a number of applications, including smart grid and smart cities, health care, data analytics, and personalized services. Because of this, research in the domain of security and privacy-preserving techniques is progressing at high pace. However, if on the one side the research community devoted large attention to the study of more efficient algorithms and the design of more efficient architectures implementing them, on the other, the energy cost and the energy implications of the use of these technologies have not yet been explored in the needed depth, with the majority of literature focusing on block ciphers. This tutorial exposes the community to the main current research results and best practices in this research area, and aims to foster the exchange of ideas between all the involved stakeholders. The tutorial presents the background and latest achievements in the field of energy assessment and reduction for security and privacy-preserving primitives. This tutorial covers the needed background on security algorithms, discusses their energy consumption, and presents, by means of relevant examples, how to design and implement security primitives that achieve a limited energy footprint. In particular, the focus is on two families of security primitives: block ciphers and privacy-preserving primitives. The tutorial introduces the basic concepts and the main algorithms belonging to these families, discusses recent advances in the domain, and presents in detail the energy consumption of these technologies and in their applications such as machine learning. Further, the tutorial will show optimizations that have been proposed to minimize the energy footprint of security primitives, with a particular focus on block ciphers, discussing also the design of lightweight and low-energy cryptographic algorithms. The tutorial concludes discussing open problems, limitations, and possible research directions. The tutorial is divided into three sections and will begin with a talk providing a detailed introduction of the needed concepts, to allow attendees not familiar with the topic to be able to successfully follow the whole tutorial. More in details, the sections are:

- "Introduction to Security Primitives and Privacy Preserving Technologies". This talk will introduce the audience to the security primitives and the relevant privacy preserving technologies and protocols, [1] that will be analyzed in the rest of the tutorial.
- "Energy Assessment of Security Primitives". This talk summarizes current research in energy assessment [2] of security primitives, reporting the method used to assess them and presenting literature result on the energy consumption of security primitives. The talk will conclude presenting open problems and future research directions.
- "Energy Efficient Design and Implementation of Security Primitives". This talk reviews the strategies that have been applied to security primitives to reduce their energy consumption and presents the algorithms that have been designed, since the beginning, to achieve a limited energy footprint [3], [4]. The talk will conclude presenting open problems and future research directions.

Acknowledgments

Partially funded by the European Union, grant No. 101135183 (MYRTUS) and grant No. 101095717 (SECURED). Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] S. N. Eshun and P. Palmieri, "A privacy-preserving protocol for indoor wi-fi localization," in *Proceedings of The 16th ACM International Conference on Computing Frontiers*, 2019, pp. 380–385.

[2] C. Hankendi, A. K. Coskun, and H. Hoffmann, "Adapt&cap: Coordinating system-and application-level adaptation for power-constrained systems," *IEEE Design & Test*, vol. 33, no. 1, pp. 68–76, 2015.

[3] S. Banik, A. Bogdanov, and F. Regazzoni, "Exploring energy efficiency of lightweight block ciphers," in *Selected Areas in Cryptography–SAC 2015: 22nd International Conference, Sackville, NB, Canada, August 12–14, 2015, Revised Selected Papers 22*. Springer, 2016, pp. 178–194.

[4] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy," in *Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21*. Springer, 2015, pp. 411–436.

979-8-3315-2710-5/25/$31.00 ©2025 IEEE