Preface

In the recent years, we have assisted at a rising interest and dialogue between two approaches to security: the well-established cryptographic approach based on computational security and the recently explored physical-layer (or information theoretic) security, also known as unconditional security.

While both approaches have solid basis on the works by Shannon, their evolution over the years has taken different paths. On the one hand, cryptography typically relies on the difficulty of solving hard mathematical problems which can be drastically simplified with some a priori knowledge, i.e. the secret. This approach now faces various challenges from the ever-growing computational power available to end-users, and the increasing progress of quantum computing that promises to ultimately break computational barriers. On the other hand, physical-layer security aims at exploiting the physical characteristics of the channels over which a confidential communication occurs, providing a secret not available to attackers who experience different channels: under suitable assumptions, we can ensure that the attacker does not have any knowledge of the secret communication, irrespective of its computational power. Physical-layer security also has limits since it is prone to other types of attacks typically leveraging the physical implementation of devices (such as the use of multiple antennas), allowing, for instance, to capture information on the legitimate channel conditions, thus having access to the secret shared by the legitimate parties.

The two approaches have also developed their own performance metrics and methodologies, as well as their implemented solutions. A seminal work by Bellare, Tessaro and Vardy plays the role of a Rosetta Stone by putting side by side metrics and languages of the two worlds and establishing a bridge between them. In the meantime, engineers have been studying how to integrate the solutions into their products rather than relying exclusively on one of the two. Since then, works on code design and secure system architectures have been appearing, confirming this trend. Moreover, practical implementations of security systems may de-facto incorporate cryptography and physical-layer security. Examples include the use of physical characteristics (such as electrical noise) for the generation of random numbers then used for cryptography, or the use of two factors in authentication,

where the user is identified both by a password and physical characteristics (e.g. biometric features).

The aim of the Second Workshop on Communication Security (WCS), organized in 2017 in Paris and affiliated with Eurocrypt 2017, was to provide a forum to discuss cutting-edge cross-disciplinary research in these areas and to share visions for future advances. This book collects the contributions presented at the workshop.

The first two chapters are devoted to recent advances in physical-layer security techniques. Chapter "A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems" studies the vulnerabilities of physical-layer secret key generation schemes to denial of service attacks based on signal jamming and injection by an active attacker. Some relevant countermeasures based on optimal signalling schemes are also described. A scenario of the same type is considered in Chapter "Robust Secret Sharing for End-to-End Key Establishment with Physical Layer Keys Under Active Attacks" which addresses the issue of end-to-end key establishment between a sender and a receiver in the presence of a special class of active attackers, able to modify or drop messages in transit. This and other adversarial attacks are counteracted by using a robust secret sharing scheme.

The second group of chapters is devoted to cross-layer approaches between cryptography and physical-layer security. In the rigorous framework of semantic security, Chapter "Semantically-Secured Message-Key Trade-off over Wiretap Channels with Random Parameters" considers the secret message/secret key trade-off over wiretap channels with non-causal encoder channel state information and establishes a new bound on the region of semantically secure message/key pairs using a novel superposition coding scheme. This work lives in the physical-layer security domain, but benefits from a unified language to which cryptographers can also relate. With a similar cross-disciplinary approach, Chapter "Hash-then-Encode: A Modular Semantically Secure Wiretap Code" proposes a modular semantically secure wiretap code, relying on cryptographic tools such as efficiently invertible universal hash functions, as well as error correcting codes. Proof of security and capacity analysis provide a formal framework to a simple and elegant solution. Chapter "A CCA-Secure Cryptosystem Using Massive MIMO Channels" also combines physical-layer security with computational security and proposes to use the massive multiple input multiple output (MIMO) channel as a key to encrypt messages between the legitimate transmitter and receiver, while leaving the eavesdropper with an exponentially complex decoding problem. In this case, both the physical channel (which is not needed to be secret but clearly links the two legitimate parties) and the complexity associated with lattice decoding provide the desired security.

The third group of chapters is devoted to computational security approaches, with special focus on authentication techniques. Chapter "You Are How You Play: Authenticating Mobile Users via Game Playing" proposes the use of cognitive skills to complement password-based user authentication on mobile devices. In this two-factor approach, the user is requested to play small games which are based on the attentional paradigm of cognitive psychology. Chapter "Fuzzy Authentication Using Rank Distance" deals with authentication techniques specifically designed

for using biometric features, like fingerprints. Fuzzy authentication schemes using rank metric codes and linearized polynomials are proposed, as a valid alternative to classical schemes based on codes in the Hamming metric. Chapter "A McEliece-Based Key Exchange Protocol for Optical Communication Systems" proposes an application of the McEliece cryptosystem, that is a well-known public-key cryptosystem able to resist attacks based on quantum computers, to the context of authentication protocols for optical networks. In Chapter "An ICN-Based Authentication Protocol for a Simplified LTE Architecture", the authentication protocol used in the long-term evolution (LTE) cellular communication system is revised, and a simplified infrastructure supporting Internet protocol (IP) mobility is proposed, using the information centric networking paradigm. The proposed solution reduces the number of messages required to perform authentication.

The results presented in this book advance the state of the art in cross-disciplinary security research and significantly contribute to a vision of improved joint security.

Ancona, Italy
Egham, UK
Padova, Italy
March 2017

Marco Baldi
Elizabeth A. Quaglia
Stefano Tomasin

http://www.springer.com/978-3-319-59264-0

Proceedings of the 2nd Workshop on Communication Security
Cryptography and Physical Layer Security
Baldi, M.; Quaglia, E.A.; Tomasin, S. (Eds.)
2018, XIII, 141 p. 27 illus., 14 illus. in color., Hardcover
ISBN: 978-3-319-59264-0