Mauro Barni, Ton Kalker, and
Stefan Katzenbeisser

Inspiring New Research in the Field of Signal Processing in the Encrypted Domain

We are excited to bring you this special issue of *IEEE Signal Processing Magazine* on signal processing in the encrypted domain (SPED). At first glance, processing of encrypted signals seems like an oxymoron: once signals are encrypted the necessary information to do any meaningful processing is obscured. Fortunately this contradiction is only seemingly, and there is a growing community of researchers exploring and discovering new methods to manipulate encrypted signals.

Among others, the need for SPED technologies originates from a growing societal awareness and relevance of security and privacy. On a daily basis, almost every one of us is sharing more personal data of greater diversity within an increasingly larger circle. Controlling access to and the use of this data is an ever more important concern, and cryptography-based techniques typically come to the rescue. Unfortunately, classic cryptographic primitives are designed to protect data at rest, but fail if the processor itself is untrusted. At the same time, the use of personal data becomes more varied, requiring more flexibility in processing and presentation. Being able to process a plethora of sensitive signals at potentially untrusted sites, without or minimally leaking information, is one of the main motivators for SPED technologies. Core technologies that are being investigated in the SPED community include foundational principles, cryptographic techniques specifically tailored towards processing of fuzzy signals, or homomorphic encryption schemes, allowing the performance of algebraic operations on encrypted data. Applying SPED technologies to real-world problems and enhancing the efficiency of SPED techniques is a second active focus of research that addresses a wide variety of contexts from biometry to video distribution.

[BEING ABLE TO PROCESS A PLETHORA OF SENSITIVE SIGNALS AT POTENTIALLY UNTRUSTED SITES, WITHOUT OR MINIMALLY LEAKING INFORMATION, IS ONE OF THE MAIN MOTIVATORS FOR SPED TECHNOLOGIES.]

In this special issue, we aim to provide the reader with a broad overview of the state of the art in SPED, both for core technologies and applications. The first two articles in this special issue introduce some general principles of SPED, one by Rane and Boufounos on nearest neighbor methods with minimal leakage of information and one by Troncoso-Pastoriza and Pérez-González on secure signal processing in the cloud.

The following four articles consider applications of SPED technologies for privacy protection: privacy-preserving biometrics by Bringer et al., private media search by Fanti et al., privacy-preserving speech processing by Pathak et al., and privacy preservation in smart metering systems by Erkin et al.

The next two articles focus on SPED in the context of media processing: secure watermarking by Bianchi and Piva and video distribution by Boho et al.

The final article in this issue by Aguilar-Melchor et al. takes us to the forefront of SPED, discussing fully homomorphic encryption as a candidate for solving many SPED-type problems.

Readers interested in a comprehensive, tutorial-like introduction to the basic cryptographic tools SPED relies on may refer to [1].

We wish you happy reading and hope that this special issue of *IEEE Signal Processing Magazine* will inspire new research in the exciting field of SPED.

REFERENCE

[1] R. (Inald) L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, 2013.

Digital Object Identifier 10.1109/MSP.2012.2229069
Date of publication: 12 February 2013