J Cryptol (2023)36:4
https://doi.org/10.1007/s00145-023-09444-8

Journal of CRYPTOLOGY

Editorial

Topical Collection on Computing on Encrypted Data

David Pointcheval
DIENS, École normale supérieure, CNRS, Inria, PSL University, Paris, France
david.pointcheval@ens.fr

Nigel Paul Smart
imec-COSIC, KU Leuven, Leuven, Belgium
Zama, Paris, France
nigel.smart@kuleuven.be

Online publication 25 January 2023

This issue contains the first in a series of papers which were solicited to Journal of Cryptology on the topic of Computing on Encrypted Data; which we broadly interpreted to mean Fully Homomorphic Encryption, Functional Encryption and Multi-Party Computation. These papers form a Topical Collection. Topical Collections are a kind of virtual Special Issues. Papers of a topical collection are published together with ordinary papers in one or more issues, but on the journal webpage they are indexed twice: once in their issue and once in a separate tab with the name of the Topical Collection.

The topic of Computing on Encrypted Data was selected due to the fact that this topic, which has a long theoretical pedigree, now has an increasing commercial and practical interest. This is not only due to improved technology, but also due to new regulations and applications such as provided by GDPR and blockchain applications.

We were particularly interested in papers which cover research related to implementation aspects, new applications of these technologies, real-life deployment issues, and other more applied aspects, as well as the more traditional cryptographic papers covering new schemes and protocols and relatively short papers. Papers which were extended versions, or merges, of conference papers, were considered out of scope for this Topical Collection.

We received twenty submissions, and we tried to ensure that all papers were refereed by three people within three months. Sometimes reviewers did not respond quickly, so for those papers we went with the two received reviewers when the two reviewers were in agreement. Being a journal we were able to, after the initial reviews, enable a back-forth conversation between the authors and the reviewers via various resubmissions of new versions. This was done until the (majority of the) reviewers and authors were happy with the final version of the papers.

We thank the authors who submitted their papers to this Topical Collection. We also thank the reviewers who agreed to review the papers in a short time frame (much shorter than is normal for Journal of Cryptology reviews). We hope that such short turn arounds for reviews can soon become the norm and not the exception. Finally, we hope you enjoy reading the papers.