Journal of Computer Security 30 (2022) 1–2
DOI 10.3233/JCS-219000
IOS Press


# Special issue: Security and Cryptography for Networks – SCN 2020

Clemente Galdi [a,*] and Vladimir Kolesnikov [b]
[a] *University of Salerno, Italy*
*E-mail: clgaldi@unisa.it*
[b] *Georgia Tech, GA, United States*
*E-mail: kolesnikov@gatech.edu*

Keywords: Cryptography, secure computation

This special issue includes several papers that have been selected from the program of the 12th Conference on Security and Cryptography for Networks. The conference, originally planned in Amalfi (SA), Italy, was held online on Sept. 14–16, 2020, due to Covid-19. The papers appearing in the present issue have been extended from their original conference versions, and have gone through a second rigorous reviewing process. We briefly review the papers included in this issue:

*Efficient Protocols for Oblivious Linear Function Evaluation from Ring-LWE* by Carsten Baum, Daniel Escudero, Alberto Pedrouzo-Ulloa, Peter Scholl and Juan Ramón Troncoso-Pastoriza constructs Oblivious Linear Function Evaluation (OLE) protocols from the Ring-LWE problem. OLE has recently been shown to be very useful in practical multiparty computation, and this work proposes lattice-based OLE protocols and analyzes their standalone efficiency.

In *Double-Authentication-Preventing Signatures in the Standard Model*, Dario Catalano, Georg Fuchsbauer and Azam Soleimanian present efficient DAPS schemes that are secure in the standard model and support large address spaces. DAPS is a special type of signature meant to punish the signer if it signs two messages with the same "address." For example, this may be desired if the signer issues two different certificates for the same domain.

The paper *Private Identity Agreement for Private Set Functionalities* by Benjamin Terner, Benjamin Kreuter and Sarvar Patel explores an interesting twist on private set intersection. If we want to compute a function of the intersection of our data, we need to first "align" our data so that we hold identical identifiers for any records that match. The situation is even more complicated when identifiers are "fuzzy" as in real-world data. In those cases, one party may hold several records corresponding to the same person, but be unaware of this fact. Only when combined with another data set will this fact be evident (if the other data set contains a record that connects with both). This paper proposes a method for two parties to privately assign identifiers to records in this kind of scenario. The main challenge here is the transitive nature of whether two records match.

In *Fast Threshold ECDSA with Honest Majority*, Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, Jakob Illeborg Pagter and Michael Bæksvang Østergaard propose a new faster threshold variant of the ECDSA signature scheme.

*Corresponding author. E-mail: clgaldi@unisa.it.

In *Anonymity and Rewards in Peer Rating Systems*, Lydia Garms, Siaw-Lynn Ng, Elizabeth A. Quaglia, and Giulia Traverso study rewards/reputation in peer-rating systems while preserving anonymity. Being anonymous allows users to provide honest reviews without the risk of retaliation, but it also allows malicious users to provide negative feedback, or collude to inflate their reputation. The approach taken here is to reward honest ratings, and ensure accurate rewarding by splitting the roles of keeping reputation and keeping tabs of rewards into two parties/servers.

Finally, in *Gradual GRAM and Secure Computation for RAM Programs*, Carmit Hazay and Mor Lilintal consider the notion of Gradual ORAM and Garbled RAM (GRAM), which they build by optimizing previous GRAM. At the high level, Gradual ORAM/GRAM does not consider an explicit initialization algorithm. Instead, it views initialization as a list of insertions, which can be executed in CPU steps at the beginning of the program.

This special issue has been possible thanks to the joint work of many people. We would like to thank all the authors of papers in this special issue, and all SCN 2020 authors. We thank the reviewers for providing helpful comments to authors, which undoubtedly improved presentation. Finally, we would like to thank the Editors in Chief of Journal of Computer Security and the staff of the Journal Editorial Office for their kind help and support.