cryptography

MDPI

Editorial

Special Issue on Cryptographic Protocols

Andreas Vogt

School of Engineering, University of Applied Sciences Northwestern Switzerland, Bahnhofstrasse 6,
5210 Windisch, Switzerland; andreas.vogt@fhnw.ch

Received: 21 August 2018; Accepted: 21 August 2018; Published: 22 August 2018

Cryptographic protocols, originating from the goal to guarantee confidentiality, authentication, and integrity, nowadays go far beyond these traditional goals. More and more complex protocols have been developed that play a more and more important role in our daily lives, and are about to replace classic non-electronic procedures, such as voting, or even cash.

This Special Issue covers some aspects of this broad area. More specifically, four interesting papers each focusing on a different aspect of our daily lives, namely Voting, Cash, Smart Metering, and Key Distribution, are published in this issue.

The first paper deals with Smart Metering which enables fine-grained utility consumption measurements. However, such fine-grained measurements raise privacy issues as the precise time at which utilities were consumed might leak sensitive information. Two smart meter billing protocols addressing the problem are described and their performance characteristics are analyzed on a variety of hardware with the conclusion that some of the widely used primitives, Pedersen Commitments for instance, may take too much time for the fine-grained billing.

The second paper belongs to the field of quantum cryptography, more specifically, quantum key distribution. As there are information-theoretic secure crypto schemes, such as the one-time pad, a secure distribution of symmetric keys is of great importance. In this paper, a quantum key distribution system was built on the basis of the scheme with automatic compensation of polarization mode distortions.

The third paper takes a critical look at Blockchain-based systems. The famous Bitcoin crypto currency is one example of a system which is based on the Blockchain technology. Such systems have many advantages, in particular when it comes to privacy of both the transactor and the recipient. Furthermore, there is no need of a central authority which would be kind of a single point of attack. The biggest criticism of such systems found in this paper are the demand for anonymity (which encourages cybercrime) and the increasing amount of computational power (which means energy) for the mining.

The last paper deals with E-voting. A new protocol is proposed that addresses the inherent conflicts in voting, such as anonymity vs. accountability and privacy vs. verifiability, exploiting existing multi-party political dynamics such as in the US by splitting the trust equally among tallying authorities who have conflicting interests. The authors propose a fully transparent, auditable, and end-to-end verifiable voting protocol to enable open and fair elections. This is an important step in the development of a protocol suitable for national elections. It seems feasible (and the authors plan to do so) to further improve the system addressing coercion resistance.

Acknowledgments: The guest editor would like to thank all authors and reviewers for their contributions that helped to achieve this Special Issue.

Conflicts of Interest: The author declares no conflict of interest.