SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Giulia Traverso • Denise Demirel
Johannes Buchmann

Homomorphic Signature Schemes

A Survey

Springer

Giulia Traverso
Theoretische Informatik
Technische Universität Darmstadt
Darmstadt, Hessen, Germany

Denise Demirel
Theoretische Informatik
Technische Universität Darmstadt
Darmstadt, Hessen, Germany

Johannes Buchmann
Theoretische Informatik
Technische Universität Darmstadt
Darmstadt, Hessen, Germany

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-32114-1 ISBN 978-3-319-32115-8 (eBook)
DOI 10.1007/978-3-319-32115-8

Library of Congress Control Number: 2016935494

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

In the last years, there has been an increasing interest in homomorphic signature schemes. Thus, many schemes have been proposed that are suitable for a lot of different applications. In this work, we overcome the extensive state of the art by presenting a survey of the existing approaches and the properties they provide. In addition, we look into three interesting use cases for homomorphic operations on authenticated data; these are electronic voting, smart grids, and electronic health records. We discuss their requirements, show to what extent the existing solutions meet these conditions, and highlight promising directions for future work.

Homomorphic signature schemes have been initially designed to establish authentication in network coding and to address pollution attacks (see [18]). However, since they allow for computations on authenticated data, they are also a useful primitive for many other applications. In fact, after Johnson et al. introduced a formal definition and a precise framework for homomorphic signatures in 2002 (see [46]), in the following years, many schemes have been presented and discussed. The first schemes proposed only allow to perform linear computations on authenticated data (e.g., [71, 72, 76], and [24]). These approaches have been further improved with respect to efficiency, security, and privacy [5–7, 15, 18, 21, 22, 22, 34, 36, 65]. In addition, to be more flexible, solutions have been developed supporting polynomial functions [14, 23, 43], or even coming without any restrictions on the functions themselves, so-called fully homomorphic signature schemes [19, 41]. However, all these solutions assume that each input signature has been generated using the same private key. To overcome this restriction, the homomorphic property has been added to the aggregate signature schemes [45, 74] allowing for operations on signatures generated using even different secret-public key pairs.

In this work, we start by providing a formal definition of these four types of homomorphic signature schemes. First, the passage from the digital signature schemes to the homomorphic ones is formally described, where the novelties introduced by the homomorphic property itself are highlighted. Afterward, it is described how to obtain the linearly homomorphic signature schemes from the merely homomorphic ones. And then, starting from the linearly homomorphic signature schemes, it is shown how to derive the schemes supporting polynomial

functions and how to define the fully homomorphic signature schemes. Finally, schemes that allow computations on signatures generated using different secret-public key pairs are formally described.

Up to our knowledge, this survey is the first such work providing both a description of each single homomorphic signature scheme and a description of the whole general framework in a methodical and didactic approach. Indeed the survey proposed in [73] is not up to date, while in [20] the existing homomorphic signature schemes are just listed, without any deeper discussions. Furthermore, in this survey, we also discuss the possible use cases electronic voting, smart grids, and electronic health records. For each use case, concrete examples of how improvements can be achieved by the usage of homomorphic signature schemes are provided, together with the definition of the minimal requirements these schemes should fulfill. Furthermore, it is shown which of the currently existing homomorphic signature schemes are suitable for which of the use cases in question. When that is not the case, directions for future works are proposed.

In Chap. 1, the definition of general digital signature schemes is recalled, and the formal description of the homomorphic signature schemes is provided. Chapter 2 provides a description of the linearly homomorphic signature schemes, the homomorphic signature schemes for polynomial functions, the fully homomorphic signature schemes, and the homomorphic aggregate signature schemes. In Chap. 3, interesting properties of homomorphic signature schemes are discussed. The description of each of the currently existing homomorphic signature scheme and the properties they provide follow in Chap. 4. In Chap. 5, the usage of homomorphic signature schemes for each of the aforementioned use cases is presented. Finally, in Chap. 6, a conclusion is given and possible directions for future work are shown.

Darmstadt, Germany
February 2016

Giulia Traverso
Denise Demirel
Johannes Buchmann

Acknowledgments

This work has been co-funded by the European Union's Horizon 2020 research and innovation program under grant agreement no. 644962. In addition, it has received funding from the DFG as part of project Long-Term Secure Archiving Within the CRC 1119 CROSSING. We would like to thank also Lucas Shabhüser, Nina Bindel, Daniel Slamanig, and David Derler for the nice discussions.

Contents