

# SpringerBriefs in Computer Science

## Series Editors

Stan Zdonik, Brown University, Providence, USA  
Shashi Shekhar, University of Minnesota, Minneapolis, USA  
Jonathan Katz, University of Maryland, College Park, USA  
Xindong Wu, University of Vermont, Burlington, USA  
Lakhmi C. Jain, University of South Australia, Adelaide, Australia  
David Padua, University of Illinois Urbana-Champaign, Urbana, USA  
Xuemin (Sherman) Shen, University of Waterloo, Waterloo, Canada  
Borko Furht, Florida Atlantic University, Boca Raton, USA  
V.S. Subrahmanian, University of Maryland, College Park, USA  
Martial Hebert, Carnegie Mellon University, Pittsburgh, USA  
Katsushi Ikeuchi, University of Tokyo, Tokyo, Japan  
Bruno Siciliano, Università di Napoli Federico II, Napoli, Italy  
Sushil Jajodia, George Mason University, Fairfax, USA  
Newton Lee, Newton Lee Laboratories, LLC, Tujunga, USA

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

© The Author(s) 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

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

<b>1</b>	<b>From Digital to Homomorphic Signature Schemes</b>	1
1.1	Digital Signatures	1
1.2	Digital Signature Schemes Security Definition	2
1.2.1	Known-Message Attack	3
1.2.2	Chosen-Message Attack	4
1.2.3	Adaptive Chosen-Message Attack	5
1.3	Homomorphic Signature Schemes	6
1.4	Homomorphic Signature Schemes Security Definition	9
<b>2</b>	<b>Homomorphic Signature Schemes</b>	11
2.1	Homomorphic Signature Schemes for the Single-User Scenario	11
2.1.1	Linearly Homomorphic Signature Schemes	11
2.1.2	Homomorphic Signature Schemes for Polynomial Functions	13
2.1.3	Fully Homomorphic Signatures	14
2.2	Homomorphic Signature Schemes for the Multi-Users Scenario	14
2.2.1	Multiple Sources Homomorphic Signature Schemes	15
2.2.2	Homomorphic Aggregate Signature Schemes	17
<b>3</b>	<b>Evaluation of Homomorphic Signature Schemes</b>	23
3.1	Hardness Assumptions	23
3.1.1	Bilinear Groups	23
3.1.2	RSA	26
3.1.3	Lattices	27
3.2	Efficiency and Size	29
3.3	Security	30
3.3.1	Weak Adversary	30
3.3.2	Strong Adversary	31
3.4	Privacy	32
3.5	Random Oracle Model vs. Standard Model	33

- 4 State of the Art of Homomorphic Signature Schemes** ..... 35
  - 4.1 Linearly Homomorphic Signature Schemes Defined Over Bilinear Groups ..... 35
    - 4.1.1 Signing a Linear Subspace: Signature Schemes for Network Coding, by Boneh et al. [18] ..... 36
    - 4.1.2 Homomorphic Network Coding Signatures in the Standard Model, by Attrapadung and Libert [5] ..... 36
    - 4.1.3 Computing on Authenticated Data: New Privacy Definitions and Constructions, by Attrapadung et al. [6]..... 37
    - 4.1.4 Efficient Network Coding Signatures in the Standard Model, by Catalano et al. [22] ..... 37
    - 4.1.5 Improved Security for Linearly Homomorphic Signatures: A Generic Framework, by Freeman [34] ..... 37
    - 4.1.6 Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures, by Attrapadung et al. [7] ..... 38
    - 4.1.7 Secure Network Coding Against Intra/Inter-Generation Pollution Attacks, by Guangjun and Bin [42] ..... 38
    - 4.1.8 Summary of Linearly Homomorphic Signature Schemes Defined over Bilinear Groups..... 39
  - 4.2 RSA-Based Linearly Homomorphic Signature Schemes ..... 39
    - 4.2.1 Secure Network Coding Over the Integers, by Gennaro et al. [36] ..... 40
    - 4.2.2 Adaptive Pseudo-Free Groups and Applications, by Catalano et al. [21] ..... 40
    - 4.2.3 Efficient Network Coding Signatures in the Standard Model, by Catalano et al. [22] ..... 41
    - 4.2.4 Improved Security for Linearly Homomorphic Signatures: A Generic Framework, by Freeman [34] ..... 41
    - 4.2.5 Summary of RSA-Based Linearly Homomorphic Signature Schemes..... 41
  - 4.3 Lattice-Based Linearly Homomorphic Signature Schemes ..... 42
    - 4.3.1 Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures, by Boneh and Freeman [15] ..... 43
    - 4.3.2 Lattice-Based Linearly Homomorphic Signature Scheme over Binary Fields, by Wang et al. [65] ..... 43
    - 4.3.3 Summary of Lattice-Based Linearly Homomorphic Signature Schemes ..... 43
  - 4.4 Homomorphic Signature Schemes for Polynomial Functions ..... 44
    - 4.4.1 Homomorphic Signatures for Polynomial Functions, by Boneh and Freeman [14] ..... 44

- 4.4.2 Homomorphic Signatures for Polynomial Functions with Shorter Signatures, by Hiromasa et al. [43] ..... 44
- 4.4.3 Homomorphic Signatures with Efficient Verification for Polynomial Functions, by Catalano et al. [23]..... 45
- 4.4.4 Summary of Homomorphic Signature Schemes for Polynomial Functions ..... 45
- 4.5 Fully Homomorphic Signature Schemes..... 46
  - 4.5.1 Leveled Fully Homomorphic Signatures from Standard Lattices, by Gorbunov et al. [41] ..... 46
  - 4.5.2 Adaptively Secure Fully Homomorphic Signatures Based on Lattices, by Boyen et al. [19] ..... 47
  - 4.5.3 Leveled Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures, by Wang et al. [66] ..... 47
  - 4.5.4 Summary of Fully Homomorphic Signature Schemes ..... 48
- 4.6 Multiple Sources Linearly Homomorphic Signature Schemes ..... 48
  - 4.6.1 Signatures for Multi-Source Network Coding, by Czap and Vajda [30] ..... 48
  - 4.6.2 Short Signature Scheme for Multi-Source Network Coding, by Yan et al. [69] ..... 49
  - 4.6.3 Efficient Multiple Sources Network Coding Signature in the Standard Model, by Zhang et al. [75],..... 49
  - 4.6.4 Summary of Multiple Sources Linearly Homomorphic Signature Schemes ..... 49
- 4.7 Linearly Homomorphic Aggregate Signature Schemes ..... 50
  - 4.7.1 A Homomorphic Aggregate Signature Scheme Based on Lattice, by Zhang et al. [74] ..... 50
  - 4.7.2 An Efficient Homomorphic Aggregate Signature Scheme Based on Lattice, by Jing [45] ..... 51
  - 4.7.3 Summary of Linearly Homomorphic Aggregate Signature Schemes ..... 51
- 5 Suitable Homomorphic Signature Schemes for eVoting, Smart Grids, and eHealth ..... 53**
  - 5.1 Electronic Voting ..... 53
  - 5.2 Smart Grids ..... 56
  - 5.3 Electronic Health Records ..... 57
- 6 Conclusion ..... 59**
- References ..... 61**