

# Contents

<b>1</b>	<b>From Digital to Homomorphic Signature Schemes</b>	<b>1</b>
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>	<b>11</b>
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>	<b>23</b>
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

<b>4</b>	<b>State of the Art of Homomorphic Signature Schemes</b>	<b>35</b>
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
<b>5</b>	<b>Suitable Homomorphic Signature Schemes for eVoting, Smart Grids, and eHealth .....</b>	<b>53</b>
5.1	Electronic Voting .....	53
5.2	Smart Grids .....	56
5.3	Electronic Health Records .....	57
<b>6</b>	<b>Conclusion .....</b>	<b>59</b>
	<b>References .....</b>	<b>61</b>



<http://www.springer.com/978-3-319-32114-1>

Homomorphic Signature Schemes

A Survey

Traverso, G.; Demirel, D.; Buchmann, J.

2016, XI, 64 p., Softcover

ISBN: 978-3-319-32114-1