

Contents

Part I Introduction

1	Thesis Overview	3
1.1	Motivation.	3
1.2	Thesis Statement	4
1.3	Summary of Contributions	5
1.4	Thesis Organization	6
	References	6
2	Speech Processing Background	7
2.1	Tools and Techniques.	7
2.1.1	Signal Parameterization	7
2.1.2	Gaussian Mixture Models	8
2.1.3	Hidden Markov Models	8
2.2	Speaker Identification and Verification	10
2.2.1	Modeling Speech	10
2.2.2	Model Adaptation	12
2.2.3	Supervectors with LSH.	13
2.2.4	Reconstructing Data from LSH Keys	15
2.3	Speech Recognition	16
	References	17
3	Privacy Background	19
3.1	What is Privacy?	19
3.1.1	Definitions	19
3.1.2	Related Concepts	20
3.1.3	Privacy-Preserving Applications.	21
3.1.4	Privacy-Preserving Computation in this Thesis	22

3.2	Secure Multiparty Computation	22
3.2.1	Protocol Assumptions	24
3.2.2	Adversarial Behavior	25
3.2.3	Privacy Definitions: Ideal Model and Real Model	26
3.2.4	Encryption	27
3.2.5	Masking	33
3.2.6	Zero-Knowledge Proofs and Threshold Cryptosystems	35
3.2.7	Oblivious Transfer	37
3.2.8	Related Work on SMC Protocols for Machine Learning	39
3.3	Differential Privacy	39
3.3.1	Exponential Mechanism	41
3.3.2	Related Work on Differentially Private Machine Learning	42
3.3.3	Differentially Private Speech Processing	42
	References	43

Part II Privacy-Preserving Speaker Verification

4	Overview of Speaker Verification with Privacy	49
4.1	Introduction	49
4.2	Privacy Issues and Adversarial Behavior	50
4.2.1	Imposter Imitating a User	51
4.2.2	Collusion	52
4.2.3	Information Leakage After Multiple Interactions	52
	References	53
5	Privacy-Preserving Speaker Verification Using Gaussian Mixture Models	55
5.1	System Architecture	55
5.2	Speaker Verification Protocols	57
5.2.1	Private Enrollment Protocol	58
5.2.2	Private Verification Protocols	58
5.3	Experiments	60
5.3.1	Precision	61
5.3.2	Accuracy	61
5.3.3	Execution Time	61
5.4	Conclusion	62
5.5	Supplementary Protocols	63
	References	66

6	Privacy-Preserving Speaker Verification as String Comparison	67
6.1	System Architecture	68
6.2	Protocols	69
6.3	Experiments.	70
6.3.1	Accuracy	70
6.3.2	Execution Time	71
6.4	Conclusion	72
	References	72

Part III Privacy-Preserving Speaker Identification

7	Overview of Speaker Identification with Privacy	75
7.1	Introduction.	75
7.1.1	Speech-Based Surveillance	75
7.1.2	Preliminary Step for Other Speech Processing Tasks	76
7.2	Privacy Issues and Adversarial Behavior.	77
7.2.1	Collusion	78
7.2.2	Information Leakage After Multiple Interactions	78
8	Privacy-Preserving Speaker Identification Using Gaussian Mixture Models	79
8.1	Introduction.	79
8.2	System Architecture	80
8.3	Speaker Identification Protocols.	81
8.3.1	Case 1: Client Sends Encrypted Speech Sample to the Server	81
8.3.2	Case 2: Server Sends Encrypted Speaker Models to the Client	83
8.4	Experiments.	85
8.4.1	Precision.	85
8.4.2	Accuracy	85
8.4.3	Execution Time	85
8.5	Conclusion	86
	References	86
9	Privacy-Preserving Speaker Identification as String Comparison	89
9.1	Introduction.	89
9.2	System Architecture	90

- 9.3 Protocols 91
 - 9.3.1 Oblivious Salting 91
 - 9.3.2 Speaker Identification 92
- 9.4 Experiments 93
 - 9.4.1 Accuracy 93
 - 9.4.2 Execution Time 94
- 9.5 Conclusion 95
- References 95

Part IV Privacy-Preserving Speech Recognition

- 10 Overview of Speech Recognition with Privacy 99**
 - 10.1 Introduction 99
 - 10.2 Client-Server Model for Speech Recognition 99
 - 10.3 Privacy Issues 100
 - 10.4 System Architecture 101
 - Reference 102
- 11 Privacy-Preserving Isolated-Word Recognition 103**
 - 11.1 Introduction 103
 - 11.2 Protocol for Secure Forward Algorithm 104
 - 11.2.1 Secure Logarithm Protocol 104
 - 11.2.2 Secure Exponent Protocol 104
 - 11.2.3 Secure Logsum Protocol 105
 - 11.2.4 Secure Forward Algorithm Protocol 105
 - 11.2.5 Security Analysis 106
 - 11.3 Privacy-Preserving Isolated-Word Recognition 106
 - 11.3.1 Simplified Secure Forward Algorithm 106
 - 11.3.2 Protocol for Privacy-Preserving Isolated-Word Recognition 107
 - 11.3.3 Computational Complexity 107
 - 11.3.4 Practical Issues 108
 - 11.3.5 Experiments 108
 - 11.4 Discussion 109
 - References 109

Part V Conclusion

- 12 Thesis Conclusion 113**
 - 12.1 Summary of Results 113
 - 12.2 Discussion 115

13 Future Work 117

13.1 Other Privacy-Preserving Speech Processing Tasks 117

13.1.1 Privacy Preserving Music Recognition
and Keyword Spotting 117

13.1.2 Privacy Preserving Graph Search for Continuous
Speech Recognition 118

13.2 Algorithmic Improvements 118

13.2.1 Ensemble of LSH Functions 118

13.2.2 Using Fully Homomorphic Encryption 118

References 119

Appendix: Differentially Private Gaussian Mixture Models. 121

Author Biography 141



<http://www.springer.com/978-1-4614-4638-5>

Privacy-Preserving Machine Learning for Speech
Processing

Pathak, M.A.

2013, XVIII, 142 p., Hardcover

ISBN: 978-1-4614-4638-5