

1. Introduction	1
2. Literature Review	5
2.1. PUF Definition	5
2.2. Applications of PUFs	6
2.3. Main PUF Types	8
2.3.1. Silicon and Arbiter PUFs	8
2.3.2. SRAM PUFs	8
2.3.3. Ring Oscillator PUFs	9
3. Transform Coding for Key Agreement with Correlated PUFs	13
3.1. Motivation	13
3.1.1. Summary of Contributions and Organization	14
3.2. System Model and the Fuzzy Commitment Scheme	15
3.3. Transform Coding Steps	17
3.4. Quantizer and Code Designs	18
3.4.1. Quantizer Design with Fixed Measurement Channels	19
3.4.2. Quantizer Design with Fixed Number of Errors	20
3.5. Performance Evaluations	21
3.5.1. Decorrelation Performance	21
3.5.2. Maximum Secret-key Length	22
3.5.3. Transform Complexity	23
3.5.4. Uniqueness and Security	27

3.6. Privacy and Secrecy Analysis of Proposed Error-Correction Codes	28
3.6.1. Codes for the Quantizer Design with Fixed Measurement Channels	28
3.6.2. Codes for the Quantizer Design with Fixed Number of Errors	29
4. Key Agreement with Multiple Measurements of Identifiers	33
4.1. Motivation	33
4.1.1. Models for Identifier Outputs	35
4.1.2. Summary of Contributions and Organization	35
4.2. System Models and Rate Regions	36
4.2.1. System Models	36
4.2.2. Key-leakage-storage Regions	37
4.3. Binary Identifier Measurements	38
4.3.1. Measurements Through Dependent BSCs	39
4.3.2. Mixtures of BSCs	41
4.3.3. Two Lemmas	42
4.3.4. Simplified Rate Region Characterizations	42
4.4. Model Comparisons	43
4.4.1. Hidden Source Model	43
4.4.2. Mismatched Code Design	44
4.4.3. Single Encoder and Multiple Decoder Measurements	45
4.4.4. Multiple Encoder and Decoder Measurements	47
5. Optimal Code Constructions	49
5.1. Motivation	49
5.1.1. Summary of Contributions	50
5.1.2. Organization	50
5.2. Problem Formulations	51
5.2.1. Generated-secret (GS) and Chosen-secret (CS) Models	51
5.2.2. Wyner-Ziv (WZ) Problem	52

5.2.3. Functional Equivalence	53
5.3. Prior Art and Comparisons	54
5.4. First WZ-coding Construction	55
5.4.1. Optimality of the Proposed Construction for the GS Model	58
5.4.2. Optimality of the Proposed Construction for the CS Model	59
5.5. Second WZ-coding Construction	60
5.5.1. Polar Code Construction for the GS Model	60
5.5.2. Proposed Codes for the GS Model	62
5.5.3. Code Comparisons and Discussions	63
6. Controllable Measurements for Private Authentication	67
6.1. Motivation	67
6.1.1. Summary of Contributions and Organization	68
6.2. Problem Formulations	69
6.2.1. Hidden Source, GS Model	69
6.2.2. Hidden Source, CS Model	70
6.3. Key-leakage-storage-cost Regions	71
6.3.1. Rate Region Comparisons and Discussions	72
6.4. Example	73
7. Other Contributions	79
7.1. Key Agreement with Multiple PUF Enrollments	79
7.1.1. Two-Enrollment Model with the Same Measurement Channels	80
7.1.2. Zero Secrecy Leakage for Symmetric PUFs	81
7.2. Coding for Positive Rate in the Key Agreement Problem	82
7.2.1. Literature Review	84
7.2.2. Main Results	84

A. Appendices for Chapter 4	91
A.1. Achievability Proofs	91
A.1.1. Achievability Proof for Theorem 4.1	91
A.1.2. Achievability Proof for Theorem 4.2	95
A.2. Converses	96
A.3. Cardinality Bound	98
A.4. Alternative Convexity Proof for Independent BSCs	99
A.5. On A Lower Bound for Binary Asymmetric Channels	101
B. Appendices for Chapter 5	105
B.1. Strong Secrecy	105
B.2. Extensions to Hidden Sources with Multiple Decoder Measurements	107
C. Appendices for Chapter 6	109
C.1. Proofs of Rate Regions	109
C.2. Proof for $\mathcal{R}_{gs}$	109
C.2.1. Proof of Achievability	109
C.2.2. Proof of Converse	112
C.3. Proof for $\mathcal{R}_{cs}$	115
C.3.1. Proof of Achievability	115
C.3.2. Proof of Converse	116
C.4. Proof of Theorem 6.1	118
C.4.1. Proof of Achievability	118
C.4.2. Proof of Converse	121
C.5. Proof of Theorem 6.2	122
C.5.1. Proof of Achievability	122
C.5.2. Proof of Converse	123