

Contents

List of Figures	XIII
List of Tables	XV
1 Introduction	1
1.1 Authentication in Insecure Environments	1
1.2 Overview	4
I Preliminaries	7
2 Mathematical and Cryptographic Foundation	9
2.1 Preliminaries and Notation	9
2.1.1 Functions and Algorithms	9
2.1.2 Basic Group Theory	18
2.2 Encryption Schemes	22
2.2.1 Notions of Security	27
2.2.2 Passive Attacks	28
2.2.3 Security Models	35
2.2.4 Active Attacks	45
2.2.5 Practical Security	53
2.3 Cryptographic Hardness Assumptions	58
2.3.1 The Factoring and RSA Assumption	58
2.3.2 The Discrete Logarithm and Diffie-Hellman Assumptions	61
2.4 Hash Functions and Digital Signature Schemes	67
2.4.1 Hash Functions	67
2.4.2 Digital Signature Schemes	68
2.4.3 Blind Signatures	72

.

II	Human Decipherable Encryption Schemes	79
3	Introduction, Scenario, and Related Work	81
3.1	Background and Purpose	81
3.2	Overview	84
3.3	Scenarios	85
3.4	Related Work	85
4	Human Decipherable Encryption Scheme	87
4.1	Notation and Terminology	87
4.1.1	Messages, Codings, Ciphertexts and Keys	87
4.1.2	Unicity Distance	89
4.1.3	Encodings and Decodings	95
4.1.4	Human Decipherable Encryption Scheme	103
4.1.5	XOR, EQV and Hamming Functions	117
4.2	Visual Cryptography	119
4.2.1	Pixel-based Visual Cryptography	120
4.2.2	Segment-based Visual Cryptography	124
4.2.3	Applications of Visual Cryptography	127
4.2.4	Using Key-Transparencies Multiple Times	130
5	Human Decipherable Encryption Schemes Based on Dice Codings	135
5.1	Dice Codings	135
5.1.1	Underlying Spaces and Parameters	135
5.1.2	Coding Scheme	137
5.2	Basic Version	139
5.2.1	EQV Encryption Scheme	139
5.2.2	Basic Human Decipherable Encryption Scheme	141
5.3	Security Analysis of the Basic Version	145
5.3.1	Ciphertext-Only Attacks Without Side Information	146
5.3.2	Ciphertext-Only Attacks With Side Information	149
5.3.3	Security Models	167
5.4	Dice Codings with Noise	174
5.4.1	Changes in Underlying Spaces and Parameters	174
5.4.2	EQV Encryption Scheme with Noise	175
5.4.3	Human Decipherable Encryption Scheme with Noise	178
5.5	Security Analysis of Dice Codings with Noise	183
5.5.1	Ciphertext-Only Attacks Without Side Information	184
5.5.2	Ciphertext-Only Attacks With Side Information	185
5.5.3	Security Models	192

6	Conclusion and Future Work	197
6.1	Summary and Conclusion	197
6.2	Future Work	198
6.2.1	Addressing Other Senses than Sight	198
6.2.2	Security Assumptions and Models	201
6.2.3	Methods to Improve Reusing the Key-Transparencies	202
III	Non-Transferable Anonymous Credentials	207
7	Introduction, Scenario, and Related Work	209
7.1	Background and Purpose	209
7.2	Overview	210
7.3	Scenarios	210
7.4	Related Work	211
8	Privacy and Data Security	213
8.1	Notions and Terms of Privacy	213
8.1.1	Anonymity, Pseudonymity, Unlinkability, Untraceability	213
8.1.2	Trust Levels Regarding Privacy	214
8.2	Anonymous Credentials	215
8.2.1	Properties of Anonymous Credentials	216
8.2.2	Zero-Knowledge Proofs	217
8.2.3	Wallet-With-Observer Architecture	219
8.3	Smartcards and Biometrics	220
8.3.1	Smartcards	220
8.3.2	Biometrics	221
9	Analysis of Non-Transferable Anonymous Credentials	229
9.1	Approaches Aiming at Non-Transferability	229
9.1.1	Embedding Valuable Secrets	229
9.1.2	Biometrically Enforced Non-Transferability	230
9.1.3	Consideration of Other Approaches	231
9.1.4	Security Issues	232
9.1.5	Limiting the Consequences of Security Breaches	242
9.2	Templateless Biometric-Enforced Non-Transferability	244
9.2.1	Adapting Schemes to Work without Templates	246
9.2.2	Comparison of Approaches' Security	249

10 Conclusion and Future Work	253
10.1 Summary and Conclusion	253
10.2 Future Work	254
 IV Outlook and Appendix	 257
11 Summary, Conclusion and Outlook	259
11.1 Summary	259
11.2 Conclusion	260
11.3 Outlook	261
 Example of Pixel-based Visual Cryptography in Detail	 265
 Auxiliary Tables and Proofs	 271
 Source Code Listings	 281
 Bibliography	 307
 List of Symbols and Abberviations	 349
 Index of Keywords	 353
 Index of Names	 359