

Table des matières

Avant-propos	1
David POINTCHEVAL	
Chapitre 1. Chiffrement à clé publique et notions de sécurité	5
Nuttapong ATTRAPADUNG et Takahiro MATSUDA	
1.1. Définitions de base du PKE	6
1.1.1. Notations	6
1.1.2. Chiffrement à clé publique	6
1.1.3. Sécurité IND-CPA et IND-CCA	7
1.1.4. Autres notions de sécurité basiques et assimilées	9
1.2. Schémas PKE de base	10
1.2.1. Preuves par jeux	10
1.2.2. Chiffrement ElGamal	10
1.2.3. Chiffrement CS simplifié	12
1.2.4. Chiffrement Cramer-Shoup	16
1.2.5. D'autres schémas PKE spécifiques	19
1.3. Constructions génériques pour des PKE sécurisés IND-CCA	21
1.3.1. Chiffrement hybride	22
1.3.2. Construction de Naor-Yung et extensions	24
1.3.3. Fujisaki-Okamoto et autres transformations dans le ROM	26
1.3.4. Autres constructions génériques pour PKE sécurisé IND-CCA	28
1.4. Sujets avancés	30
1.4.1. Notions intermédiaires liées au CCA	30
1.4.2. Sécurité IND-CCA dans une configuration à utilisateurs multiples et sécurité restreinte	32
1.4.3. Sécurité pour des messages dépendants de la clé	34

1.4.4. Plus d'informations sur PKE	36
1.5. Bibliographie	37
Chapitre 2. Signatures et notions de sécurité	55
Marc FISCHLIN	
2.1. Schémas de signature	55
2.1.1. Définition	55
2.1.2. Exemples de schémas pratiques	57
2.2. Infalsifiabilité	60
2.2.1. Discussion	60
2.2.2. Infalsifiabilité existentielle face à des attaques à messages choisis	62
2.2.3. Infalsifiabilité de schémas pratiques	63
2.3. Infalsifiabilité forte	65
2.3.1. Discussion	65
2.3.2. Infalsifiabilité existentielle forte face à des attaques à messages choisis	67
2.3.3. Infalsifiabilité forte de schémas pratiques	67
2.3.4. Construction de schémas fortement infalsifiable	68
2.4. Résumé	69
2.5. Bibliographie	70
Chapitre 3. Preuves à divulgation nulle de connaissance	73
Ivan VISCONTI	
3.1. Introduction	73
3.2. Notations	74
3.3. Preuves à divulgation nulle de connaissance classiques	74
3.3.1. Divulgation nulle de connaissance (<i>zero knowledge</i>)	76
3.4. Comment construire un système de preuves à divulgation nulle de connaissance	78
3.4.1. Preuves ZK pour tout $\mathcal{N}^{\mathcal{P}}$	81
3.4.2. Complexité en nombre de tours	82
3.5. Systèmes de preuves à sécurité relaxée	83
3.5.1. ZK à vérificateur honnête (<i>honest-verifier ZK</i> ou HVZK)	83
3.5.2. Dissimulation de témoin/indistinguabilité	84
3.5.3. Protocoles Σ	86
3.6. Divulgation nulle de connaissance non boîte noire	87
3.7. Notions avancées	87
3.7.1. Divulgation nulle de connaissance publiquement vérifiable	87
3.7.2. ZK concurrent et plus	89

3.7.3. ZK avec des joueurs sans état	91
3.7.4. Systèmes de preuves à entrée différée	92
3.8. Conclusion	92
3.9. Bibliographie	93

Chapitre 4. Calcul multi-parties sécurisé 99

Yehuda LINDELL

4.1. Introduction	99
4.1.1. Terminologie	101
4.2. Sécurité du MPC	101
4.2.1. Le paradigme définitionnel	101
4.2.2. Paramètres additionnels définitionnels	104
4.2.3. Implications définitionnelles importantes	106
4.3. Faisabilité du MPC	108
4.4. Techniques	109
4.4.1. Partage de secret de Shamir	109
4.4.2. MPC à majorité honnête avec partage de secret	110
4.4.3. Intersection d'ensembles privés	112
4.4.4. Cryptographie à seuil	114
4.4.5. MPC à majorité malhonnête	115
4.4.6. MPC pratique et efficace	115
4.5. Cas d'usage du MPC	116
4.5.1. Le fossé salarial de Boston	116
4.5.2. La conversion publicitaire	117
4.5.3. Le MPC pour la protection de clés cryptographiques (<i>unbound security, seipior, curv</i>)	117
4.5.4. Collaboration gouvernementale (<i>sharemind</i>)	117
4.5.5. Analytiques préservant la confidentialité (<i>duality</i>)	118
4.6. Discussion	118
4.7. Bibliographie	119

Chapitre 5. Cryptographie à base de couplages 123

Olivier BLAZY

5.1. Introduction	124
5.1.1. Notations	124
5.1.2. Généralités	124
5.2. Un petit pas pour l'homme, un pas de géant pour la cryptographie	125
5.2.1. Ouvrir la boîte de Pandore, éclaircir le mystère	126
5.2.2. Un nouveau monde d'hypothèses	128

5.3. Un nouveau monde de protocoles cryptographiques au bout des doigts	133
5.3.1. Chiffrement basé sur l'identité	133
5.3.2. Signature compacte efficace déterministe	134
5.4. Bibliographie	135

Chapitre 6. Diffusion chiffrée et traçage de traîtres 139

Duong HIEU PHAN

6.1. Introduction	139
6.2. Notions de sécurité pour la diffusion chiffrée et le traçage de traîtres	141
6.3. Vue d'ensemble de la diffusion chiffrée et du traçage de traîtres	143
6.4. Méthodes à base d'arbres	147
6.5. TT à base de codes	151
6.6. Schémas algébriques	154
6.7. Approche par réseaux avec une sécurité <i>post-quantum</i>	162
6.8. Bibliographie	164

Chapitre 7. Chiffrement par attributs 173

Romain GAY

7.1. Introduction	173
7.2. Groupes de couplage	174
7.2.1. Groupes cycliques	174
7.2.2. Groupes avec couplage	175
7.3. Encodage de prédicat	175
7.3.1. Définition	175
7.3.2. Constructions	176
7.4. Chiffrement par attributs	179
7.4.1. Définition	179
7.4.2. Construction modulaire	180
7.5. Bibliographie	188

Chapitre 8. Signatures avancées 191

Olivier SANDERS

8.1. Introduction	191
8.2. Quelques constructions	193
8.2.1. Le cas des messages entiers	193
8.2.2. Le cas des messages non entiers	196
8.3. Applications	197

8.3.1. Accréditations anonymes	198
8.3.2. Signatures de groupe	201
8.3.3. Attestations directes anonymes	205
8.4. Bibliographie	209

Chapitre 9. Échange de clé 213

Colin BOYD

9.1. Fondamentaux des échanges de clé	213
9.1.1. Parties d'échange de clé	214
9.1.2. Messages d'échange de clé	215
9.1.3. Fonctions de dérivation de clé	216
9.2. Échange de clé non authentifié	218
9.2.1. Définition formelle et modèles de sécurité	218
9.2.2. Constructions et exemples	219
9.3. Échange de clé authentifié	221
9.3.1. Échange de clé non interactif	221
9.3.2. Modèles de sécurité AKE	223
9.3.3. Constructions et exemples	228
9.4. Conclusion	235
9.5. Bibliographie	235

Chapitre 10. Échange de clé authentifié par mot de passe : protocoles et modèles de sécurité 241

Stanislaw JARECKI

10.1. Introduction	241
10.2. Premier PAKE : EKE	244
10.3. Modèle par jeu pour la sécurité du PAKE	246
10.3.1. Le modèle de sécurité BPR	247
10.3.2. Authentification implicite et authentification explicite	250
10.3.3. Limites du modèle BPR	251
10.3.4. EKE instancié avec un KE de Diffie-Hellman	252
10.3.5. Implémenter le chiffré idéal sur des groupes arbitraires	253
10.4. Sécurité PAKE avec un modèle par simulation	255
10.4.1. Le modèle de sécurité BMP	255
10.4.2. Avantages de la définition BMP : mots de passe arbitraires, sécurité stricte	259
10.4.3. EKE utilisant un chiffrement à masque jetable dérivé du RO	260
10.4.4. Modèle BMP pour PAKE avec authentification explicite (PAKE-EA)	261

10.5. Modèle de sécurité PAKE universellement composable	262
10.6. Protocoles PAKE dans le modèle standard	267
10.7. Optimisations d'efficacité du PAKE	271
10.8. PAKE asymétrique : PAKE dans une configuration client-serveur . .	274
10.9. PAKE à seuil	276
10.10. Bibliographie	278

Chapitre 11. Calculs vérifiables et arguments succincts pour NP . . 291

Dario FIORE

11.1. Introduction	291
11.1.1. Contexte	292
11.2. Préliminaires	294
11.3. Calcul vérifiable	294
11.4. Construction de VC	296
11.4.1. VC pour des circuits en trois étapes	296
11.4.2. Arguments succincts non interactifs pour calculs non déterministes	297
11.4.3. Calcul vérifiable à partir de SNARG	298
11.5. Construction modulaire de SNARG	299
11.5.1. Preuves algébriques linéaires non interactives	300
11.5.2. Groupes bilinéaires	302
11.5.3. SNARG à partir de NILP algébrique avec des vérificateurs de degré 2 utilisant des groupes bilinéaires	304
11.6. Construction de NILP algébrique pour des circuits arithmétiques . . .	306
11.6.1. Circuits arithmétiques	306
11.6.2. Programmes arithmétiques quadratiques	307
11.6.3. NILP algébrique pour QAP	309
11.7. Conclusion	314
11.8. Bibliographie	315

Liste des auteurs 317

Index 319