

Spis treści

Rozdział 1

Kryptografia – 11

- 1.1. Wczesna historia – 11
- 1.2. Systemy kryptograficzne z kluczem publicznym – 13
 - 1.2.1. Zadania dla kryptografii z kluczem publicznym – 15
 - 1.2.2. Szyfrowanie przypadkowe – 16
- 1.3. Kryptosystem RSA – 16
 - 1.3.1. Szyfrowanie – 16
 - 1.3.2. Funkcje skrótu – 17
 - 1.3.3. Podpis – 18
- 1.4. Schemat Diffiego–Hellmana i DSA – 19
 - 1.4.1. Wymiana kluczy – 19
 - 1.4.2. Algorytm DSA – 20
- 1.5. Dzielenie sekretów, rzut monetą i czas spędzony nad zadaniem domowym – 22
 - 1.5.1. Dzielenie sekretów – 22
 - 1.5.2. Zobowiązanie bitowe – 22
 - 1.5.3. Ukrywanie informacji – 23
- 1.6. Hasła, podpisy i szyfry – 24
- 1.7. Kryptosystemy praktyczne i niepraktyczne, ale użyteczne – 26
 - 1.7.1. Kryteria praktyczności kryptosystemu – 26
 - 1.7.2. „Niewytłumaczalna efektywność” teorii – 28
 - 1.7.3. Potrzeba kryptografii niepraktycznej – 29

Rozdział 2

Złożoność obliczeniowa – 32

- 2.1. Notacja wielkie- O – 32
- 2.2. Długość liczb – 37
- 2.3. Szacowanie czasu – 40
 - 2.3.1. Operacje bitowe – 40
 - 2.3.2. Algorytmy – 42

- 2.3.3. Algorytm Euklidesa – 44
- 2.3.4. Od czasu wielomianowego do czasu wykładniczego – 46
- 2.4. Klasy P, NP i NP-zupełność – 51
- 2.4.1. Problemy poszukiwawcze i decyzyjne – 51
- 2.4.2. Klasy P i NP – 55
- 2.4.3. Redukowalność jednego problemu do innego – 57
- 2.4.4. Problemy NP-zupełne – 59
- 2.5. Problemy z obietnicą – 63
- 2.5.1. Problem złamania – 63
- 2.5.2. Problem zapadki – 64
- 2.6. Algorytmy probabilistyczne a klasy złożoności – 65
- 2.6.1. Przykład – 65
- 2.6.2. Klasa złożoności RP – 66
- 2.6.3. Klasa złożoności BPP – 67
- 2.7. Niektóre inne klasy złożoności – 69
- 2.7.1. Hierarchia wielomianowa – 69
- 2.7.2. Klasa UP – 70
- 2.7.3. Przeciętny czas – 70
- 2.7.4. Oddziaływanie – 71
- 2.7.5. Obliczenia równoległe i nonuniformizacja – 72

Rozdział 3

Algebra – 75

- 3.1. Ciała – 75
- 3.2. Ciała skończone – 78
- 3.2.1. Generatory multiplikatywne ciał skończonych – 79
- 3.2.2. Istnienie i jedyność ciał skończonych – 81
- 3.2.3. Bezpośrednia konstrukcja – 83
- 3.3. Algorytm Euklidesa dla wielomianów – 88
- 3.4. Pierścienie wielomianów – 90
- 3.4.1. Podstawowe definicje – 90
- 3.4.2. Twierdzenie Hilberta o bazie – 92
- 3.4.3. Homomorfizmy i elementy przestępne – 93
- 3.4.4. Twierdzenie Hilberta o zerach – 94
- 3.5. Bazy Gröbnera – 97
- 3.5.1. Porządek wyrazów – 98
- 3.5.2. Dzielenie wielomianów – 99
- 3.5.3. Bazy Gröbnera ideału I – 101
- 3.5.4. Zredukowane bazy Gröbnera – 105

Rozdział 4

Kryptosystemy niejawnie jednomianowe – 109

- 4.1. System Imaiego–Matsumota – 109
- 4.1.1. System – 109
- 4.1.2. Kryptoanaliza Patarina – 113

- 4.2. „Mały smok” Patarina – 117
 - 4.2.1. System – 117
 - 4.2.2. Nieudana kryptoanaliza – 119
 - 4.2.3. Słabe wykładniki dla $q = 2$ – 121
 - 4.2.4. „Mały smok” papierowym tygrysem: kryptoanaliza Copersmitha i Patarina – 122
- 4.3. Systemy, które mogą okazać się bezpieczniejsze – 127
 - 4.3.1. „Wielki smok” – 127
 - 4.3.2. Dwustopniowy szyfr kwadratowy – 129
 - 4.3.3. Podpisy – 132

Rozdział 5

Kryptosystemy kombinatoryczno-algebraiczne – 136

- 5.1. Historia – 136
- 5.2. Nieadekwatność twierdzenia Brassarda – 137
- 5.3. Konkretnie systemy kombinatoryczno-algebraiczne – 139
 - 5.3.1. „Polly Cracker” – 139
 - 5.3.2. Specjalne przypadki szyfru „Polly Cracker” wynikające ze znanych problemów kombinatorycznych – 140
 - 5.3.3. Uogólnienia szyfru „Polly Cracker” – 142
- 5.4. Podstawowy problem algebraiczny – 146
- 5.5. Kryptograficzna wersja problemu przynależności do ideału – 147
- 5.6. Ataki oparte na algebrze liniowej – 148
- 5.7. Projektowanie bezpiecznego systemu – 150

Rozdział 6

Kryptosystemy eliptyczne i hipereliptyczne – 153

- 6.1. Krzywe eliptyczne – 154
 - 6.1.1. Równanie – 154
 - 6.1.2. Reguła dodawania – 155
 - 6.1.3. Współrzędne rzutowe – 158
 - 6.1.4. Krzywe eliptyczne nad \mathbb{C} – 159
 - 6.1.5. Krzywe eliptyczne nad \mathbb{Q} – 161
 - 6.1.6. Charakterystyki 2 i 3 – 162
 - 6.1.7. Krzywe eliptyczne nad ciałami skończonymi – 163
 - 6.1.8. Pierwiastki kwadratowe – 166
- 6.2. Kryptosystemy używające krzywych eliptycznych – 170
 - 6.2.1. Historia – 170
 - 6.2.2. Wymiana kluczy i przesyłanie wiadomości – 171
 - 6.2.3. Algorytm logarytmu dyskretnego w grupach gładkiego rzędu – 173
 - 6.2.4. Podpis cyfrowy – 175
- 6.3. Analogi klasycznych problemów teorii liczb w teorii krzywych eliptycznych – 177
 - 6.3.1. Ustalamy „globalną” krzywą eliptyczną i zmieniamy liczbę pierwszą – 178
 - 6.3.2. Ustalamy krzywą eliptyczną nad małym ciałem \mathbb{F}_q , a następnie rozważamy ją nad \mathbb{F}_{q^r} dla różnych r – 179

- 6.3.3. Ustalamy ciało \mathbb{F}_q i zmieniamy współczynniki – 179
- 6.4. Tło kulturowe: hipotezy dotyczące krzywych eliptycznych i ich nieoczekiwane związki z innymi problemami – 180
 - 6.4.1. Liczby kongruentne – 180
 - 6.4.2. Wielkie twierdzenie Fermata – 181
 - 6.4.3. Hipoteza Bircha i Swinnertona-Dyera – 182
 - 6.4.4. Rozkład Sato–Tate’a – 183
 - 6.4.5. Powrót do kryptografii: Dlaczego nikt nie wie, jak znaleźć „bazę rozkładu” – 184
- 6.5. Krzywe hipereliptyczne – 185
 - 6.5.1. Definicje – 185
 - 6.5.2. Dodawanie w jacobianie – 187
 - 6.5.3. Funkcja dzeta – 189
- 6.6. Kryptosystemy hipereliptyczne – 191
 - 6.6.1. Przykłady w charakterystyce 2 – 192
 - 6.6.2. Przykład nad dużym ciałem prostym – 193
 - 6.6.3. Zadania na przyszłość – 197

Dodatek

Elementarny wstęp do krzywych hipereliptycznych – 199

(Autorzy: *Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato*)

- D.1. Podstawowe definicje i własności – 200
- D.2. Funkcje wielomianowe i wymierne – 203
- D.3. Zera i bieguny – 207
- D.4. Dywizory – 213
- D.5. Reprezentacja dywizorów półzredukowanych – 215
- D.6. Dywizory zredukowane – 218
- D.7. Dodawanie dywizorów zredukowanych – 220

Odpowiedzi do ćwiczeń – 228

Bibliografia – 245

Skorowidz – 254