# Index


## A

account generation 197, 199-205
additive encryption function 48-49, 71-72, 85-87, 125-127, 150, 158, 160-162, 200, 215
advanced encryption technoligies 2
alias 148
alias management 148-150, 199
anonymity 1
anonymous action systems 186-190, 216
anonymous authentication mechanisms 134
anonymous channel 112, 114, 116-120, 122, 243
anonymous memory 194-199, 201-207, 213-216
anonymous monitoring systems 194-195
anonymous object delivery 194-195
anonymous tag 53, 88-89, 154, 177
anonymous token 84
auction buyer 187, 192-193
auctioneer 187

## B

bit strings 9
blind calculations 48
blind signature 51
blind sum 124-126
Bulletin boards (BBs) 20, 35

## C

challenge and response protocols 93
check code (CC) 31
check value (CV) 31
cloud computing 4
coefficient matrix calculations 28
common password 136
communication mechanisms 2
concealing pattern (CP) 112
confirmation numbers (CNs) 65, 226
CP Generator 112-119, 122
credentials 136, 150
credit card system transaction 158
  account balancing 158, 160, 167-169, 182
  initial transaction 158-159, 164
  registration 149-150, 158-159, 163, 169, 175, 189, 195, 197-198, 208
  state recovery 158, 168
  token acquisition 158-159, 163, 228, 233
  transaction 28, 32, 34-35, 49, 55-56, 69, 125, 140-141, 150, 156-175, 183, 189, 198, 201, 204, 206
Crowds 104
cut and choose protocol 93, 95

## D

Data Encryption Standard (DES) 15
DC-net 104
decryption algorithms 8
denial of service (DOS) 3
digital signatures 20-21, 24, 69
dishonest operations 157
dummy elements 28, 30, 72, 76, 127, 130

## E

electronic cash (e-cash) 3
electronic governance 1, 4, 219
electronic payment (e-payment) 156
electronic poll (e-poll) 219
electronic procurement (e-procurement) 185
electronic signals 220
electronic voting systems 4
ElGamal encryption algorithm 18
encryption algorithms 7-10, 12-13, 15-17, 19, 23, 34, 36-37, 39, 41, 43-44, 51, 56-57, 61, 65-68, 84, 97, 107-109, 112, 115, 161, 175, 189, 198, 208-209, 223, 227, 231, 236-237
  asymmetric key encryption 12-13
  symmetric key encryption 12

English auction schemes 186
Enhanced Symmetric key Encryption Based Mix-Net (ESEBM) 101, 112
e-voting systems 219-220, 226
accuracy and verifiability 221
dispute-freeness 222, 226, 239-240
fairness 216, 221, 223-226, 236, 239-240
incoercibility 221-222, 226, 239-240, 242
practicality 222, 227, 240
privacy 3, 5, 11, 35, 50, 52-53, 65-67, 69, 71, 74-76, 82-83, 85, 91, 98-99, 123, 132, 135, 143, 151, 153, 156, 160, 181, 183, 186, 194-198, 216, 218-223, 225-226, 236, 238, 240
receipt-freeness 222, 225-226, 239-240
robustness 222, 226, 240
scalability 222, 227, 240
extended next tokens 80-81, 159

## G

group authentication mechanisms 137

## H

Hamming code 21
hash function 21-24, 94, 96
hidden vote 222, 224-226
hidden voter 222-226
hidden voter with hidden vote schemes 222, 225-226
homomorphic anonymous token 85
homomorphic encryption functions 11, 49

## I

ID based mechanisms 136
identities (IDs) 134
Implicit Transaction Links (ITLs) 32
ITL based anonymous authentication mechanism 139-140, 142, 207

## L

Lagrange interpolation formula 130
limiting expenditures of clients 170
linear equation based encryption function 73, 126, 128, 162, 166, 170
linear equations 19, 26-31, 33-34, 44, 48-49, 71-73, 76, 86, 126, 128, 140, 143, 158, 160, 162-163, 166, 170, 198, 200
LU-decomposition method 30

## M

MACs (Message Authentication Codes) 20-21
memory acquisition 197, 200-202, 204-205
memory manager 195
access control 195
accounting 195
error detection 21, 32, 195
memory access 195, 197, 201-207
message forgeries 3
Mix-net 106
multi party computation schemes 124-125
mutually anonymous communication channel 122

## N

non-dummy elements 30
non-interactive zero knowledge proof (NIZKP) 96

## O

offline credit card systems 175
of Rivest, Shamir and Adelman (RSA) 15
onetime pad 13
onion routing 121
open token scheme 82-85, 138, 140-141, 149, 159, 163, 169, 189, 234

## P

password leaks 146
password protection 146-147
permutation operation 14
plain text attacks 14, 27, 44, 73, 78, 113, 126, 128, 144, 163, 171
probabilistic encryption algorithms 10
public encryption key 16, 18, 23, 41, 64, 88-89, 107-108, 131, 144, 223-225

## R

receiver anonymous communication channel 104, 122
receivers 1, 14, 101-102, 209, 217
re-decryption 10
re-encryption 10
relay servers 102
remote payments 157
Reply Messages in ESEBM 120
re-signing mechanisms 24

## S

secret decryption key 16, 18, 23, 42, 44, 84, 86, 89, 97, 113, 121, 128, 142, 161, 210, 224-225, 227
senders 102
servers 102
signature pair 52, 65, 68
signing key 23, 51, 53, 56-57, 62, 66-67, 70, 83-85, 90, 94-95, 111, 137, 141, 151, 153, 165, 177, 200, 227, 233
stealing password 146
substitution operation 14

## T

tags 88
tallying managers 227
tamper resistnat memories 157
temporally unlinkable signature scheme 61
token invalidation mechanism 142
token issuing mechanism 139
token refreshing 142
tokens 28, 34-35, 50, 55-56, 69-87, 90-95, 97, 99, 135-143, 145-146, 149-151, 153-155, 158-165, 167, 169-170, 175, 177, 182-183, 189-192, 197, 199-200, 202, 205-206, 211, 213, 227, 229-231, 233-235, 239
transaction records 157-158, 160-162, 164, 183

## U

unlinkable signature schemes 51

## V

verifiability 60
verification key 23, 51, 56-58, 70-71, 85, 90-91, 165, 180, 227, 233
Vickrey auction schemes 186
voting manager (VM) 227, 229, 231, 233-234, 236

## W

wire-tappers 102

## Z

zero knowledge proof (ZKP) 50, 95, 99