Index

account, 189
account-based issuing protocol, 189
account-less issuing protocol, 190
ACES, 4, 13, 18, 25
active attack, 46
adaptively chosen formula attack, 96
adaptively chosen message attack, 79
addition chain, 51, 56
adversary, 46
algorithm, 42
    adversary, 46
    attacker, 45
        active, 46
        infinitely powerful, 46, 92, 215–216
        passive, 46
    black-box, 45, 48
    honest, 45
    interactive, 44
    simulator, 68, 87, 100, 205
anonymity, 11, 31, 34, 190
anonymous
    account, 190, 209, 216
    attribute recertification, 34, 145, 209
    certificate issuing
        drawbacks of, 190, 209
    channel, 265–266
    extortioner, 17, 230, 245, 251
    issuing of smartcard, 252–253
    refreshing of attributes, 190
    updating of attributes, 34, 191, 212, 216
anonymous channel, 265–266
anonymous registration
    drawbacks of, 26
atomic formula, 119
attack
    active, 46
    adversary, 46
    fake-terminal, 224
    model, 45–48
    on digital signatures, 78–79
        adaptively chosen message attack, 79
        existential forgery, 79
        forgery from scratch, 79
        key-only attack, 79
        total break, 79
    passive, 46
attacker, 45
    active, 46
    infinitely powerful, 46, 92, 215–216
    passive, 46
attribute, 9
attribute certificate, 9–13
    privacy dangers of, 20–25
    recertification of, 34, 145, 209
    refreshing of, 190
    SPKI, 12, 22, 27
    SPKI/SDSI 2.0, 15

Tokeneer, 12, 19
updating of, 34, 191, 212, 216

batch-verification, 82, 85, 126, 128, 201
blind signatures, 27, 78, 81, 83, 208
drawbacks of, 28, 227
restrictive, 131–179
security in random oracle model, 81
technique of Okamoto and Ohta, 81, 83, 86
blinding-invariant, 33, 132

C-SET, 18
central database paradigm, 6
drawbacks of, 6–9
certificate
attribute, *see* attribute certificate
digital, *see* digital certificate
identity, *see* identity certificate
paper-based, 1, 208, 253
Certificate Authority, 3
certificate issuing protocol, 32
restrictive blind, 131–179
certificate showing protocol, 33
with selective disclosure, 27, 31, 35, 91–130
certified key pair, 86
extortion of, 17, 145, 230, 245, 251
certified public key, 86
challenge
of the verifier, 71
self-chosen, 120, 128
semantics, 247
Chaum-Pedersen signatures, 175
chipcard, 6
collision-intractable function, 58–59
commitment
function, 50, 58, 61, 65, 76, 91
opening a, 50, 61, 65
common coin flips, 230, 244, 245
drawbacks of preventing, 230
completeness, 67
composition of protocols, 46, 69
computation error channel, 221, 243
computing device
software-only, 15, 225
tamper-resistant
iButton, 18
smartcard, *see* smartcard
correction factor, 202–204
correlation-intractable function, 84
credential, 11, 28, 228
credit report accuracy, 8
CRL, 13, 17, 23, 209, 210, 250, 253
drawbacks of, 14
cryptographic action, 88
cryptographic coprocessor, 248
performance of, 248
cyberspace, 2
systematical monitoring of, 21

data leakage
computation error channel, 221, 243
Faraday Cage, 192, 226
halting channel, 221, 244
physical broadcast channel, 221
piggyback channel, 221, 227
subliminal channel, 37, 221, 227
inflow, 222, 239–240
outflow, 222, 240–242
timing channel, 221, 244
van Eck effect, 24, 221, 226
delta-CRL, 13
designated-verifier proof, 191
Diffie-Hellman problem, 164
digital bearer certificate, 208, 253
digital certificate, 3, 86–89
attribute, 9–13
bearer, 208, 253
discarding, 2, 17, 26, 213
extortion, 17, 230, 245, 251

  identity, 3–5
  issuing protocol, 32
    account-based, 189
    account-less, 190
    restrictive blind, 131–179
  lending, 211–212
    remote, 251–252
  limited-show, 13, 35, 197–208
    overruling of, 208
  long-lived, 14, 190
  one-show, 197–207
    dynamic, 201–207
    static, 197–201
  personal, 16, 26, 208, 211
  privacy dangers of, 20–25
  pseudonymous, 25, 26
  public-key, 86
  returning a, 250–251
  revocation of, 13–15, 17, 20, 23
  secret-key, 34, 87–89
  short-lived, 13, 15, 19, 38, 190
  showing protocol, 33
    with selective disclosure, 27, 31, 35, 91–130
  unlimited-show, 35, 208, 234
  validation, 13, 190
digital pseudonym, 35, 189, 209
digital signature, 77–86
  blind, *see* blind signatures
  Chaum-Pedersen, 175
  DSA, 171, 236, 249
  elliptic curve DSA, 175
  Guillou-Quisquater, 85
  of the Fiat-Shamir type
    in random oracle model, 80
  restrictive blind, 131–179
  RSA, 87
  Schnorr, 83
  signed proof, 80
  unforgeability of, 77
discarding certificates, 2, 17, 26, 213
distance bounding, 252, 255
DL function, 51–56
DL-representation, 59
  proving knowledge of, 71–75
  trivial, 59
DLREP function, 59–62, 90
  compared to RSAREP function, 65–66
  proof of knowledge for, 71–75
drawbacks
  of anonymous certificate issuing, 190, 209
  of anonymous registration, 26
  of blind signatures, 28, 227
  of central database paradigm, 6–9
  of certificate revocation, 14
  of computational privacy, 39
  of designated-verifier proofs, 192
  of identity certificates, 10, 20–25, 31
  of key escrow, 262–266
  of preventing common coin flips, 230
  of privacy legislation, 257–259
  of self-regulation, 259–262
  of smartcard-only setting, 219–224
DSA, 171, 236, 249
  elliptic curve variant, 175
DSig, 12

ECDSA, 175
Echelon, 21
Enfopol, 21
European Privacy Directive, 25n
exact security, 48
extortion attack, 17, 230, 245, 251
  protection against, 145, 265

factoring problem, 55, 57
fake-terminal attack, 224
Faraday Cage, 192, 226

Fiat-Shamir type proof of knowledge, 79
forgery from scratch, 79
formula
  atomic, 119
  status of, 96
Fortezza, 4, 18
FPKI, 4, 24, 270
function, 42
  collision-intractable, 58–59
  commitment, 50, 58, 61, 65, 76, 91
  correlation-intractable, 84
  DL, 51
  DLREP, 59–62
  idealized, 49
  infinite collection, 49
    index set for, 49
  instance generator for, 49
    invulnerable, 50
  negligible, 43
  non-negligible, 43
  one-way, 49–58
    sufficiently strong, 84
  overwhelming, 43
  RSA, 56–58
  RSAREP, 62–65

generic description (of protocol), 71, 98, 113, 115, 202
group of prime order, 51–53
  elliptic curve construction, 53
  subgroup construction, 51
Guillou-Quisquater proof of knowledge, 76
Guillou-Quisquater signatures, 85

halting channel, 221, 244
handheld device
  PDA, 226
honest algorithm, 45
honest-verifier zero-knowledge, 68

iButton, 18n
ICE, 21
idealized function, 49
identifier, 3
identity certificate, 3–5
  PGP, 5, 14, 18, 26
  privacy dangers of, 20–25
  SDSI 1.0, 12, 22, 26
  X.509, 3, 210
    ACES, 4, 13, 18, 25
    C-SET, 18
    Fortezza, 4, 18
    FPKI, 4, 24, 270
    PEM, 4
    PKIX, 4, 13
    S/MIME, 4
    SET, 4, 18, 27, 248
identity fraud, 9, 10, 31
immunization, 162–171
index set, 49
indistinguishable
  computationally, 44
  perfectly, 43
  statistically, 43
inflow, 222, 239–240
infomediaries, 261
initial witness, 71
  master, 205
  set, 120
instance generator, 49
  invulnerable, 50
    for the DL function, 51–54
    for the DLREP function, 60–61
    for the RSA function, 56–57
    for the RSAREP function, 63–65
interactive algorithm, 44
Internet Archive, 21
interval proof, 129–130
intractable problem, 43
invulnerable instance generator, 50

issuing protocol, 32
  account-based, 189
  account-less, 190
  restrictive blind, 131–179

key escrow, 262–266
  electronic cash, 264
  electronic voting, 263
  encryption, 264
key pair, 66
  certified, 86
key set-up, 66, 70
key-only attack, 79
knowledge extractor, 67, 95, 111

language, 43
  computationally indistinguishable, 44
  perfectly indistinguishable, 43
  statistically indistinguishable, 43
lending of certificate, 211–212
  remote, 251–252
limited-show certificate, 13, 35, 197–208
  overruling of, 208
linkability, 26, 30, 35, 189, 190, 212, 253
long-lived certificate, 14, 190
long-term security, 201, 207
low-cost smartcards, 225, 248–250

metric of authentication, 5
move, 44

national ID card, 25
negligible function, 43
non-negligible function, 43
non-negligible uncertainty, 73
non-repudiation, 26, 189, 212–213
normalized form, 63

OCSP, 13
OECD Policy Guidelines, 25n
one-show certificate, 197–207
  dynamic, 201–207
  static, 197–201
one-time public key, 200
one-way function, 49–58
online certificate validation, 13
  drawbacks of, 14
  OCSP, 13
OpenCard Framework, 225
OPS, 12, 27
  privacy dangers of, 27
outflow, 222, 240–242
overwhelming function, 43
overwhelming probability, 43

P3P, 12, 21, 27
  privacy dangers of, 27
paper-based certificate, 1, 208, 253
passive attack, 46
PC/SC Workgroup, 225
PDA, 226
PEM, 4
perfect crime, 230
personal certificate, 16, 26, 208, 211
PGP, 5, 14, 18, 26
physical broadcast channel, 221
piggyback channel, 221, 227
PKI, 3
PKIX, 4, 13
  Jonah implementation of, 4
PolicyMaker, 11
polylogarithmic running time, 80n
privacy
  dangers, *see* privacy dangers
  definition of, 20, 262
  European Privacy Directive, 25n
  legislation, 257–259
  OECD Policy Guidelines, 25n
  pragmatist, 31
  ways to protect, 257–271
privacy dangers
  of central databases, 7–9

of digital certificates, 20–25
of key escrow, 262–266
of OPS/P3P, 27
of self-regulation, 259–262
of smartcards, 24, 219–223
privacy-enhancing technologies (benefits), 266–268
probability
negligible, 43
non-negligible, 43
overwhelming, 43
proof of knowledge, 66–71
completeness, 67
convert into digital signature, 79–81
designated-verifier, 191
Guillou-Quisquater, 76
knowledge extractor, 67, 95, 111
of the Fiat-Shamir type, 79
Schnorr, 73
signed, 80
soundness, 67
witness-hiding, 69
witness-indistinguishable, 68–69
zero-knowledge, 68
honest-verifier, 68
protocol, 44
accepting view, 45
arbitrary composition of, 46, 69
certificate issuing, 32, 131–179
certificate showing, 33, 37, 91–130
generic description of, 71, 98, 113, 115, 202
immunization, 162–171
move, 44
round, 44
transcript, 45
verification relation, 44
view, 45
witness-indistinguishable, 68–69
zero-knowledge, 68
honest-verifier, 68
pseudonymous certificates, 25, 26
drawbacks of, 26
PEM, 4
PGP, 26
SDSI, 12, 22, 26
X.509v3, 26
pseudorandom generator, 249
public key, 66
one-time, 200
self-certified, 88
public key infrastructure, 3
public-key certificate scheme, 86

random oracle model, 49, 50, 58, 80, 84
REFEREE, 12
refreshing a certificate, 190
remote lending, 251–252
repeated squaring, 51, 56
reputation, 7, 8, 26, 189, 211
restrictive blinding, 131–179
returning a certificate, 250–251
revocation, 13–15, 17, 20, 23, 38
CRL, 13, 17, 23, 209, 210, 250, 253
delta-CRL, 13
drawbacks of, 14
online validation, 13
round, 44
RSA
function, 56–58
signature scheme, 87
RSA-representation, 63
proving knowledge of, 75–76
trivial, 63
RSAREP function, 62–65
compared to DLREP function, 65–66
proof of knowledge for, 75–76
running time, 43
polylogarithmic, 80n

superpolynomial, 43n

S/MIME, 4
Schnorr proof of knowledge, 73
Schnorr signature scheme, 83
SDSI, 12, 22, 26
secret key, 66
secret-key certificate scheme, 87
  delegation strategy in, 185–189
  simulator in, 87
security
  long-term, 201, 207
  parameter, 42
  reduction, 48–49
    exact, 48
    optimal tightness, 48
    overhead factor, 48
    tight, 48
self-certified public key, 88
self-regulation, 259–262
SET, 4, 18, 27, 248
  C-SET, 18
short-lived certificate, 13, 15, 19, 38, 190
showing protocol, 33
  t out of u, 128
  adaptively chosen formula attack, 96
  Boolean formula, 119–128
  interval enclosure, 129–130
  linear inequality, 108–119
  linear relation, 93–108
  polynomial relation, 129
  with selective disclosure, 27, 31, 35, 91–130
signed message, 77
signed proof, 80, 102
  unforgeability of, 77
  unmodifiability of, 101
simulator
  in secret-key certificates, 87
  in zero-knowledge proofs, 68, 100
simultaneous repeated squaring, 62, 63
Smart Cards for Windows, 225
smartcard, 15–19, 38, 219–255
  anonymous issuing of, 252–253
  low-cost, 225, 248–250
  non-privacy dangers of, 19, 223–224
  physical attacks, 29, 228, 253
  privacy dangers of, 24, 219–223
  security advantages of, 16–18
  Smart Cards for Windows, 225
  standardization
    OpenCard Framework, 225
    PC/SC Workgroup, 225
  tamper-resistance, 223, 228
  with cryptographic coprocessor, 248
    performance of, 248
smartcard-only paradigm
  drawbacks of, 219–224
software-only computing device, 15, 225
soundness (of proof of knowledge), 67
SPKI, 12, 22, 27
SPKI/SDSI 2.0, 15
status (of a formula), 96
subliminal channel, 37, 221, 227
  inflow, 222, 239–240
  outflow, 222, 240–242
sufficiently strong one-way function, 84
superpolynomial running time, 43n
surveillance, 20
system parameters, 66
  properly formed, 54, 57, 70

tamper-resistant computing device, 16–18, 220, 221
  iButton, 18
  smartcard, *see* smartcard
timing channel, 221, 244
TLS, 12

Tokeneer, 12, 19
traceability, 28, 31, 226, 228, 253
transcript (of protocol), 45
trust management system
  PolicyMaker, 11
  REFEREE, 12

uncertainty (non-negligible), 73
unforgeability of signature scheme, 77
unlimited-show certificate, 35, 208, 234
unlinkability, 26, 30, 31, 189, 190, 212, 253
  self-revocable, 266
unmodifiability (of signed proof), 101
untraceability, 28, 31, 226, 228, 253
  self-revocable, 266
updating a certificate, 191

van Eck effect, 24, 221, 226
vector addition chain, 62
verification relation, 44
  compound, 82, 205–207
view, 45
  accepting, 45
  aggregate, 47

witness
  extractor, 69
  initial, 71
witness-hiding proof of knowledge, 69
witness-indistinguishable protocol, 68–69

X.500, 4, 210
X.501, 9
X.509, 3, 210
  ACES, 4, 13, 18, 25
  extensions, 12
  Fortezza, 4, 18
  FPKI, 4, 24, 270
  PEM, 4
  PKIX, 4, 13
  S/MIME, 4
  SET, 4, 18, 27, 248
    C-SET, 18
  version 1, 4, 13
  version 2, 4, 13
  version 3, 4, 10, 12, 13, 210
X9, 7
  X9.55, 4
  X9.57, 12

zero-knowledge, 68
  honest-verifier, 68
  simulator, 68, 100
zeroization, 16