Glossary

Access control [7] The procedures and functions put in place to restrict access to specific objects or resources

Access control policy [7] A formal specification of the rules governing who is given what kind of access (and under which circumstances) to each protected resource

Access structure [7] When multiple parties need to work together to obtain a resource, an access structure describes who needs to cooperate with whom, and how, in order to access the resource (in **ABE**, the "parties" are attributes)

Accuracy/correctness of a data set [6] A measure indicating whether the data in a data set can be relied upon to be true (as opposed to error-ridden or deliberately falsified)

Anonymity [3] Other entities are unable to determine the identity (i.e., the "real name") of the party that is associated with a particular action or piece of data (see **anonymity set**)

Anonymity set [6] A set of entities that potentially have the same attributes. Thus, **anonymity** means that a given entity is not identifiable (or distinguishable) within a particular anonymity set

Anonymous credential [6] A specific type of **credential system**

Anonymous remailer [3] A PET for sending anonymous e-mail (originally proposed in 1988)

APEX [8] Architecture for Privacy Enforcement using XML (a PET for privacy enforcement proposed in 2006)

APPEL [8] A P3P Preference Exchange Language (an XML encoding for user preferences in P3P environments, proposed in 2002)

The following is a glossary of terms and acronyms used in this book. A number in brackets (e.g. "[3]") is a reference to the chapter in which the term is first used.

C. Adams, *Introduction to Privacy Enhancing Technologies*,
https://doi.org/10.1007/978-3-030-81043-6

Application proxy [3] A service that sits between protected and unprotected networks (an application sends a request to the proxy and the proxy creates its own request and sends it to the recipient; the response is sent to the proxy which then creates its own response and sends it to the application) so that senders and receivers never interact directly and all messages can be completely inspected

Attribute-based encryption (ABE) [7] A type of public key cryptography in which specified attributes are required in order to decrypt the ciphertext into its corresponding plaintext

Authenticated channel [8] A communications channel in which the receiver of a message knows the identity of the sender of that message. The channel has integrity (the message cannot be modified in transit by an adversary), but it may not provide confidentiality

AWGN [7] Additive White Gaussian Noise

Background knowledge attack [6] A security attack in which the adversary has some prior knowledge (or auxiliary knowledge) about the target of his/her attack, which can make the attack more effective

Black-box setting [9] Knowing, or having access to, only the input-output functionality of a system, application, or environment (see also **white-box setting**)

Broadcast channel [8] A communications channel in which a message is sent from one sender simultaneously to multiple receivers

CAPTCHA [3] Completely Automated Public Turing test to tell Computers and Humans Apart (a challenge-response test initiated by a website in order to determine whether the entity visiting the website is a human or a piece of software)

CP-ABE [7] Ciphertext-Policy Attribute-Based Encryption (the **access structure** is specified in the ciphertext, and the private key is a set of attributes)

Composability property [7] Multiple **differentially private** mechanisms can be composed (i.e., used sequentially or in parallel) to create a combined mechanism with a guaranteed level of $\boldsymbol{\varepsilon}$**-differential privacy**

Contextual integrity [2] A theory of privacy in which the "contexts" are social domains (such as health, finance, family, political framework, etc.) and an assessment of the appropriateness of information flow considers the data subject, the sender, the recipient, the type of data, and the transmission principle (consented, coerced, stolen, buying, selling, national security, and so on)

Credential system [6] A PET for minimizing information disclosure in online transactions (proposed in 2000)

Dark web [3] A part of the Internet that is not indexed by traditional search engines and that requires special software, configuration, or authorization to access

Data minimization [2] The practice of limiting the collection of personal information to that which is directly relevant and necessary for accomplishing a specified purpose

Data perturbation [8] The practice of adding "noise" (i.e., random values) to a database so that individual record values cannot be relied upon (because they are incorrect), although aggregate values such as "average" may still be correct

DDoS [9] Distributed Denial of Service

Deep Neural Network [9] An artificial neural network with multiple layers between the input and output layers

Digital credential [6] A specific type of **credential system**

Disclosure [2] The simultaneous acquisition of both the attribute of a user and the identity of that user, by an unintended party

DNS [3] Domain Name Server

DPIA [9] Data Protection Impact Assessment

EEA [8] European Economic Area

Entry funnel [3] The node in an **onion routing network** that takes data from the sender's **application proxy** and **onion proxy**, and passes it to the first of several **onion routers**

ε-**Differential Privacy [7]** A PET for database privacy proposed in 2006

EU [8] European Union

Exit funnel [3] The node in an **onion routing network** that takes data from the sequence of **onion routers**, and passes it to the receiver's **onion proxy** and **application proxy**

Exposure [2] The simultaneous acquisition of both the action of a user and the identity of that user, by an unintended party

FTP [3] File Transfer Protocol

Garbled circuit [7] A way to "encrypt a computation" such that the output of the computation is revealed, but no information about the inputs or intermediate values is revealed (a garbled circuit is sometimes referred to as a *scrambled circuit*)

GDPR [8] General Data Protection Regulation (a regulation in EU law on data protection and privacy in the **EU** and the **EEA**)

Guard node [3] A specific **onion router** (perhaps one of a very small fixed set of **onion routers**) that will be used as the first **onion router** for Alice's messages (the remaining **onion routers** in her **onion routing network** may be freely chosen). The guard node must satisfy certain criteria in order to minimize the risk of compromise (and, therefore, the risk of anonymity loss for Alice)

HDB [8] Hippocratic database (a PET for database privacy proposed in 2002)

Hidden services [3] Services that can only be accessed through Tor (they are invisible to ordinary Web browsers and search engines)

Homogeneity attack [6] In a set of records having identical **quasi-identifiers**, if the value of the sensitive attribute is always the same, then observers will be able to deduce the value of the sensitive attribute for anyone whose record they know is in that set

HTML [8] Hypertext Markup Language

HTTP, HTTPS [3] Hypertext Transfer Protocol; HTTP over SSL

IACR [7] International Association for Cryptologic Research

Identifier [6] Information (such as a *social security number*) that distinguishes one entity from all others in a set of entities (also referred to as a *unique identifier*)

IETF [4] Internet Engineering Task Force (an international body responsible for the creation and development of Internet standards)

IM [5] Instant Messaging

Inference attack [6] An attacker infers information that he or she should not know, given only information that he or she is allowed to know

IP [3], IPv4, IPv6 [4] Internet Protocol (a communications protocol for transmitting datagrams (packets of data) across networks; the first major version of IP is known as "Internet Protocol Version 4" (IPv4) and its successor is known as "Internet Protocol Version 6" (IPv6))

IPsec protocol [4] IP security protocol (a protocol for protecting IP packets transmitted between devices; it can be operated either in **transport mode** or in **tunnel mode**)

IRC [3] Internet Relay Chat

Issuing protocol [6] An interaction between a user and a Certification Authority (CA) which results in the CA digitally signing a **credential** for the user

***k*-Anonymity [6]** A PET for database privacy proposed in 1998

KP-ABE [7] Key-Policy Attribute-Based Encryption (the **access structure** is specified in the private key and the ciphertext is a set of attributes)

LAN [5] Local Area Network

MAC address [9] Media access control address (a unique identifier assigned to a network interface controller for use as a network address)

Mix network [3] A PET for untraceable e-mail proposed in 1981

ML [9] Machine learning

MPC [7] Multi-party computation (a PET that allows multiple entities to jointly compute a function without any party seeing the private inputs of any other party; MPC was proposed in 1986)

MTD [9] Moving target defense (dynamically and constantly changing network configuration in order to increase the difficulty of reconnaissance and intrusion by an attacker)

NFS [3] Network File System

NIST [9] National Institute of Standards and Technology, an agency of the US Department of Commerce whose mission is to promote innovation and industrial competitiveness (in part through standardization of various technologies)

Nonce [11] A contraction for "number used once" (for example, in an authentication protocol, Alice may send to Bob a random number that has not been used before and will not be used again; when Bob returns a signature on this nonce, Alice will be convinced that she is in a live session with Bob)

NNTP [3] Network news transfer protocol (the protocol used to connect to Usenet servers and to transfer newsgroup articles between systems)

OECD [8] Organization for Economic Co-operation and Development

OCSP [4] Online Certificate Status Protocol (a protocol to check the current revocation status of a public key certificate)

Onion proxy [3] The node in an **onion routing network** that receives data from the sender's **application proxy** and prepares it for transmission through the network, or that receives data from the network and prepares it for reception by the receiver's **application proxy**

Onion router [3] A node in an **onion routing network** that receives a message, decrypts the outer layer to reveal the next node, and forwards the internal portion to that next node

Onion routing network [3] A PET for anonymous real-time communications, proposed in 1996

Operation tuple [2] The pair (*identity*, *action*) that causes **exposure** if known by an unintended party

OTR [5] Off-the-Record messaging protocol (a PET for private messaging in **IM** environments, proposed in 2004)

Output perturbation [6] The practice of adding "noise" (i.e., random values) to query responses from a database so that the correct response values cannot be learned

P3P [8] Platform for Privacy Preferences Project (a PET for creating **privacy policies** proposed in 2002)

P3P policy [8] A **privacy policy** that conforms to the **P3P** specification

PDP [8] Policy Decision Point (in the **XACML** processing model, the PDP is the component that renders an **access control** decision (i.e., "permit" or "deny"))

PEP [8] Policy Enforcement Point (in the **XACML** processing model, the PEP is the component that enforces an **access control** decision which has been made by the **PDP**)

PET, PETs [1] Privacy Enhancing Technology; Privacy Enhancing Technologies

PGP [5] Pretty Good Privacy (a format and protocol for adding encryption and digital signatures to e-mail messages)

PIN [6] Personal Identification Number

PIR [4] Private information retrieval (a PET for database privacy proposed in 1995)

Point-to-point network [8] A network in which there are only two communicating nodes (thus they communicate only with each other)

Policy reference file [8] A statement about what **P3P policy** applies to any given **URI** within a website

Privacy Bird [8] A **P3P** user agent (proposed in 2006)

Privacy level of a data set [6] The maximum probability of re-identification for individuals in the data set

Privacy policy [1] A collection of rules specifying who is allowed to access what data, and what they can do with this data once they have it

Privacy seal program [8] An independent (3rd-party) audit and review of an organization's website and data processing practices in order to assess the organization's website safety and compliance with their publicized **privacy policy**

Private set intersection [7] an example of **MPC** (in which two parties determine whether they have elements in common from their respective private sets)

Property of an attribute [6] information about an attribute that does not reveal its actual value (for example, if the attribute is an integer, a property might be that the attribute is "greater than x", or "less than y", or "in the range $[x, y]$")

Pseudonym [3] An **identifier** of a party that is not one of the party's "real names"

Pseudonymity [3] The use of pseudonyms as **identifiers**

PSTN [9] Public Switched Telephone Network

Quasi-identifier [6] Attributes (which are not themselves unique **identifiers**) that can be grouped together (possibly with other external information) to re-identify a specific individual

Query restriction [8] Disallowing specific queries, or specific types of queries, from some or all users

RBAC [7] Role-Based Access Control (a form of **access control** in which privileges are assigned to roles (such as "manager" or "system administrator") rather than to individual names/identities)

Record tuple [2] The pair (*identity*, *attribute*) that causes **disclosure** if known by an unintended party

RFC [4] Request for Comments (an **IETF** standards-track specification)

SDN [9] Software Defined Networking (an approach to network management that enables dynamic network configuration)

S/MIME [5] Secure Multipurpose Internet Mail Extensions (a standardized format and protocol for adding encryption and digital signatures to e-mail messages)

Sensitivity of a function [7] The sensitivity of a database query function A is the amount that A will change if a particular person's data is removed from the database (*global sensitivity* is the maximum possible change, when all individual records are taken into consideration)

Showing protocol [6] An interaction between two entities Alice and Bob in which Alice proves ownership of some attributes in her **credential** to Bob (while hiding all remaining attributes). If the **credential** can only be used in one showing protocol, it is called *single-show*; if it can be used in many showing protocols without diminishing Alice's privacy, it is called *multi-show*

SMTP [3] Simple Mail Transfer Protocol (a standardized communication protocol for e-mail transmission)

Social engineering [1] The art of exploiting social means, rather than technical hacking procedures, to gain access to buildings, systems, or data. In the context of information security, it generally refers to the psychological manipulation of people into performing actions or divulging confidential information (such as a password) that will be of benefit to an attacker

Social sorting [1] The partition of raw data about people into various categories, based on separators such as income, education, race, occupation, social status, geographic residence, and so on

SOCKS protocol [3] Socket service protocol (an Internet protocol that exchanges packets between a client and a server through a proxy server)

SSH [3] Secure Shell (a protocol for operating network services securely over an unsecured network)

SSL [4] Secure Sockets Layer (a protocol to provide communications security over a network; a modified version of SSL was standardized as **TLS**)

Synchronous network [7] A network in which all communications connections are synchronized to a shared clock

TCP [3] Transmission Control Protocol (a connection-oriented service that is typically implemented on top of **IP** in the Internet communications protocol stack)

TLS [4] Transport Layer Security (a protocol to provide communications security over a network; this standardized protocol was based on the earlier **SSL** protocol)

Tor [3] The onion routing (a specific implementation of the **onion routing network**, developed in 2002)

Traffic analysis [3] The process of intercepting and examining messages on a network in order to deduce information from communication patterns

Transport mode [4] A mode of operation for the **IPsec protocol** in which only the packet body is protected (the packet header information is left in the clear)

Tunnel mode [4] A mode of operation for the **IPsec protocol** in which both the packet body and the packet header information are protected

UDP [4] User datagram protocol (a connectionless service that is typically implemented on top of **IP** in the Internet communications protocol stack)

URL Uniform Resource Locator (a reference to a Web resource that specifies its location on a network and a mechanism for retrieving it)

URI [8] Uniform Resource Identifier (a globally unique sequence of characters that identifies a physical or logical resource on a network)

Utility of a data set [6] A measure of how useful a set of data is for achieving a given purpose

VPN [3] Virtual Private Network (a protocol to create a private network connection across a public network connection)

W3C [8] World Wide Web Consortium (an international body responsible for the creation and development of Web standards)

Website fingerprinting [3] The process of collecting sufficient features, information, and traffic from a website to be able to uniquely distinguish it from other websites

White-box setting [9] Knowing, or having access to, the internal structures, workings, and documentation of a system, application, or environment (see also **black-box setting**)

WSDL [8] Web Services Description Language (an **XML**-based language that is used for describing the functionality offered by a Web service)

XACML [8] eXtensible Access Control Markup Language (a human- and machine-readable language for writing **access control policies**)

XACML policy [8] An **access control policy** that conforms to the **XACML** specification

XML [8] eXtensible Markup Language (a text format to enable and facilitate data exchange on the Web)

XSLT [8] eXtensible Stylesheet Language Transformation (a language for transforming XML documents into other XML documents)

Index

A
ABE, *see* Attribute-Based Encryption (ABE)
Acceptable suppression threshold, 114
Access control policy, 145, 190–192, 252
Access controls, 78, 109, 144, 145, 149, 150, 176–178, 190, 214, 221, 223, 231
Access structures, 145–150, 170
Action analysis, 33
Actions, 2, 5, 25, 29, 32–35, 39, 52, 64, 69, 75, 79, 81, 82, 89, 95, 96, 98, 99, 105, 110, 183, 190, 192, 203, 210–212, 215, 219, 221, 228, 229, 232–235
Active enforcement system, 181
Additive white Gaussian noise (AWGN), 160
Adjustment factors, 147
Advanced Encryption Standard (AES), 42, 73, 100, 144, 195, 246
Adversary, Adversary model
  active (*see* Malicious)
  byzantine, 259, 262
  covert, 155
  fail-stop, 155, 259, 262
  honest-but-curious, 259, 262
  malicious, 155, 259
  man-in-the-middle, 259
  passive, 47, 62, 155, 258, 260
  semi-honest, 155
AES, *see* Advanced Encryption Standard (AES)
After-the-fact protection, 216
After-the-fact recourse, 215, 216
AI algorithms, 9
AKE, *see* Authenticated Key Exchange (AKE)
Alert protocol, 71
Anon.penet.fi, 49–51, 228
Anonym, 212
Anonymity, 22, 27, 28, 44, 45, 47, 49–53, 56, 58–65, 106, 110, 113, 120, 228
Anonymity set, 111, 118, 137, 139, 228
Anonymity/pseudonymity, 218, 219
Anonymizer architectures, 24
Anonymous
  connections, 33, 54, 55, 57, 58, 60, 61
  credential (*see* Credential system) (*see* Digital credential)
  E-voting protocol, 218
  payment mechanism, 218
  remailers, 39, 49–54, 63, 228
Anti-adware, 212
Anti-spyware, 212, 213, 221
Antivirus, 213, 221, 223
APEX, *see* Architecture for Privacy Enforcement using XML (APEX)
Application data protocol, 71
Application protocol, 71
Application proxy, 55–58
Approximate differential privacy, 165
Approximation algorithms, 120
A P3P Preference Exchange Language (APPEL), 178, 185, 187, 189, 194, 195
Architecture for Privacy Enforcement using XML (APEX), 110, 175, 189–196, 203, 229
Artificial intelligence (AI), 8, 10, 219
Asymmetric
  algorithms, 251, 260
  ciphers, 248, 249, 260
  encryption algorithms, 42, 248, 256
  (public key) algorithm, 245
Attacker models, 63, 88, 258, 259, 262, 265

C. Adams, *Introduction to Privacy Enhancing Technologies*,
https://doi.org/10.1007/978-3-030-81043-6

Attackers, 41, 42, 47, 48, 51, 52, 56, 60–62, 75, 76, 89, 102, 104, 118, 135, 137, 148, 166, 167, 220, 221, 233, 258–260, 262, 263
Attacks targeting a specific user, 63
Attribute auditing center (AAC), 149
Attribute values, 110, 113, 116, 117, 125, 126, 128–133, 135–138, 143, 147, 148, 150, 196, 202, 204, 229
Attribute-Based Encryption (ABE), 143–146, 148, 169, 171, 251
See also CP-ABE, KP-ABE
Attributes, 3, 25, 29, 33–35, 39, 72, 79, 110–121, 125, 131–137, 139, 144–151, 170, 175–177, 179, 185, 186, 191, 196–205, 210, 212, 213, 215, 216, 219, 221, 228, 229, 231, 251, 255
Audit log information, 145
Audit trail, 177
Auditing framework, 179
Auditing system, 180
Authenticated encryption (AE), 258
Authenticated encryption ciphers, 73
Authenticated key exchange (AKE), 101–103, 258
Authentication, 54, 70, 71, 75, 76, 78–80, 100–102, 104, 231, 242, 243, 254–256, 258
Authentication Header (AH), 76–80
Authentication protocol, 255
Authentication technique, 255, 256
Authenticity, 71, 75, 99, 100, 243, 244, 255–258
Authorized users, 177, 178
Automated profiling, 9, 10
Autonomous systems (ASes), 62
AWGN, *see* Additive White Gaussian Noise (AWGN)

B
Background knowledge attacks, 116, 117, 119
Bandwidth, 45, 48, 61, 63–65
Bandwidth allocation mechanism, 63
Batch issuing protocol, *see* Showing protocol
Bidirectional anonymity, 59
Big-O notation, 261
See also Little-O notation
Bilinear maps, 264
Bilinear pairing-based cryptography, 148
Bilinear pairings, 264, 265
Black-box setting, 220, 221
See also White-box setting
Blind digital signatures, 257
Blinding factors, 131, 257
Blind signatures, 123–125, 138, 257
Block ciphers, 246, 258
Broadcast channel, 156, 251
Broadcast encryption, 145, 251
Border Gateway Protocol (BGP), 62
Byzantine
failures, 88
robust PIR, 87

C
CA, *see* Certification Authority (CA)
CAPTCHAs, 62
Cascades, 42–45, 47, 48, 64
Cell-level access control, 179
Certificate management, 250, 252
Certificates, 71, 72, 75, 121–123, 126, 144, 233, 247, 250, 251, 256
Certification Authority (CA), 100, 122, 123, 125, 126, 128–136, 250–252, 256
ChaCha20, 245
ChaCha20 stream cipher, 73
Chaining, 51
Challenge-response authentication, 242
Challenge-response protocol, 123
Change Cipher Spec messages, 72, 73
Change Cipher Spec protocol, 71
Checksum, 253
Chief Privacy Officers, 2, 21
Cipher block chaining (CBC), 73, 78, 246
Cipher suite, 71, 72
CipherSpec, 71–73
Ciphertext Policy Attribute-Based Encryption (CP-ABE), 143, 144, 146, 148–150, 169–171, 229, 251
See also Attribute-Based Encryption
See also KP-ABE
Ciphertexts, 40–44, 96, 143–146, 148–150, 153, 169–171, 193, 229, 244, 245, 247, 248, 250–252, 256, 257, 259, 260, 263, 265
Circuit scheduling, 63
Classification, vii, 22, 24, 25, 27, 28, 30–33, 35–37, 62, 213, 214, 216
See also Privacy tree
Classification of PETs, *see* Privacy tree
Classification for privacy, *see* Privacy tree
Classification summary, *see* Privacy tree
Client authentication, 71
Client hello, 72–74
Client-server interaction, 71, 78, 81
Coding theory, 85, 160
Colluding servers, 88

Collusion resistance, 251
Commitments, 123–128, 132, 133, 138, 198, 201, 263
  See also Pedersen commitment
Communications confidentiality, 70
Communications privacy, 109, 110
Communications protocol stack, 57, 81, 89
Compact policies, 186
Compliance auditing mechanism, 181
Composability property of differential privacy, 164
Composition
  concurrent, 156
  modular, 156
  sequential, 156, 167
  universal composability, 156
Computational
  complexity theory, 260–262
  Diffie-Hellman (CDH) assumption (*see* Decisional Diffie-Hellman (DDH) assumption)
  privacy (*see* Information-theoretic privacy)
  Security (*see* Information-theoretic security)
Computational privacy, 83, 86, 88, 262
Computational security, 262
Computationally binding, *see* Computationally hiding, *see* Unconditionally binding, *see* Unconditionally hiding
Computationally hiding, *see* Computationally binding, *see* Unconditionally binding, *see* Unconditionally hiding
Computationally-bounded, 83, 89, 132
Computationally-bounded attacker, 40, 167, 262
Computationally secure PIR (C-PIR), 86, 87, 89, 90
Computationally-unbounded, 263
Confidentiality, 25, 27, 40, 50, 70, 71, 75, 78, 79, 89, 101, 103, 104, 149, 151, 243–253, 255, 258, 260
Congestion control, 58, 63
Consented sharing, 176
Constant pool, 46
Consumer privacy, 23
Contextual integrity, 26, 29
Cookies, 5, 13, 194, 223, 233
Correctness, viii, 115, 151, 153, 155, 163, 170, 177
Corruption strategies
  adaptive, 155, 167
  proactive, 155
  static, 155
Cover traffic, 58
Covering codes, 84, 85
CP-ABE, *see* Ciphertext Policy Attribute-Based Encryption (CP-ABE), *see* KP-ABE
C-PIR, *see* Computationally secure PIR (C-PIR)
Credential, 121
Credential systems, 110, 120–123, 132, 135–139, 175, 196–203, 228
  See also Anonymous credential
  See also Digital Credential
Credential transfer, 132
  See also Lending problem
Cryptanalysis, 56, 241, 258
Cryptanalysts, 242, 244, 258
Cryptographic
  algorithms, 36, 64, 71–73, 76, 77, 144, 150, 156, 158, 241–244, 254, 256, 258, 260, 262–265
  authentication, 54, 79
  confidentiality, 70, 71, 89, 103, 243, 244, 255, 258
  hash function, 73, 78, 100, 254, 260, 263, 264
  hashes, 73, 118, 119, 256
  key, 72, 73, 78, 103, 136, 144, 152, 193, 242–244, 254, 256, 257, 264
  properties, 64, 89, 103, 243, 254
  protocols, 36, 70, 76, 89, 101, 103–105, 127, 136, 150, 153, 156, 158, 241–243, 258, 262–265
  strengths, 118, 243, 244, 258, 260–263
  techniques, 36, 40, 72, 123, 127, 136, 156, 241, 242, 256
Cryptography, vii, 27, 36, 40, 42, 54, 57, 104, 241, 242, 249, 252, 253, 263, 265
Cryptology, 241, 242
Curse of dimensionality, 119
Cut-and-choose paradigm, 156
Cypherpunk remailers, 51

D
Data
  at rest, 109
  data origin authenticity, 255
  generalizations, 112–114, 119, 138, 180
  holder, 25, 32, 33, 212, 216, 221
  in motion, 109
  minimization, 27–29
  mining, 5, 6, 120
  origin authentication, 243
  ownership, 3, 7, 18, 149, 234
  perturbation, 176

Data (*cont.*)
privacies, 2, 3, 5, 13, 15, 17, 18, 25, 27–29, 35, 39, 81, 86, 89, 105, 106, 111, 113, 114, 116, 118, 139, 143, 145, 149, 164, 168–170, 175, 176, 179, 181, 184, 188, 190, 192, 195, 196, 203, 215, 218, 222, 224, 229, 230, 234, 236
Protection Impact Assessment (DPIA), 220
purging, 176
randomization, 213
subjects, 25, 26
Data Encryption Standard (DES), 42, 78, 246
Database privacy, 176, 179
Data-link protocol, 71
DBDH, *see* Decisional Bilinear Diffie-Hellman assumption (DBDH)
DDH, *see* Decisional Diffie-Hellman (DDH) assumption
DDoS attacks, 217
Deanonymize users, 62
Decipher, 244
Decisional Bilinear Diffie-Hellman assumption (DBDH), 148, 265
Decisional Diffie-Hellman (DDH) assumption, 264
Decryption, 41, 54, 57, 99, 104, 132, 144, 145, 147–149, 157, 170, 244–246, 248–250, 252, 256, 260
Decryption algorithms, 54, 244, 245, 248
Decryption operations, 54, 145, 149, 256, 260
Deep neural networks, 220
Defense-in-depth, 231, 235
De-identifying data, 213
Delegatable anonymous credentials, 257
Delegation, 255
Deniability, 27, 99, 101–105
DES, *see* Data Encryption Standard (DES)
ε-differential privacy, 16, 110, 143, 158–169, 171, 182, 222, 229
Differential privacy (DP), 165–168
ε-differentially private, 159
Diffie-Hellman (D-H) key exchange protocol, 100
Diffie-Hellman key agreement, 72
Diffie-Hellman protocol, 247, 250
Digital
cash, 242
Credential (*see* Anonymous credential) (*see* Credential system)
digital currency, 257
Signature (*see* RSA digital signature)
trail, 21
Digital credentials, 121–123, 125–128, 130–133, 136, 139, 196, 201–203, 218, 229, 257
Digital signature algorithm (DSA), 124, 248, 256, 257
Digital Signature Standard (DSS), 257
Digital vehicle forensics, 12
Dimensions of DP
background knowledge, 166
computational power, 167
formalism change, 166, 167
neighbourhood definition, 166
quantification of privacy loss, 166
relativization of knowledge gain, 167
variation of privacy loss, 166
Directory servers, 51, 58
Disclosure-reducing transformation, 35
Disclosures, 25, 34, 35, 39, 110, 118, 143, 145, 151, 158, 177, 179–181, 184, 188, 195, 196, 210, 213, 215, 216, 221, 228, 229
Distinct l-diversity, 116
DOI, *see* Internet IP Security Domain of Interpretation for ISAKMP
Domain generalization hierarchy, 114
DP, *see* Differential privacy (DP)
DSA public key, 126
Dummy traffic, 48, 51, 222
Dynamic pool, 46

E
Earth Mover's Distance (EMD), 117
Eavesdropper, *see* Unintended observer
Electronic elections, 242
Electronic mail, 22, 39, 40
Elliptic curve groups, 148, 263
E-mail, 40, 44, 49–55, 59, 63, 78, 81, 96, 104, 132, 193, 250, 252
Encapsulating Security Payload (ESP), 76–80
Encipher, 244
Encryption, 15, 28, 64, 71, 99, 109, 176, 211, 229, 248
encryption algorithms, 40, 56, 57, 73, 78, 100, 244–252, 260
Encryption operation, 256
End-point authentication, 70
End-to-end integrity checking, 59
Entropy l-diversity, 116–118
Entry funnel, 55
Entry guard selection, 61
Entry node, 55, 60
Ephemeral, 58, 73, 102, 247
Ephemeral key, 247
ESP, *see* Encapsulating Security Payload (ESP)
Exit funnel, 55

Exit nodes, 60
Exploit tools, 2
Exposure, 25, 34, 35, 39, 70, 77, 81, 98, 110, 210, 215, 221, 228
Exposure privacy, 76, 81, 211, 215
Exposure-reducing transformation, 35
EXtensible Access Control Markup Language (XACML), 190–194
EXtensible Markup Language (XML), 182–184, 186, 187, 190, 191
EXtensible Stylesheet Language Transformation (XSLT), 190–194
Extensions and variants of differential privacy, 166
Extensions for PIR, 87
External observers, 15, 40–42, 89, 116, 118, 137, 143, 196
External recipients, 177

F
Facebook Messenger, 103
Fair Information Practices, 23
Fairness, 151, 156
Fingerprints, 13, 102, 132, 253
Firewalls, 78, 81, 96–98, 191, 213, 221, 223, 231, 233, 252
Free route, 45
Fuzzy-IBE, *see* Policy-Based Encryption

G
Gaim, 102
  See also Pidgin
Garbled circuit, 152–154, 170
  See also Scrambled circuit
Garbled gate, *see* Scrambled circuit
Gaussian distributions, 160–162
General communications security protocols, 82
General Data Protection Regulation (GDPR), 195, 196, 220
General database security mechanism, 176
General security mechanism, 144
Generalizations, 26, 113–115, 119, 121, 144, 154, 165, 180, 199
Generic group model, 148
  See also Standard model
Global sensitivity, 164, 169
GTK + AOL Instant Messenger (gaim), *see* Pidgin
Guaranteed output delivery, 151, 156
Guard nodes, 60, 62

H
Handshake protocol, 71, 72, 75
Hash functions, 73, 78, 100, 126, 254, 256, 260, 263, 264
Hash-based message authentication code (HMAC), 78, 100, 254
HDB, *see* Hippocratic databases (HDB)
Health data, 110, 111
Helper nodes, 60
Heuristic, 120, 138, 139
Hidden services, 59, 63
Hide the revealed attributes, 196
Hiding
  the actions, 36, 39, 64, 69–90, 95, 98, 105, 109, 203, 228
  the attributes, 36, 39, 105, 109, 110, 118, 143–171, 175, 179, 196, 203, 212, 221, 228, 229
  the identities, 36, 39–65, 69, 74, 82, 98, 99, 109–139, 143, 151, 170, 175, 179, 196, 203, 228, 229
  the identity-action linkage, 105
  the identity-action pair, 36, 95–106
  the identity-attribute linkage, 105, 110
  the identity-attribute pair, 36, 175–205
Hippocratic databases (HDB), 175–182, 196, 203, 205, 229
HMAC, *see* Hash-based Message Authentication Code (HMAC)
Holder, 4, 25, 33, 35, 210, 211, 213, 215–217, 221
Homogeneity attacks, 116, 117, 119
Homomorphic encryption, 252
Homomorphic encryption algorithms, 86
Hop-by-hop, 46
Host-to-host communications, 97
Host-to-network communications, 97
Human profiling, 7, 9, 16

I
IBE, *see* Identity-Based Encryption (IBE)
Identifiable individual, 30
Identification, 25, 45, 137, 243
Identifiers, 41, 79, 121–123, 135, 136, 242, 250
Identity
  certificates, 121, 144, 252
  misbinding, 102
  mixer (idemix), 122
  theft, 7, 8, 16
Identity-Based Encryption (IBE), 144, 192, 251, 252
  See also Policy-Based Encryption

IETF, *see* Internet Engineering Task Force (IETF)
IETF Network Working Group, 70
IKE, *see* Internet Key Exchange
IKEv1, *see* Internet Key Exchange
IKEv2, *see* Internet Key Exchange
Internet Key ExchangeIND-CCA, *see* Indistinguishability of encryptions
IND-CCA2, *see* Indistinguishability of encryptions
IND-CPA, *see* Indistinguishability of encryptions
Independence of inputs, 151
ε-indistinguishability, 159
Indistinguishability of encryptions, 265
Induced throttling attacks, 63
Inference control techniques, 213, 221
Inference controls, 221
Information
  aggregation, 23, 26, 34
  collection, 6, 23, 28, 33, 34, 76, 145, 176, 178, 216, 221
  dissemination, 8, 26, 221
  monitoring, 5, 12, 23
  personalization, 23
  privacies, 1–4, 7, 12, 13, 23–26, 29–33, 35, 36, 39, 64, 74, 86–89, 115, 117, 118, 120, 135, 148, 151, 158, 160, 163, 166, 167, 176–179, 181, 185, 187, 189, 193, 195, 211–213, 215, 216, 220, 221, 227, 230, 233, 243, 258
  storage, 23, 192, 233
  theoretic privacy (*see* Computational privacy)
  theoretic security (*see* Computational security)
  theoretically hidden, 83
  theoretically secure PIR, 89, 90
  transfers, 23, 81, 259
Information Theoretically secure PIR, 86–89
Information-theoretic privacy, 83, 86, 263
Information-theoretic security, 131, 135, 137, 156, 158, 263
Input-output correspondence, 40
Instance hiding problem, 86
Instant messaging, 61, 98, 99, 105
Instant messaging clients, 104
Integrity, 23, 26, 29, 70, 71, 75, 78, 79, 89, 96, 105, 243, 244, 253–256, 258
Integrity mechanism, 70, 243
Integrity protection, 78
Intended recipients, 25, 33, 35, 43, 47, 50, 55, 64, 75, 82, 89, 95, 99, 120, 137, 196, 212, 213, 215, 218
Intended targets, 33, 69, 211, 215
Internet
  Engineering Task Force (IETF), 70, 74, 80
  IP Security Domain of Interpretation for ISAKMP, 79
  Key Exchange (IKE), 76, 79, 80
  protocols, 70, 75, 79, 80, 98
  Security Association and Key Management Protocol (ISAKMP), 79, 80
Internet IP Security Domain of Interpretation for ISAKMP, 79
Internet Key Exchange, 76, 79
Internet Protocol (IP)
  layer, 57, 77, 89
  network, 57
  Security Working Group, 76, 80
Interrogation, 3, 25
Intersection attack, 41
Intractable, 265
Intrusion detection, 213, 221, 223, 231
IP, *see* Internet Protocol (IP)
IPsec, 64, 69, 76–82, 89, 95–98, 105, 211, 218, 219, 228
IPsec Maintenance and Extensions (IPsecME), 80
IPsec-v2, 76–80, 89
IPsec-v2 Architecture document, 97
IPsec-v3, 77, 80, 89, 97
ISAKMP, *see* Internet Security Association and Key Management Protocol (ISAKMP)
Issuing protocol, 125, 130, 131, 133, 134, 136, 138, 201
  See also Showing protocol
IT-PIR, *see* Information Theoretically secure PIR (IT-PIR)

K

K-anonymity, 105, 110–120, 137–139, 180, 213, 228
K-anonymity requirement, 112
Key
  agreements, 72, 73, 136, 246
  blocks, 73, 149, 254
  derivation, 246
  derivation function (KDF), 152, 153, 246, 249
  distribution problem, 40, 246
  establishment, 79, 246, 258
  exchanges, 72, 73, 77, 79, 80, 89, 99, 102, 103, 242, 246, 259
  generation center (KGC), 149
  pairs, 44, 45, 75, 125, 152, 193, 245, 249, 250
  partitioning, 73, 247

Policy Attribute-Based Encryption (*see* CP-ABE)
rotation, 51
stream, 245
Key policy attribute-based encryption (KP-ABE), 145, 251
K-minimal generalization, 114, 115
KP-ABE, *see* Key Policy Attribute-Based Encryption (KP-ABE)

L
Laplacian distribution, 163, 165
Latency, 45, 52, 53, 64, 65
L-diversity, 115–119, 138
Leaky-pipe circuit, 58
Legal infrastructure, 189, 204, 209, 214–217, 223, 229
Lending problem, 132
See also Credential transfer
Limiting disclosure, 36, 105, 109–139, 143–171, 175–205, 221, 228
Limiting exposure, 36, 39–65, 69–90, 95–106, 109, 110, 203
Link padding, 58
Little-O notation, *see* Big-O notation
Load balancing, 61
Loss of confidentiality, 41
Lower-latency mix network, 53
Low-latency anonymity network, 62

M
MAC, *see* Message Authentication Code
MAC algorithm, *see* Message Authentication Code
Machine learning (ML), 9, 167, 217, 219–224, 229
Malleable, 134, 135, 257
Malleable signatures, 134, 135, 257
Malware, 15, 99, 137, 253
Man-in-the-Middle (MITM), 76, 258, 259
Man-in-the-Middle (MITM) attack, 102
Marker attacks, 56
Master key, 148, 149, 246
Master secret, 73, 133
Maximum likelihood estimator (MLE), 165
MD5, 73, 78, 254
Membership inference attacks, 220, 221, 223
Mental poker, 151
Message
authentication code (MAC), 78, 100–102, 254, 255
fragmentation, 102
protection technologies, 98
tracing, 41, 45
Message Authentication Code (MAC), 71, 72, 78, 101, 102, 218, 254, 255, 260
Millionaires Problem, 103
See also Socialist Millionaires Problem
Minimal generalizations, 114
Minimal query, 178
Minimal required suppression, 114
Minimal suppression, 114
Minimum-cost 2-anonymity, 120
Minimum-cost 3-anonymity, 120
MITM, *see* Man-in-the-Middle (MITM)
Mix
networks, 36, 39–44, 47–49, 51–54, 60, 63–65, 82, 110, 134, 211, 218, 228
nodes, 40–45, 47, 48, 51, 53, 54, 64, 218
Mixmaster remailers, 46, 51
Mixminion remailers, 51, 52
ML, *see* Machine Learning (ML)
ML algorithm, 220, 222
ML model, 9, 220–224
ML outputs, 220–223
Model outputs, 220, 224
Model parameters, 220
Modified public key, 123, 129
Modified showing protocol, 130
Moving target defense (MTD), 217
MPC, *see* Multi-Party Computation
MPC protocol, *see* Multi-Party Computation
Multi-factor authentication, 231
Multi-level secure relations, 176
Multi-party, 47, 154
Multi-Party Computation, *see* MPC protocol, *see* Secure Multi-Party Computationl
Multi-party computation (MPC), 47, 143, 150–158, 168–171, 229, 242
Multiplexing, 58
Multi-show, *see* Single-show credential
Multi-show credential, 135
See also Single-show credential
Multi-user group chat, 104
Mutual authentication, 75, 255
See also Unilateral

N
National Institute of Standards and Technology (NIST), 76, 220, 257
Network eavesdroppers, 33
Network layer security, *see* IPsec
Networking protocol, 71
Network-to-network communications, 97

NIST, *see* National Institute of Standards and Technology (NIST)
Non-policy-centered approach to disclosure protection, 175
Non-transferability, 131, 132, 136, 138, 243
NP-complete, 262
NP-hard, 120, 139, 261

O
OAKLEY Key Determination Protocol, 79
Oblivious polynomial evaluation, 212
Oblivious transfer, 154, 252, 253
Oblivious transfer protocol, 153, 154
OECD data protection principles, 176
Off-the-Record (OTR), 98–106, 211, 228
Off-the-Record (OTR) messaging, 95, 98–105, 228
One-time pad, 245
Onion
  proxies, 55, 58
  routers, 54–59, 211
  routing, 16, 53–64, 82, 110, 211, 218
  routing networks, 39, 54–57, 60, 61, 63, 228
Opaque, 131, 218
Open Whisper Systems, 103
Operation tuple, 34, 210
Order-Preserving Encryption Scheme (OPES), 181
OTR, *see* Off-the-Record (OTR)
Otr-dev, 101
Otr-users, 101
Output perturbation, 111

P
P3P
  1.0, 182, 183, 185, 186
  1.1, 182, 185, 186
  extension mechanism, 186
  policies, 183–188, 191–195, 203
  user agents, 183–188, 193, 194 (*see also* Platform for Privacy Preferences Project (P3P))
Packet sniffer, 62
Pairing-based cryptography, *see* Bilinear pairing-based cryptography
Passive adversary, 47, 62, 258, 260, 262
Password managers, 119
Path selection algorithms, 61
Payload data, 78, 79
PBE, *see* Policy-Based Encryption (PBE)
Pedersen commitment, *see* Commitment
Pedersen commitment on a biometric, 132
Peer authentication process, 80
Peer Authorization Database (PAD), 80
Perfect forward secrecy, 58, 73, 79, 99, 101, 104, 243
Performance enhancing mechanisms attacks, 63
Personal
  information, 1–4, 6–9, 12–15, 25, 29–33, 35, 36, 39, 40, 132, 151, 176, 177, 179, 181, 185, 192, 193, 195, 201, 202, 210–213, 215, 216, 219, 220, 227, 230, 232, 233, 235, 236
  privacies, 3, 21, 32, 176, 210, 231
  security, 7, 14, 33, 144, 177, 210, 211, 213
PETs, *see* Privacy Enhancing Technologies
PET techniques, *see* Privacy Enhancing Technologies
PETs community, *see* Privacy Enhancing Technologies
Phi-hiding, 86
Physical danger, 7, 16
Pidgin, 102, 104
  See also Gaim
PIR, *see* Private Information Retrieval (PIR)
Plaintext, 40, 41, 45, 51, 56, 57, 64, 75, 81, 97, 147, 149, 203, 244–246, 248, 250, 252, 256, 259, 260, 263–265
Platform for Privacy Preferences Project (P3P), 175, 182–189, 203
Plausible deniability, 106, 228
Policy
  Decision Point (PDP), 191
  Enforcement Point (PEP), 191
  meta-language, 179
  reference file, 185, 189, 193, 194
Policy-Based Encryption, *see* Identity-Based Encryption
Policy-based encryption (PBE), 193, 195, 203, 251, 252
Policy-centered PET, 182
Polynomial time, 120, 155
Polynomially-bounded attacker, 262
Polynomially-computable function, 151–154, 170, 261
Preference policy, 115
Premaster secret, 72, 73
Pretty Good Privacy (PGP), 98, 99, 104
Principles of a Hippocratic database
  accuracy, 177
  compliance, 177
  consent, 176

limited collection, 177
limited disclosure, 177
limited retention, 177
limited use, 177
openness, 177
purpose specification, 176
safety, 179
Privacy
advocates, vii, 15, 21
auditors, 2, 190, 192, 193, 195, 203, 215
audits, 28, 189, 190, 192, 193, 203
bird, 185–187, 189, 203
breaches, 2, 26, 31, 111, 118, 216, 234
certification teams, 2
Commissioners, 2, 21, 28, 220
communities, 1, 21, 36, 153, 176
definitions, 3, 4, 16, 18, 25, 27, 29–31, 110, 117, 144, 165–167, 169, 227
enforcement, 23, 28, 179, 192, 193, 195, 203
goals, 3, 17, 22, 25, 26, 29, 31, 36, 63, 99, 104, 113, 118, 122, 151, 158, 176, 177, 184, 204, 209–211, 216, 217, 219–224, 229, 231, 234, 235, 255
guidelines, 2, 26, 176, 203, 215
implications of machine learning, 220
law, 3, 26, 30, 183, 184, 215
levels, vii, 1, 2, 8, 22, 27, 28, 31–35, 49, 63, 75, 111, 114, 118, 120, 122, 134, 144, 163–165, 168–170, 180, 210, 229, 231, 232
metadata, 24, 88–90, 109, 177–179
metrics, 109, 117
minefield, 1–18
policies, 2, 3, 7, 13, 16, 18, 21, 24, 26, 144, 175–181, 183, 184, 187–190, 192, 193, 195, 203, 229
policy enforcement architectures, 214, 221, 223
practices, vii, 21, 88, 109, 120, 183–185, 188–190, 192, 196, 204, 209–224, 227, 231
preferences, 176–178, 180, 187, 189, 203, 213, 229
preservation, 24
preserving data mining, 212
privacy bird user agent, 186
protection goals, 23, 29
risks, 8, 16, 74, 75, 81, 89, 104, 106, 111, 149, 165, 166, 168, 190, 220, 230, 232–234, 255
seals, 189, 190, 192, 193, 195, 203
techniques, vii, 4, 13, 24, 25, 28, 29, 31–37, 39, 86, 87, 111, 118, 144, 149, 159, 167, 170, 176, 181, 201, 210–217, 221–224, 228, 229
transformations, 192, 211–213, 221
tree, vii, 17, 21–37, 39, 148, 170, 175, 203, 204, 209–224, 228, 229, 235
violations, 3, 4, 6, 26, 29, 216
Privacy enhancing technologies (PETs), vii, 2–4, 7, 15–18, 21–29, 36, 37, 39, 40, 53, 61, 63, 64, 69, 82, 88, 89, 95, 96, 105, 106, 109, 110, 122, 135, 137, 138, 143–145, 169, 175, 196, 203, 204, 209–211, 214, 216, 219, 221–224, 227–232, 234–236, 241, 242, 251, 261, 265
Privacy threats, 6–9, 227
Privacy-in-depth, 36, 231, 234, 235
Privacy-preserving delegation, 131
Privacy-related laws, 215
Privacy-related system goals, 23
Private conversations, 98, 103, 105
Private information retrieval (PIR), 4, 64, 69, 82–90, 167, 211, 228
Private key generator (PKG), 149, 193, 195, 252
Private keys, 42, 45, 55, 72, 99, 100, 122, 123, 125, 126, 128, 129, 131, 132, 134, 136, 137, 139, 145, 148–150, 157, 170, 171, 193–195, 200, 203, 229, 245, 249, 252, 256
Private Set Intersection (PSI), *see* Multi-Party Computation
Private Set Intersection protocol, *see* Multi-Party Computation
Profiling software, 9, 10
Proofs of cryptographic strength, 264
Properties of differential privacy
adaptive composition, 167
composability, 167
convexity, 167
convexity axiom, 167
parallel composition, 167
post-processing, 167
post-processing axiom, 167
sequential composition, 167
Property of an attribute, 121, 196, 198
Pseudonym-credential pair, 133
Pseudonymity service, 44
Pseudonymous, 44, 45, 211, 218
Pseudonymous identifier, 44
Pseudonyms, 22, 27, 39, 44, 133, 212
Pseudorandom number generator (PRNG), 245

Public key
asymmetric cryptography, 256
certificates, 72, 75, 100, 122, 123, 126, 247, 250, 251, 256
cryptography, 40, 42, 57
encryption algorithm, 248, 249
encryption/decryption algorithms, 245
"fingerprints", 102
infrastructure (PKI), 75, 122, 126, 250, 256

Q
Quadratic residuosity, 86
Quasi-identifier, 113
Query
interceptor, 179
intrusion detector, 177, 181
modifications, 158, 176, 179
modifier, 179
restrictions, 176

R
Random Oracle Model (ROM), 264
See also Standard model
Randomized response techniques, 212
RC4, 245
RC4 stream cipher, 73
Real-time bidirectional communication, 54
Record
protocols, 71
tuples, 34, 35, 210
Recursive (*c*-*l*)-diversity, 116, 118
Redirect messages, 81
Reference monitor, 149
Refresh protocol, 133
Regularization, 222, 223
Re-identify a specific individual, 111, 119
Re-identify an arbitrary individual, 119
Re-keying, 100, 101, 247, 250
Remote logins, 54, 81
Rendezvous, 47
Rendezvous points, 59
Replay attack, 41
Replay protection, 78
Retention periods, 177, 178, 193
Retention requirements, 5
Revocation schemes, 251
Right-to-be-forgotten, 5
Robust PIR, *see* Private Information Retrieval
Role-Based Access Control (RBAC), 149
Routing
attacks, 16, 56, 62, 64
nodes, 61, 218
updates, 81
RSA
algorithms, 249, 257
Digital signature (*see* Digital signature)
modulus, 133, 248, 249, 256
public key, 72, 125, 126, 134, 248, 249, 256
signature verification operation, 125, 256

S
Scrambled circuit, 152, *see* Garbled circuit
SDN, *see* Software Defined Networking (SDN)_
SDN Controller, *see* Software Defined Networking (SDN)
Secondary use, 25, 26
Second-generation onion router, 55
Secret Conversations, 103
Secret sharing schemes, 154, 247, 248
Secure
channels, 72, 75, 81, 89, 103, 105, 156, 212, 254
connections, 61, 71, 74, 75
deletion, 106
E-mail protocol, 99
Function evaluation (*see* Multi-Party Computation)
MPC, 150, 156, 157
MPC protocols, 151, 156, 171
secure connection to a web server, 70
Shell (SSH), 61, 219
sockets layer, 70, 71
systems, 81, 139, 176, 242
Secure/Multipurpose Internet Mail Extensions (S/MIME), 98, 99, 104
Security
Architecture for the Internet Protocol, 76
association (SA), 77
gateways, 78
Proofs (*see* Proofs of cryptographic strength)
services, 60, 77–79, 217, 218, 243
technologies, 59, 82, 103, 209–214, 221, 223, 228, 229
Security/privacy versus usability, 139
Semantic security, 86, 265
Sensitive attribute values, 120
Series of mix nodes, 42
Server authentication, 71
Server hello, 72, 74
SHA-1, 73, 78, 100, 254
SHA-256, 73, 254
SHA-384, 254
SHA-512, 254
Shared secret cryptographic keys, 79

Showing protocol, 128–137, 197, 201, *see* Issuing protocol
SIGMA protocol, 102, 103
Signal protocol, 103, *see* TextSecure
Signature verification operation, 124, 256
Signing authority, 257
Signing operation, 256
Silent Circle Instant Messaging Protocol (SCIMP), 103
Single-show credential, 134
See also Multi-show credential
Single-Use Reply Blocks (SURBs), 51
Skype, 103
SMP, *see* Socialist Millionaires Problem (SMP)
Social engineering, 2
Social media, 5–9, 13, 18, 105, 230, 233
Social sorting, 9
Socialist Millionaires Problem (SMP), 102, 103
See also Millionaires Problem
Socket connections, 54, 55
Software defined networking (SDN), 217–220, 223, 224, 229
Source routing, 46
Sovereign Information Integration (SII) architecture, 181
Spyware, 5
SSL, *see* Secure Sockets Layer (SSL)
SSL/TLS, *see* Secure Sockets Layer (SSL)
Standard model, 148, 264
See also Generic group model
See also Random Oracle Model
Static key, 247
Statistical databases, 158, 168, 176
Store-and-forward messaging architecture, 53
Stratified, 46, 47
Stream ciphers, 104, 245, 246
Super-user, 179
Suppressions, 112–115, 119, 138
Surveillance, 3, 12, 14, 25
Sybil attacks, 62
Sybilhunter, 62
Symmetric
algorithms, 245, 254, 260
decryption algorithm, 54, 245
encryption algorithm, 54, 245
encryptions, 42, 54–57, 102, 246, 249, 251, 254
key, 54–57, 103, 245–251, 254, 255, 259, 263
key derivation, 100, 246, 247, 249, 250, 254
Symmetrically private information retrieval (SPIR), 87
System Authority, 147–150, 171, 252

T
Table-level access control, 179
Tag, 133, 253–256
Tamper-resistant smart card technology, 132
Targeted advertising, 4, 6, 8, 11
Taxonomy, *see* Classification
T-closeness, 115, 117–119, 138
TCP/UDP, 81
Technological privacy techniques, *see* Classification
TextSecure, 103
See also Signal protocol
Third parties, 3, 6, 8, 14, 18, 25, 27, 64, 69, 75, 82, 95, 97, 99, 181, 185, 190, 221, 233, 250, 255, 256
Third party cookies, 211
Threat model for the onion routing network, 56
Threats to privacy, 4–8, 16, 227
Threshold cryptography, 150, 157, 195, 248
See also Multi-Party Computation
Timestamps, 41, 242
Timing attacks, 56
TLS, *see* Transport Layer Security (TLS)
Tools of cryptography, 242
Tor
browsers, 59, 60, 65, 74, 233
projects, 58
Tracing apps, 13
Trade-off between privacy and utility, 160, 169
Traffic analysis, *see* Action analysis
Traffic shaping, 58
Training data, 219–223
Training dataset, 220, 221
Transmission Control Protocol (TCP), 48, 58, 71, 75, 78
Transparency, 81, 89, 98
Transport layer security (TLS), 64, 69–77, 81, 82, 89, 99, 105, 195, 212, 219, 228, 233, 254
1.0, 70, 73, 74, 76
1.1, 70, 73, 76
1.2, 70, 73, 76
1.3, 70, 73, 74, 76
Transport Layer Security; SSL/TLS, *see* Secure Sockets Layer
Transport mode, *see* IPsec
Trust anchor, 250
Tunnel mode, *see* IPsec
2-database solution, 84
2-factor authentication, 75
Two-party protocol (2PC), 151, 157
2-server construction, 83–85

Type
0 remailer(Original anonymous remailer), 51, 52, 54
I remailer(Cypherpunk remailer), 51
II remailer(Mixmaster remailer), 51
III remailer(Mixminion remailer), 51, 63

U
Unauthorized dissemination of personal data, 6
Unconditionally binding, *see* Unconditionally hiding, Computationally binding, Computationally hiding
Unconditionally hiding, *see* Unconditionally binding, Computationally binding, Computationally hiding
Unilateral, 75, 255, *see* Mutual authentication
Unintended observers, 33, 109, 110, 176, 211, 213, 215, 219, 229
Unintended recipients, 25, 33, 35, 212–216, 221
Unintentional release of information, 34
Unique identifiers, 111–113, 137
Unlinkable multi-show credential, *see* Single-show credential
Unlinkability, 27, 131–134, 136, 138, 243
Untraceable payment systems, 124
Untraceable return address (URA), 44, 45, 51
U-Prove, 122
User agents, 183, 185–187, 189, 193, 194
User preferences, 183, 185, 187–190, 193, 195
Users, 2, 8–10, 16, 21, 22, 25, 28, 29, 39, 42, 45, 48, 50, 51, 53, 58–64, 69, 70, 74–79, 81–85, 87–90, 95–98, 101–103, 105, 109–111, 114, 118, 120, 121, 124, 125, 132, 133, 136–139, 143–145, 148–151, 166, 169–171, 175, 177–180, 183, 184, 186–196, 203, 212, 218–222, 243, 248–252, 257, 259
Utility of a data set, 114

V
Variable exit policies, 58
Vehicle forensics, 12
Verifiably-secure randomness, 47
Verification equation, 126, 128–130, 197
Virtual private networks (VPNs), 54, 55, 58, 81, 97, 98
Volume attacks, 57, 58
Voting systems, 124
VPN, *see* Virtual Private Network (VPN)
Vulnerability goals, 23, 29

W
Wearables, 5, 8
Web browsing, 54, 62, 63, 182, 185, 188, 189, 192, 196, 203
Website fingerprinting attacks, 62, 63
WhatsApp, 103
White-box setting, 220, 221
See also Black-box setting
Wiretap laws, 216
Wiretapper, 62
World Wide Web Consortium (W3C), 182

X
XACML, *see* eXtensible Access Control Markup Language
XML, *see* Extensible Markup Language (XML)
XSalsa20, 104, 245
XSLT, *see* eXtensible Stylesheet Language Transformation (XSLT)
XSLT stylesheet, *see* eXtensible Stylesheet Language Transformation (XSLT)

Z
Zero-knowledge
proof, 127, 133, 134, 263
proof of knowledge, 127, 138, 263
protocol, 132
ZKPoK, *see* Zero-knowledge proof of knowledge (ZKPoK)