English	German
absolute anonymity	absolute Anonymität
absolute unlinkability	absolute Unverkettbarkeit
abuse	Missbrauch
accountability	Zurechenbarkeit
accountability in spite of anonymity	Zurechenbarkeit trotz Anonymität
accountability with respect to a pseudonym	Zurechenbarkeit zu einem Pseudonym
acting entity	handelnde Entität
action	Handlung
addressable pseudonym	adressierbares Pseudonym
anonymity	Anonymität
anonymity set	Anonymitätsmenge
anonymous	anonym
a-posteriori knowledge	A-Posteriori-Wissen
application design	Anwendungsentwurf
a-priori knowledge	A-Priori-Wissen
attacker	Angreifer
attacker model	Angreifermodell
attribute	Attribut
attribute authentication by third parties	Attributauthentisierung durch Dritte
attribute certificate	Attributzertifikat
attribute values	Attributwerte
authentication	Authentisierung
avatar	Avatar
background knowledge	Hintergrundwissen
biometrics	Biometrie
blocking	Sperren
broadcast	Verteilung
certification authority	Zertifizierungsinstanz
chains of identity brokers	Ketten von Identitätstreuhändern
change history	Änderungshistorie
civil identity	zivile Identität
communication network	Kommunikationsnetz
communication relationships	Kommunikationsbeziehungen
complete identity	vollständige Identität
computer	Rechner

context	Kontext
convertibility	Umrechenbarkeit
convertibility of digital pseudonyms	Umrechenbarkeit digitaler Pseudonyme
cover claims	Forderungen abdecken
credential	Credential
customer pseudonym	Kundenpseudonym
data minimization	Datenminimierung
data protection regulations	Datenschutzregelungen
data subject	Betroffener
DC-net	DC-Netz
digital identity	digitale Identität
digital partial identity	digitale partielle Identität
digital pseudonym	digitales Pseudonym
digital signature	digitale Signatur
disinformation	Desinformation
distinguish	unterscheiden
dummy traffic	bedeutungsloser Verkehr
encryption	Verschlüsselung
end-to-end encryption	Ende-zu-Ende-Verschlüsselung
entity	Instanz
entropy	Entropie
forget	vergessen
globally unique pseudonym	global eindeutiges Pseudonym
group communication	Gruppenkommunikation
group pseudonym	Gruppenpseudonym
holder	Inhaber
holder of the pseudonym	Inhaber des Pseudonyms
human being	Mensch
I	“I”
ID	ID
identifiability	Identifizierbarkeit
identifiability set	Identifizierbarkeitsmenge
identifiable	identifizierbar
identifier	Identifikator
identifier of a subject	Identifikator eines Subjektes
identity	Identität

identity broker	Identitätstreuhänder
identity card	Ausweis
identity certificate	Identitätszertifikat
identity management	Identitätsmanagement
identity management application	Identitätsmanagementanwendung
identity management system	Identitätsmanagementsystem
identity theft	Identitätsdiebstahl
imply	implizieren
IMS	IMS
indistinguishability	Ununterscheidbarkeit
indistinguishable	ununterscheidbar
individual	Individuum
initially non-public pseudonym	initial nicht-öffentliches Pseudonym
initially unlinked pseudonym	initial unverkettetes Pseudonym
insider	Insider
introducer	Introducer, Bekanntmacher
is-a-person pseudonym	Ist-eine-Person-Pseudonym
items of interest	interessierende Dinge
key	Schlüssel
knowledge	Wissen
largest possible anonymity set	größtmögliche Anonymitätsmenge
lattice	Verband
legal person	juristische Person
liability broker	Treuhänder für Verbindlichkeiten
linkability	Verkettbarkeit
linkability between the pseudonym and its holder	Verkettbarkeit zwischen dem Pseudonym und seinem Inhaber
linkability broker	Verkettbarkeitstreuhänder
Me	“Me”
mechanisms	Mechanismen
mechanisms for anonymity	Mechanismen für Anonymität
mechanisms for unobservability	Mechanismen für Unbeobachtbarkeit
message	Nachricht
message content	Nachrichteninhalt
misinformation	Missinformation
MIX-net	MIX-Netz
mobile phone number	Mobiltelefonnummer

name	Name
natural person	natürliche Person
new knowledge	neues Wissen
non-public pseudonym	nicht-öffentliches Pseudonym
notice and choice	“Notice and Choice” (d.h. Information des Betroffenen und Gelegenheit
nym	Nym
nymity	Nymity
observation	Beobachtung
one-time pad	One-Time-Pad
one-time-use pseudonym	einmal zu benutzendes Pseudonym
organization	Organisation
outsider	Außenstehender
owner	Eigentümer
partial digital identity	digitale Teilidentität
partial identity	Teilidentität
perfect secrecy	perfekte Geheimhaltung
person pseudonym	Personenpseudonym
perspective	Sicht
precise	präzise
privacy	Privatheit
privacy-enhancing application design	Privatheit fördernder Anwendungsentwurf
privacy-enhancing identity management system	Privatheit förderndes Identitätsmanagementsystem
Privacy-Enhancing Technologies	Privatheit fördernde Technik
private information retrieval	Abfragen und Überlagern
private key	privater Schlüssel
probabilities	Wahrscheinlichkeiten
property	Eigenschaft
pseudonym	Pseudonym
pseudonymity	Pseudonymität
pseudonymization	Pseudonymisierung
pseudonymous	pseudonym
public key	öffentlicher Schlüssel
public key certificate	Zertifikat für den öffentlichen Schlüssel
public pseudonym	öffentliches Pseudonym
quality of anonymity	Anonymitätsqualität
quantify pseudonymity	Pseudonymität quantifizieren

quantify unlinkability	Unverkettbarkeit quantifizieren
quantify unobservability	Unbeobachtbarkeit quantifizieren
quantity of anonymity	Anonymitätsquantität
real name	wirklicher Name
recipient	Empfänger
recipient anonymity	Empfängeranonymität
recipient anonymity set	Empfängeranonymitätsmenge
recipient pseudonymity	Empfängerpseudonymität
recipient unobservability	Empfängerunbeobachtbarkeit
recipient unobservability set	Empfängerunbeobachtbarkeitsmenge
relationship anonymity	Beziehungsanonymität
relationship pseudonym	Beziehungspseudonym
relationship unobservability	Beziehungsunbeobachtbarkeit
relative unlinkability	keine Verkettbarkeitsänderung
reputation	Reputation
revocation	Widerruf
robustness of anonymity	Anonymitätsrobustheit
role	Rolle
role pseudonym	Rollenpseudonym
role-relationship pseudonym	Rollenbeziehungspseudonym
semantic dummy traffic	(den Angreifer) irreführender Verkehr
sender	Sender
sender anonymity	Senderanonymität
sender anonymity set	Senderanonymitätsmenge
sender pseudonymity	Senderpseudonymität
sender unobservability	Senderunbeobachtbarkeit
sender unobservability set	Senderunbeobachtbarkeitsmenge
sender-recipient-pairs	Sender-Empfänger-Paare
set	Menge
set of subjects	Subjektmenge
setting	Szenario
side channel	Seitenkanal
social role	soziale Rolle
social security number	Sozialversicherungsnummer
spread spectrum	Spreizband
state	Zustand

steganographic systems	Stegosysteme
steganography	Steganographie
strength of anonymity	Anonymitätsstärke
subject	Subjekt
surrounding	Umgebung
system	System
transaction pseudonym	Transaktionspseudonym
transfer of holdership	Transfer der Inhaberschaft
transferability	Transferierbarkeit
transferable group pseudonym	transferierbares Gruppenpseudonym
transferable pseudonym	transferierbares Pseudonym
uniqueness	Eindeutigkeit
universe	Universum
unlinkability	Unverkettbarkeit
unobservability	Unbeobachtbarkeit
unobservability set	Unbeobachtbarkeitsmenge
user-controlled linkage	benutzerkontrollierte Verkettung
user-controlled release	benutzerkontrollierte Freigabe
usual suspects	die üblichen Verdächtigen
value broker	Wertetreuhänder
virtual identity	virtuelle Identität
zero-knowledge proof	Zero-Knowledge-Beweis
(un)authorized	(un)autorisiert
(in)finite	(un)endlich
(un)achievable	(un)erreichbar
(un)intended	(un)erwünscht
(un)necessary	(un)nötig
(in)secure	(un)sicher
(un)predictable	(un)vorhersagbar
mapping	Abbildung
queries	Abfragen
interceptor	Abhörer
defense	Abwehr
adaptivity	Adaptivität
addressing	Adressierung
punish	ahnden

similar	ähnlich
in general	allgemein
omnipotent	allmächtig
therefore	also
employee	Angestellter
view of attacker	Angreifersicht
neighboring	angrenzend
area of attack	Angriffsbereich
succes of attack	Angriffserfolg
type of attack	Angriffstyp
goal of attack	Angriffsziel
note	Anmerkung
assumption	Annahme
arrangement	Anordnung
inflict	anrichten
subscriber line	Anschlussleitung
command	Anweisung
application	Anwendung
equivalent	äquivalent
reveal	aufdecken
roaming information	Aufenthaltsinformation
call	Aufruf
expense	Aufwand
outlook	Ausblick
propagation	Ausbreitung
skip	auslassen
ID-card	Ausweis
authentication system	Authentikationssystem
dummy	bedeutungslos
meaningful	bedeutungsvoll
constraint	Bedingung
threat	Bedrohung
certify	beglaubigen
claim	Behauptung
example	Beispiel
arbitrarily	beliebig

user	Benutzer
observing	beobachtend
consider	berücksichtigen
restrict	beschränken
get	besorgen
pass	bestehen
determine	bestimmen
operator	Betreiber
proof	Beweis
prove	beweisen
videophone	Bildtelefon
bit stream	Bitfolge
bit string	Bitkette
block	Block
broadband	Breitband
concerning	bzgl.
respectively	bzw.
cipher	Chiffre
encryption key	Chiffrierschlüssel
Chinese Remainder Theorem	Chinesischer Restsatz
smart card	Chipkarte
data protection	Datenschutz
privacy enhancing	datenschutzfreundlich
append	dazulegen
decryption key	Dechiffrierschlüssel
domain	Definitionsbereich
service	Dienst
service delivery	Diensterbringung
disjoint	disjunkt
wireless	drahtlos
average	Durchschnitt
efficiency	Effizienz
unique	eindeutig
interference	Eingriff
arrange	einordnen
one-way	Einweg

separate	einzeln
receiving	Empfang
end-to-end	Ende-zu-Ende
terminal	Endgerät
bottleneck	Engpass
decision	Entscheidung
decryption	Entschlüsselung
appropriately	entsprechend
designer	Entwerfer
development	Entwicklung
demand	erfordern
yield	ergeben
reminder	Erinnerung
recognizable	erkennbar
permission	Erlaubnis
feasible	erreichbar
reachability	Erreichbarkeit
await	erwarten
it holds	es gilt
stages	Etappe
exponential	exponentiell
capable	fähig
factor	faktorisieren
factorization	Faktorisierung
trap	Falle
forgery	Fälschung
missing	fehlend
fault detection	Fehlererkennung
fault tolerance	Fehlertolerance
error probability	Fehlerwahrscheinlichkeit
communications satellite	Fernmeldesatellit
regional switched phone network	Fernsprechortsnetz
long-distance exchange	Fernvermittlungstelle
commit	festlegen
finger print	Fingerabdruck
follow	folgen

conclusion	Folgerung
requirement	Forderung
dial tone	Freizeichen
radio network	Funknetz
rightmost	ganz rechts
iff	gdw.
adequate	geeignet
suitable	geeignet
braided	geflochten
countermeasure	Gegenmaßnahme
secret	geheim
keep secret	geheim halten
according to	gemäß
more precise	genauer
sufficient	genügend
device	Gerät
corrupted	gestört
maintained	gewartet
desired	gewünscht
gcd	ggT
show-case	Glasvitrine
credibility	Glaubwürdigkeit
equal	gleich
even distribution	Gleichverteilung
limit	Grenze
greatest common divisor	größter gemeinsamer Teiler
basic facts	Grundlagen
liability	Haftung
manufacturer	Hersteller
at most	höchstens
radio broadcast	Hörfunk
identification	Identifikation
probabilistic	probabilistisch
disclosure of information	Informationsgewinn
information theoretic	informationstheoretisch
content	Inhalt

data on interests	Interessendaten
integrity	Integrität
inverting	Invertierung
legal provisions	juristische Regelung
cabel link	Kabelverbindung
channel coding	Kanalkodierung
plaintext	Klartext
set of plaintext	Klartextmenge
collision-resistant	kollisionsresistent
complexity theory	Komplexitätstheorie
concealment	Konzelation
encryption system	Konzelationssystem
field	Körper (math.)
cryptography	Kryptographie
maintaining message length	längentreu
running time	Laufzeit
provide	liefern
wire network	Leitungsnetz
solution	Lösung
measure	Maßnahme
multilateral	mehrseitig
human beings	Menschen
mean calculation	Mittelwertbildung
network termination	Netzabschluss
undeniable	nicht herumzeigbar
message contents	Nutzdaten
open	offen
public	öffentlich
publicly known	öffentlich bekannt
improvement	Verbesserung
local exchange	Ortsvermittlungsstelle
pair relation	Paarbeziehung
bearing	Peilung
length of period	Periodenlänge
polynomial	Polynom
predictor	Prädiktor

prefix	präfix
prime number	Primzahl
producer	Produzent
truthful to protocol	protokolltreu
batch	puffern
quadratic residue	quadratischer Rest
receipt	Quittung
guess	raten
computer networks	Rechnernetze
legal certainty	Rechtssicherheit
ring of residue classes	Restklassenring
quadratic law of reciprocity	Reziprozitätsgesetz
feedback	Rückkopplung
consideration	Rücksicht
theorem	Satz (math.)
shell-shaped	schalenförmig
estimate	schätzen
seemingly	scheinbar
layer	Schicht
shift register	Schieberegister
shielding	Schirmung
key exchange	Schlüsselaustausch
key generation	Schlüsselgenerierung
set of keys	Schlüsselmenge
ciphertext	Schlüsseltext
key value	Schlüsselwert
spring lock	Schnappschloss
write access	Schreibzugriff
batch-wise	schubweise
protection measures	Schutzmechanismen
protection goal	Schutzziel
weaken	schwächen
threshold	Schwellwert
subscriber trunk dialing	Selbstwählferndienst
security	Sicherheit
security classes	Sicherheitsklassen

seal	Siegel
decrease	sinken
useful	sinnvoll
sketch	Skizze (i.S.v. Entwurf)
memory	Speicher
initial value	Startwert
principle of search	Suchprinzip
part	Teil
coprime	teilerfremd
participant	Teilnehmer
terminal equipment	Teinehmerendgerät
test result	Testergebnis
trustee	Treuhänder
skillfull	trickreich
trojan horse	Trojanisches Pferd
fallacy	Trugschluss
correspondence	Übereinstimmung
superpose	überlagern
superposition	Überlagerung
transmission system	Übertragungssystem
renaming	Umbenennung
re-encrypt	umcodieren
circumstance	Umfeld
converse	umgekehrt
reversible (Vorgang), invertible (Funktion, Permutation)	umkehrbar
circulation	Umlauf
change order	umsortieren
cumbersome	umständlich
independently	unabhängig
unconditional	unbedingt
opaque	undurchsichtig
undecidable	unentscheidbar
cannot hold	unerfüllbar
irrelevant	unerheblich
odd	ungerade
initial	Ur-

generalization	Verallgemeinerung
modifying	verändernd
anchoring	Verankerung
legal enforceability	Verbindlichkeit
link encryption	Verbindungsverschlüssung
hidden / covert	verdeckt
invisible	verdeckt
hiding	Verdecktheit
availability	Verfügbarkeit
compare	vergleiche, vgl.
behavior	Verhalten
traffic data	Verkehrsdaten
truncated	verkürzt
switched network	Vermittlungsnetz
telephone exchange	Vermittlungsstelle
publish	veröffentlichen
different	verschieden
infinitesimal fraction	verschwindender Bruchteil
pollution	Verschmutzung
strengthen	verstärken
distributed systems	verteilte Systeme
domain of trust	Vertrauensbereich
thrustworthy	vertrauenswürdig
confidential	vertraulich
confidentiality	Vertraulichkeit
useable	verwendbar
delay	Verzögerung
von-Neumann-computer	von-Neumann-Rechner
advantage	Vorteil
choose	wählen
probability	Wahrscheinlichkeit
service and maintenance	Wartungsdienst
correlation	Wechselwirkung
somewhat analyzed	wenig untersucht
value	Wert
co-domain	Wertebereich

contradiction	Widerspruch
as mentioned above	wie oben
well analyzed	wohluntersucht
root	Wurzel
extracting roots	wurzelziehen
number theory	Zahlentheorie
payment system	Zahlungssystem
character	Zeichen
character string	Zeichenkette
interval	Zeitabstand
time-slice channel	Zeitscheibenkanal
decomposition	Zerlegung
witness	Zeuge
aim	Ziel
random number	Zufallszahl
admission control	Zugangskontrolle
access	Zugriff
access control	Zugriffskontrolle
assign	zuordnen
at present	zur Zeit
fit	zusammen passen
summary	Zusammenfassung
connectedness	Zusammenhang
intermediate	Zwischen-
indeterministic	indeterministisch
key distribution	Schlüsselverteilung
to delay	verzögern