Einführung in die Informationssicherheit

Florian Mendel

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

http://www.iaik.tugraz.at/

L7 – Privacy

Einführung in die Informationssicherheit

Ausblick und Motivation

- Was ist Privacy/Privatsphäre?
- Was sind Privacy Enhancing Technologies?
- Welche PETs gibt es für das Internet?

- Ein Beispiel: WayBack Machine
  - `www.archive.org/index.php`
  - Ca. 2 Petabyte Daten, Wachstum 20 Terabyte pro Monat.

Privacy

Definition

Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others.

- Territorial privacy – Räumliche Privatsphäre
- Privacy of the person – Persönliche/moralische Privatsphäre
- Informational privacy – Privatsphäre der Daten

Grundlegende Datenschutz-Prinzipien

- Zweck-Angabe und Zweckbindung
- Notwendigkeit von Sammlung und Verarbeitung von Daten
- Transparenz
- Benutzung von Sicherheitsmechanismen

EU Datenschutz Direktive

Prinzipen bzgl. der Qualität der Daten

Daten müssen

- fair und rechtmäßig verwendet werden
- für einen spezifizierten, expliziten und genehmigten Zweck verwendet werden und dürfen nicht auf eine widerprechende Weise verarbeitet werden.
  - Erlaubt: Verwendung der Daten für historische, statistische oder wissenschaftliche Zwecke . . . vorausgesetzt, es gibt Sicherheitsvorkehrungen;
- adäquat, relevant und für den Zweck ausreichend, für den sie gesammelt oder verwendet wurden, sein.

EU Datenschutz Direktive

Prinzipen bzgl. der Qualität der Daten

Daten müssen

- akkurat und, wo notwendig, auf dem neuesten Stand sein; es müssen alle vertretbaren Maßnahmen getroffen werden, das falsche oder unvollständige Daten (in Bezug auf den Zweck, für den sie gesammelt wurden
- in einer Form vorliegen die die Identifikation der Daten-Subjekte genau so lange wie notwendig erlaubt und zwar nur für den Zweck für den die Daten verwendet werden dürfen
  . . . Sicherheitsmaßnahmen im Falle wenn personenbezogene Daten für längere Zeit gespeichert werden (für historische, statistische oder wissenschaftliche Zwecke

Die Lage in Österreich

- 1978: Erstes Datenschutzgesetz in Österreich
- Seit 2000 “Datenschutzgesetz 2000” in Kraft:
  - Umsetzung der EU Datenschutz-Richtlinie aus dem Jahr 1995
  - Schutz der Privatsphäre und Datenaustausch
  - Grundlegende Überarbeitung 2005

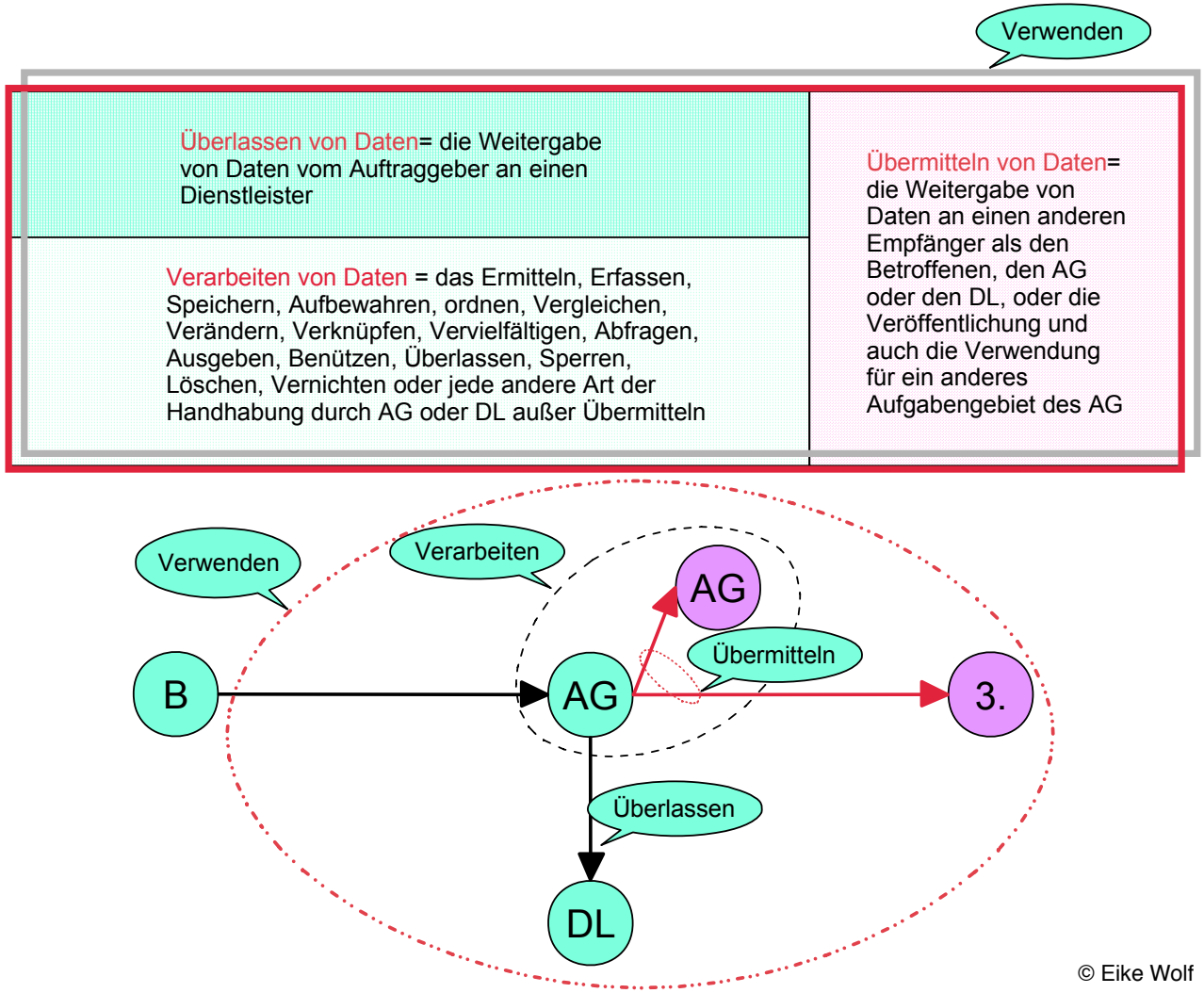
Die wichtigsten Begriffe DSG §4

- Daten (personenbezogene Daten):
  - Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist (z.B.: LH der Steiermark)
- Sensible Daten:
  - rassische und ethnische Herkunft
  - politische Meinung
  - Gewerkschaftszugehörigkeit
  - religiöse oder philosophische Überzeugung
  - Gesundheit
  - Sexualleben

Die wichtigsten Begriffe DSG §4

- Betroffener
- Auftraggeber
- Dienstleister
- Datenschutzkommission – Unabhängige Kontrollbehörde
  `www.dsk.gv.at`
- Verwenden von Daten

Die wichtigsten Begriffe DSG §4 graphisch



Übermittlung von Daten ins Ausland (§12 DSG)

- Alle EU-Mitgliedsstaaten und EWR-Staaten haben die EU-Datenschutzrichtlinie umgesetzt
  - d.h. keine Beschränkungen für den Datenverkehr mit diesen Staaten
- Ansonsten ist der Datenverkehr mit Drittstaaten genehmigungspflichtig
  - Ausnahmen: Veröffentlichte Daten, indirekt personenbezogene Daten, Zustimmung des Betroffenen, etc.
- Genehmigung durch die DSK!

Pflichten des AG und DL

- Alle Grundsätze müssen eingehalten werden
- AG haftet für DL und dessen Mitarbeiter
- Zusätzlich: Datensicherheitsmaßnahmen §14 DSG
  - Auftraggeber und Dienstleister müssen Datensicherheit gewährleisten, d.h. sicherstellen, dass Daten vor zufälliger oder unrechtmäßiger Zerstörung oder Verlust geschützt sind, ihre Verwendung ordnungsgemäß erfolgt und die Daten Unbefugten nicht zugänglich sind
  - Die Datenverwendung an das Vorliegen gültiger Aufträge binden; Jeden Mitarbeiter über seine nach diesem Gesetz bestehenden Pflichte belehren
  - Protokoll führen

Rechte des Betroffenen

- Das Auskunftsrecht (§26):
  - Dem Betroffenen ist auf Verlangen binnen 8 Wochen unentgeltlich Auskunft über die zu seiner Person verarbeiteten Daten zu erteilen
  - Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen in verständlicher Form zu geben
  - Voraussetzung dafür ist ein schriftlicher Antrag an den Auftraggeber und der Identitätsnachweis vorher oder nachher
- Recht auf Richtigstellung oder Löschung (§27)
- Widerspruchsrecht (§28)

Ausblick und Motivation

- Was ist Privacy/Privatsphäre?
- Was sind Privacy Enhancing Technologies?
- Welche PETs gibt es für das Internet?

Privacy Enhancing Technologies

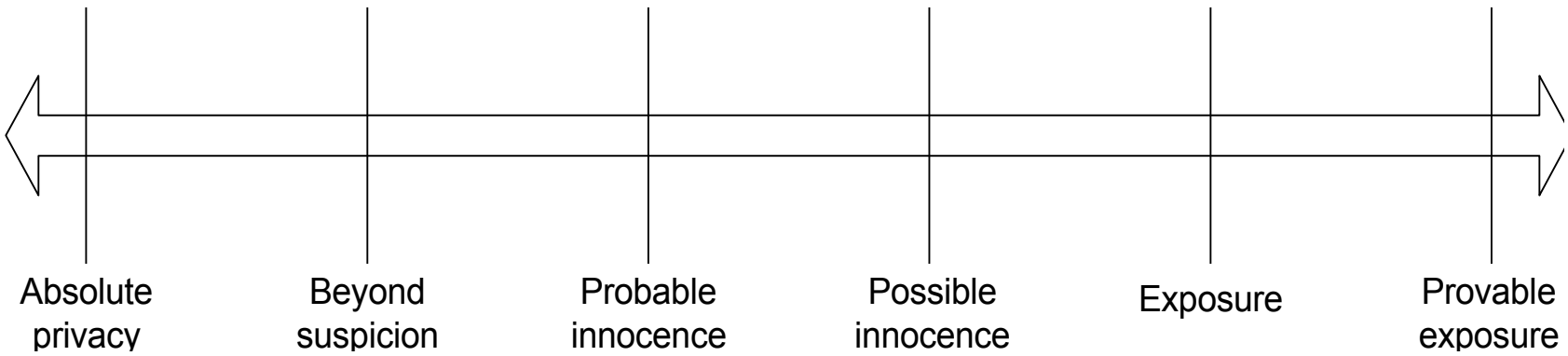
Definition

Privacy enhancing technologies have been defined as a coherent system of measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system

Kurz: PETs sind Technologien um Individuen oder Gemeinschaften vor Überwachung und Störung zu schützen

Anonymity

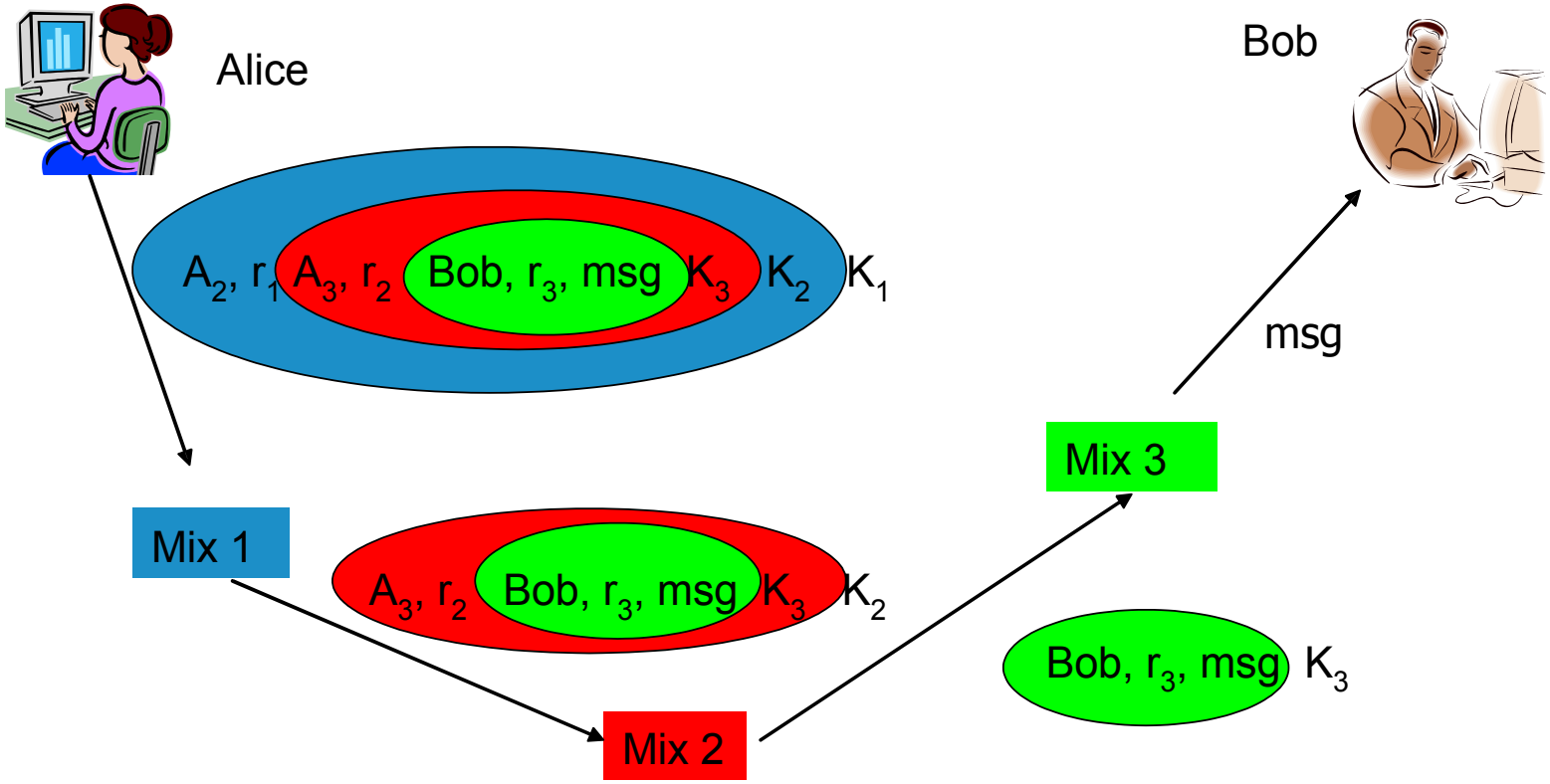
- Sender anonymity
- Receiver anonymity
- Unlinkability



Mix Network

- Versteckt den Zusammenhang zwischen den ein- und ausgehenden Nachrichten des Netzwerkes
- Eingehende Nachrichten
  - Werden gepaddet, damit alle Nachrichten diesselbe Länge haben
  - Info über Eingangszeitpunkt wird randomisiert
  - Werden verschlüsselt...

Mix Network


Alice
Bob
A_2, r_1 A_3, r_2 Bob, r_3, msg K_3 K_2 K_1
msg
Mix 1
Mix 2
Mix 3
A_3, r_2 Bob, r_3, msg K_3 K_2
Bob, r_3, msg K_3

Crowds

- Ein User (Alice) versteckt seine Aktionen in einer Gruppe
- Beispiel: Web-Transaktion
  - Alice tritt einer Gruppe/Crowd bei
  - Alice's Request wird zu einem beliebigen Mitglied der Crowd geforwarded
  - Dieses Mitglied forwarded den Request an ein anderes Mitglied der Crowd oder schickt den Request tatsächlich zum Server

Ausblick und Motivation

- Was ist Privacy/Privatsphäre?
- Was sind Privacy Enhancing Technologies?
- Welche PETs gibt es für das Internet?

Anonymous communications

- Remailers: Anonymous, Cypherpunk, Mixmaster
  `http://www.stack.nl/~galactus/remailers/index-anon.html`
- Eternity service
  `http://www.cypherspace.org/adam/eternity/`
- AnonNet service
  `http://www.authnet.org/anonnet`
- Free Haven
  `http://www.freehaven.net/`
- Privoxy Anonymizer
  `http://www.anonymizer.com/`
- JAP und TOR
  `http://anon.inf.tu-dresden.de/`
  `http://www.torproject.org/`

Pseudonyme Zertifikate

- Enthalten NICHT den echten Namen eines Subjekts
- Das Pseudonym ersetzt den echten Namen
  - Zufällig gewählt
  - Bewahrt Anonymität gegenüber Außenstehenden
  - Bewahrt Anonymität gegenüber Kommunikationspartnern

Pseudonyme Zertifikate – Nachteile

- Service Provider kann noch immer ein User-Profil erstellen
- Möglichkeit der Kombination von Daten mit anderen Service Providern um Benutzer-Info oder Identität herauszufinden
- Lösung: Transaktionsabhängige Pseudonyme

Anonyme Credentials

- Credentials sind Tokens, die einem das Recht geben, bestimmte Aktionen auszuführen
  - Named Credentials:
    - Username, Passwort
    - x509-Zertifikat
  - Anonyme Credentials: Kinoticket, Hausschlüssel
- Vergleiche: Ecash!

Anonyme Credentials – Auto mieten

- Idee: Reduzieren der bereitgestellten Information um Linkability/Data pooling zu verhindern

Was wird erbracht?	**Was wird benötigt?**
Geburtstag: 31.12.1980	Über 18
Kontostand: € 21.347.-	Kontostand > € 2000.-
Gesamte Reisepass-Info	Nationalität
Gesamte Führerschein-Info	Besitz eines Führerscheins
Echter Name	Pseudonym

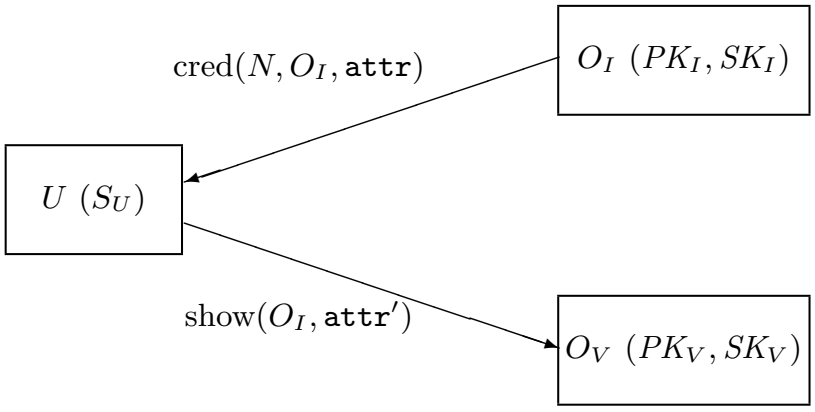
IDEMIX (IBM Zürich)

- Features:
  - Organisation kennt User nur unter Pseudonym
  - “Nyms” können nicht gelinkt werden
  - Benutzer eines Credentials kann beweisen, dass er es besitzt, OHNE es zu zeigen (Zero-knowledge Protokolle)
  - Attribute: User kann selbst wählen, welche Attribute er dem Service Provider öffnet

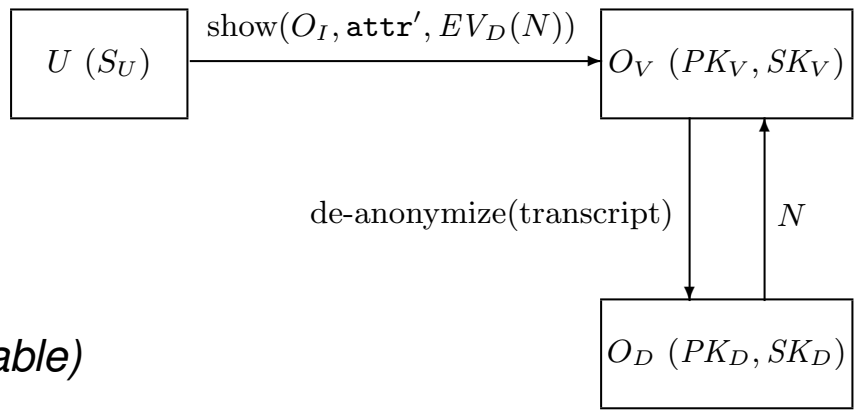
IDEMIX (IBM Zürich)

- Features:
  - Verschiedene User können ihre Credentials nicht kombinieren/teilen
  - Anonymity Revocation durch Trusted Third Party bei Zuwiderhandlung gegen Bedingungen (Auto nicht zurückgegeben)
  - Revokation von Credentials
  - “One-show credentials”

IDEMIX Protocol



U	*user*
O_i	*issuing organisation*
O_v	*verifying organisation*
N	*pseudonym*
attr	*credential's attributes*
S_u	*user's master secret*
PK / SK	*public/secret encryption key*

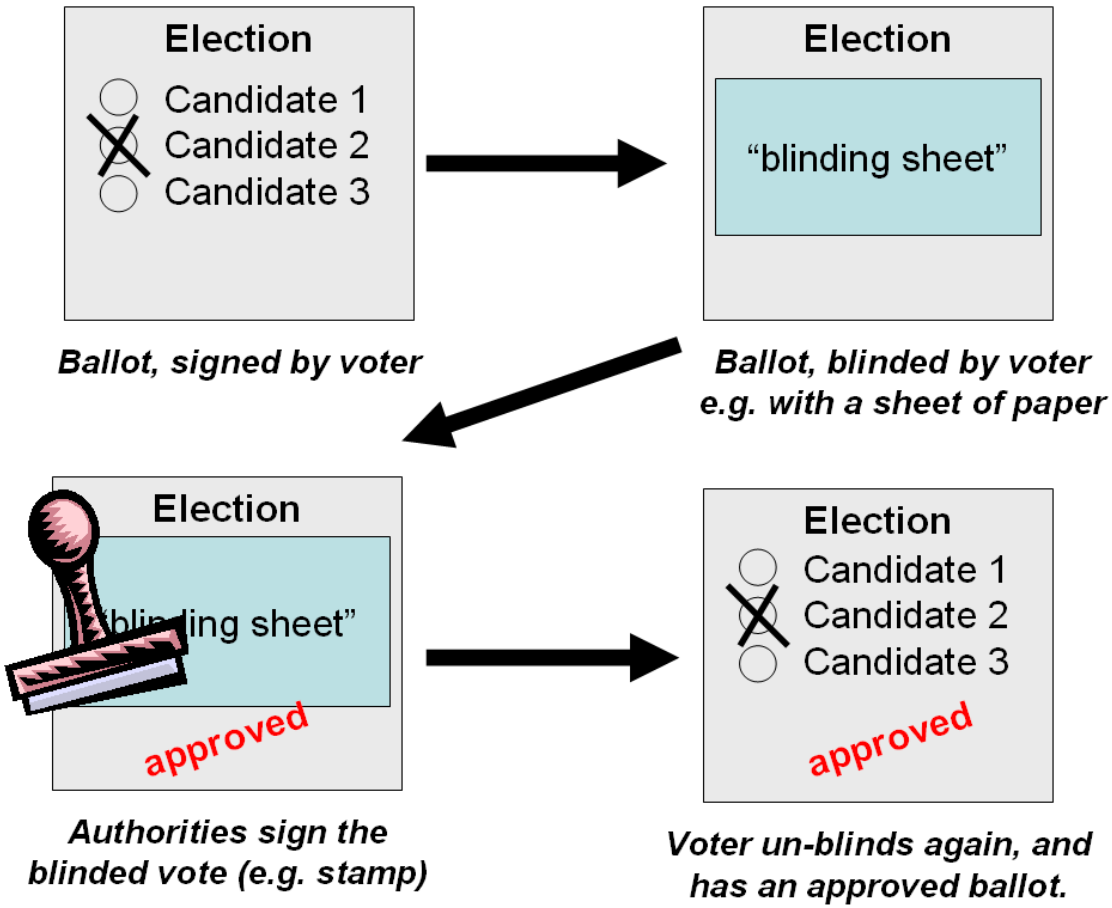


O_D	*de-anonymizing organisation*
$EV_D(N)$	*with PK_D encrypted N (verifiable)*

Electronic Voting

- Sehr oft “Security by Obscurity” (Diebold)
- Privatsphäre, allgemein verifizierbar, kein Verkaufen von Stimmen, keine Möglichkeit für Manipulation, und, und, und . . .
- Einige gute Ansätze, aber . . .

Blinde Signaturen



Blinde Signaturen

- Können garantieren, dass nur zulässige Wähler ihre Stimmen abgeben können
  - Vor der Wahl muss sich der Wähler eindeutig identifizieren
  - Danach lässt der Wähler seinen geblindeten Wahlschein von derselben Authority unterschreiben
- Echtheit des Wahlzettels kann dann durch die Signatur überprüft werden
- Die Registrierungsbehörde kennt die Wahlentscheidung nicht
- Die Wahlbehörde kann die Echtheit überprüfen, aber nicht, herausfinden, wer die Wahl getroffen hat

(Secure) Multi-Party Computation

- t User kennen t Geheimnisse x_i
- Berechne $(y_1, ..., y_t) = f(x_1, ...x_t)$, sodass User i nur y_i kennt
  - Yao's Millionaire Problem

$$f(x_1,x_2) = \begin{cases} 1, \text{ if } x_1 < x_2 \\ 0 \text{ otherwise} \end{cases}$$

  - Electronic Voting

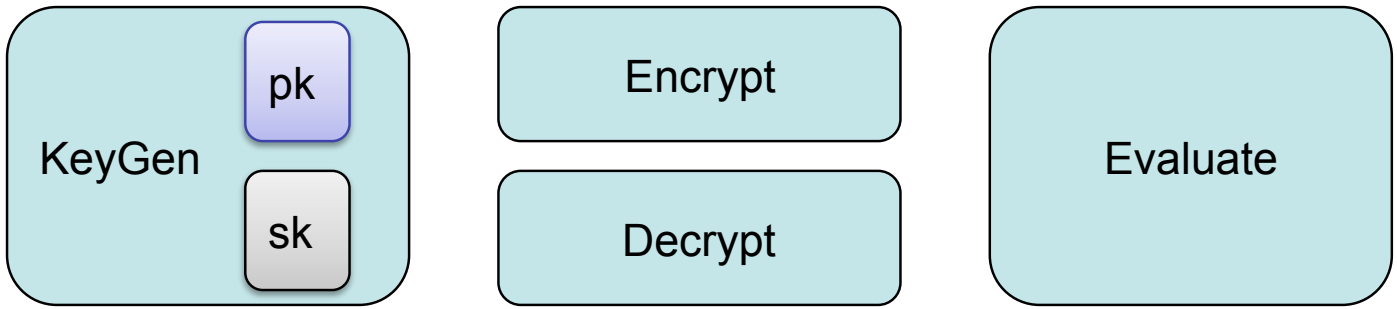
$$f(x_1,...,x_t) = \begin{cases} 1, \text{ if } \sum x_i < t/2 \\ 0 \text{ otherwise} \end{cases}$$

  - Sealed-bid auction

$$f(x_1,...,x_t) = (i,x_i) \text{ where } x_i = \max(x_1,...,x_t)$$

(Fully) Homomorphic Encryption

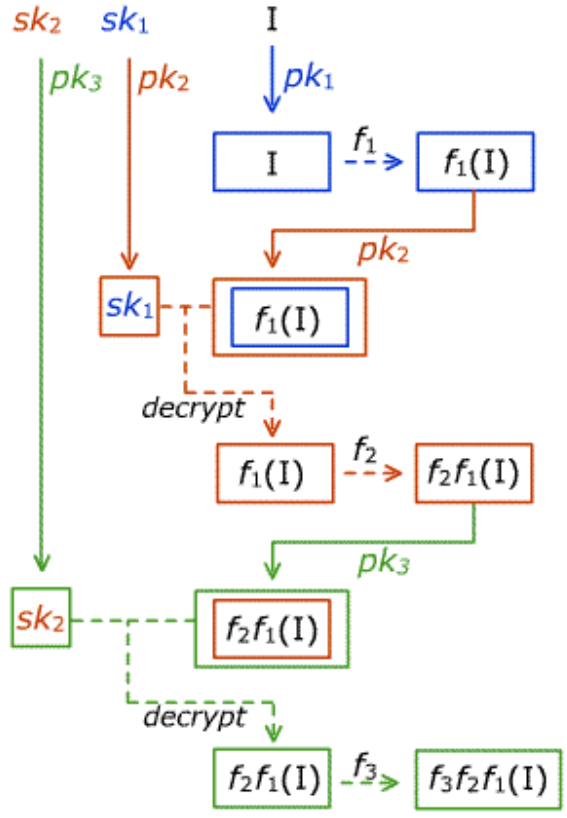
- Heiliger Gral in der Public Key Kryptographie für $\approx$ 30 Jahre (Vorschlag dafür bereits 1978)



- Für alle f in F und alle Plaintexte $m_1, \ldots, m_t$ und zugehörige $c_i = \mathit{Encrypt}(m_i)$ gilt
  - $c = \mathit{Evaluate}(f, c_1, \ldots, c_t)$
  - $\mathit{Decrypt}(c) = f(m_1, \ldots, m_t)$

Fully Homomorphic Encryption

- Cloud Security
- Encrypted Google Search
- Encrypted Database Queries
- . . .



© Tony Philips

Weitere Hot-Topics

- (Biometrische) Reisepässe
- RFID-Tags
- Internet-Zensur
- Google Inc.
- Vorratsdatenspeicherung
- US Patriots Act (auch UK)
  - Herausgabe von privaten Schlüsseln bei Terrorverdacht, etc.
  - CCTVs

Quellen

- *A Survey on Mix Networks and Their Secure Applications, Sampigethaya and Poovendran, Proceedings of the IEEE, Vol. 94, No. 12, 2006*
- *Datenschutz für Techniker, Dr. Eike Wolf, Vortrag im ÖVE, 6.11.2008*
- *An Introduction to Privacy Enhancing Technologies. G. Danezis, Cambridge University*
- *Design and Implementation of the IDEMIX Anonymous Credential System. Jan Camenisch, Els Van Herreweghen*

Vielen Dank für Ihre Aufmerksamkeit!

Appendix

Auskunftsrecht in der Praxis?

Das Auskunftsrecht nach dem Datenschutzgesetz 2000 – Eine Fallstudie von Gerhard Reichmann:

- “Im Rahmen einer am Institut für Informationswissenschaft der Universität Graz im Jahre 2003 unter Leitung des Autors dieses Beitrages durchgeführten Studie sollte untersucht werden, ob Datenschutzanfragen (Auskunftsbegehren) gesetzeskonform beantwortet werden.”

- “Zu diesem Zweck erhielten fünf Studierende (Betroffene) der Informationswissenschaft im Zuge einer Lehrveranstaltung den Auftrag, Datenschutzanfragen an jeweils fünf bis zehn Institutionen (Auftraggeber) zu richten, bei denen sie eine Speicherung von Daten zu ihrer Person vermuteten.”

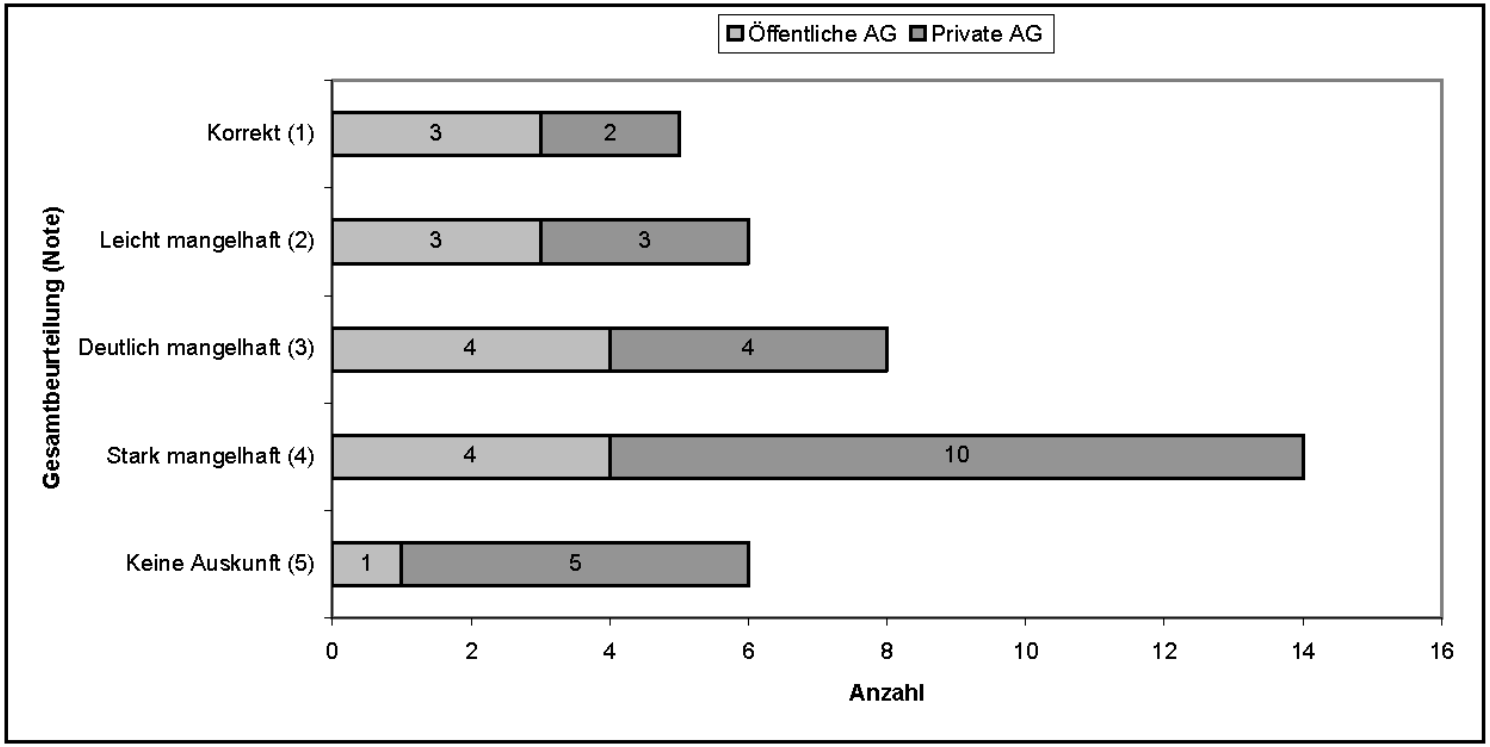
Eine Fallstudie (Gerhard Reichmann)

Anträge an folgende Institutionen:

- ihre Wohnsitzgemeinde
- das zuständige Finanzamt (Wohnsitzfinanzamt)
- den zuständigen Sozialversicherungsträger
- ihre kontoführende Bank
- eine Privatversicherung, zu der ein Vertragsverhältnis besteht
- einen Arzt, der in letzter Zeit aufgesucht wurde
- einen Verein, bei dem sie Mitglied sind
- sowie ein Telekommunikationsunternehmen, zu dem ein Vertragsverhältnis besteht

- Die genaue Auswahl der Auftraggeber blieb den Studierenden überlassen. Form und Inhalt der einzelnen Datenschutzanfragen waren dagegen exakt vorgegeben

Eine Fallstudie (Gerhard Reichmann)



Die meisten Institutionen gaben Auskunft, die Qualität war jedoch mangelhaft

Eine Fallstudie (Gerhard Reichmann)