Universität Karlsruhe (TH)
Forschungsuniversität · gegründet 1825

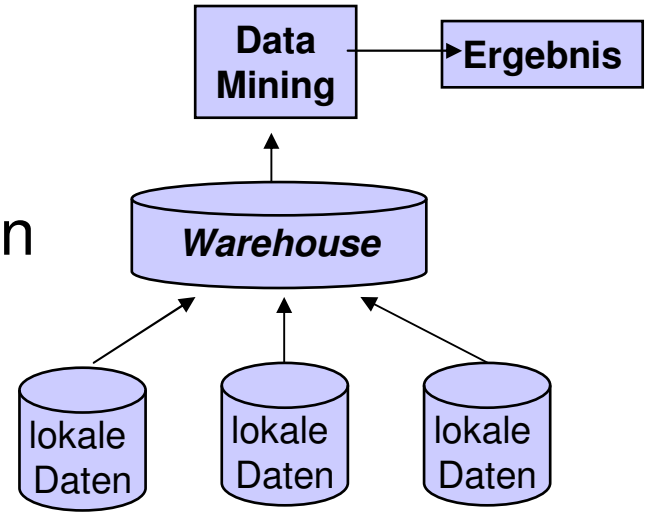
Vorlesung

Datenschutz und Privatheit in vernetzten Informationssystemen

Kapitel 7: Ergänzung

Thorben Burghardt, Erik Buchmann
buchmann@ipd.uka.de

Ergänzung



- Idee Secure Multiparty Computation
  - Emuliere die Trusted Third Party
- Ansatz: Circuit Evaluation
  - Yao [86] hat gezeigt, dass wir Kryptographie-Techniken nutzen können, um zufällige ‚output shares' eines Gatters bei zufälligen ‚input shares' berechnen zu können.
  - Mapping von ‚random inputs' auf ‚random outputs'
  - Garbled Circuit, bestehend aus
    - Garbled Gates
    - „Output Decryption Tables"
    - Die Tabellen mappen die ‚random' Werte der ‚Output-Wires' zurück auf die wirklichen Werte.

Secure Multiparty Computation: Definitions

- Unsere Definition von *Secure*
  - Niemand weiß irgend etwas bis auf die eigene Eingabe und das Ergebnis
  - Formal: ∃ polynomial time S genau so, dass {S(x,f(x,y))} ≡ {View(x,y)}

- Semi-Honest model: folgt dem Protokoll, eine Partei darf aber alles verwenden, was sie während des Protokolls lern

Was wäre der Gegensatz
  - Malicious: “cheaten” um etwas herauszufinden

Beispiel: Exklusiv-Oder

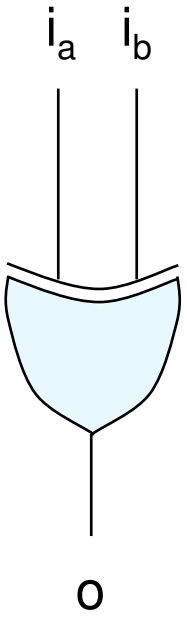
A	B	A ⊻ B
T	T	F
T	F	T
F	T	T
F	F	F

Person A

- Wähle zufälliges Bit r_a
- Schicke r_a an B
- Ersetze Input i_a durch $(i_a \oplus r_a)$
- Berechne $o_a = (i_a \oplus r_a) \oplus r_b$

Person B

- Wähle zufälliges Bit r_b
- Schicke r_b and A
- Ersetze Input i_b durch $(i_b \oplus r_b)$
- Berechne $o_b = (i_b \oplus r_b) \oplus r_a$



Bisher nichts preisgegeben außer der Zufallszahl

$$o = o_a \oplus o_b = ((i_a \oplus r_a) \oplus r_b) \oplus ((i_b \oplus r_b) \oplus r_a)$$
$$= i_a \oplus i_b \oplus r_a \oplus r_a \oplus r_b \oplus r_b$$
$$= i_a \oplus i_b$$

XOR = (A + B) mod 2
→ Assoziativ & Kommutativ

Ergänzung

- Selbst wenn ein Zwischenergebnis im Schaltkreis bekannt ist, lässt das keine Rückschlüsse auf den Input zu, da die Schlüssel des Inputs gleich Wahrscheinlich sind

- Yao [82] hat eine Lösung für das ‚Millionaires-Problem' für zwei Parteien geliefert. Beispielablauf des Protokolls gegeben in http://www.proproco.co.uk/million.html