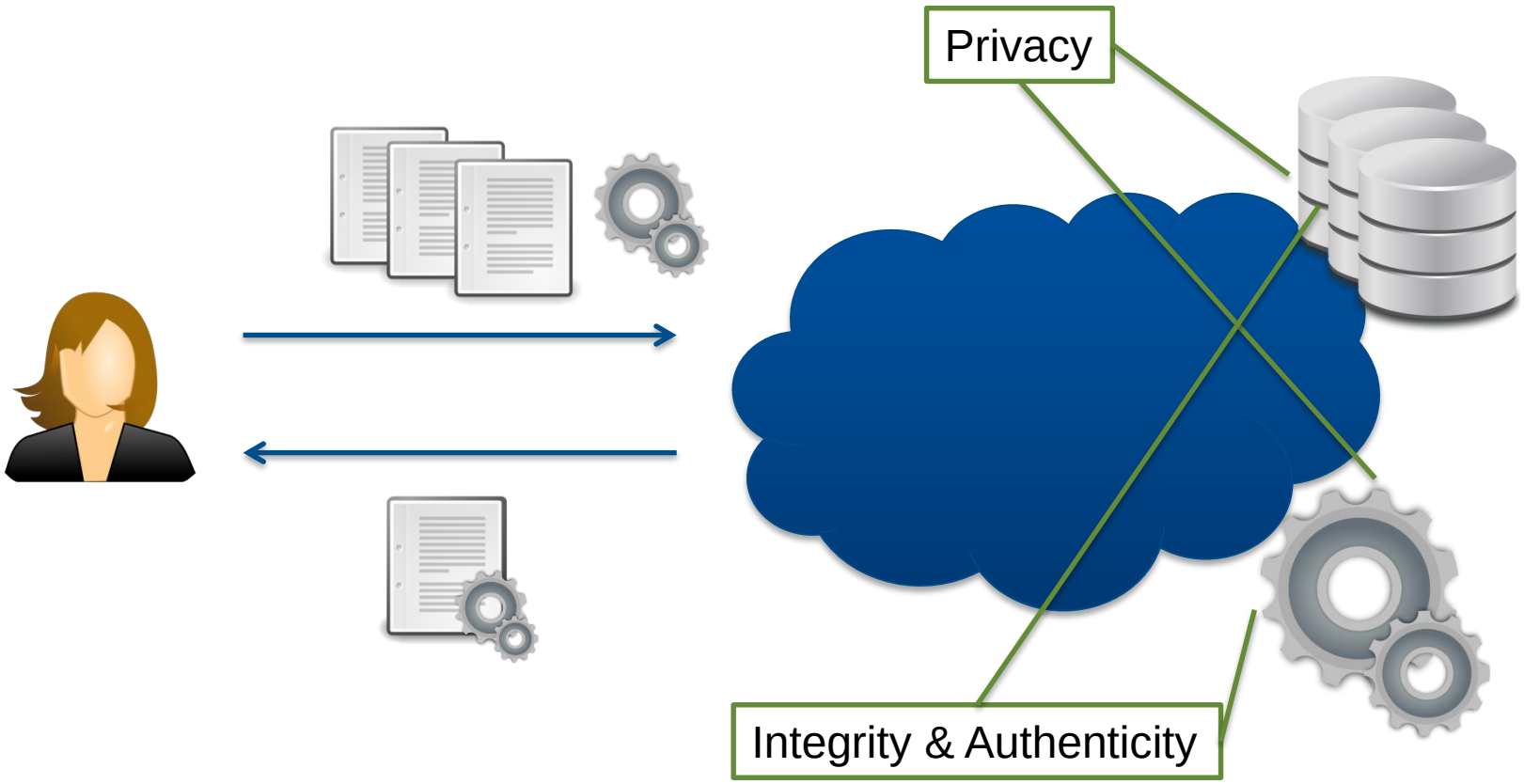
Security-Preserving Operations on Big Data

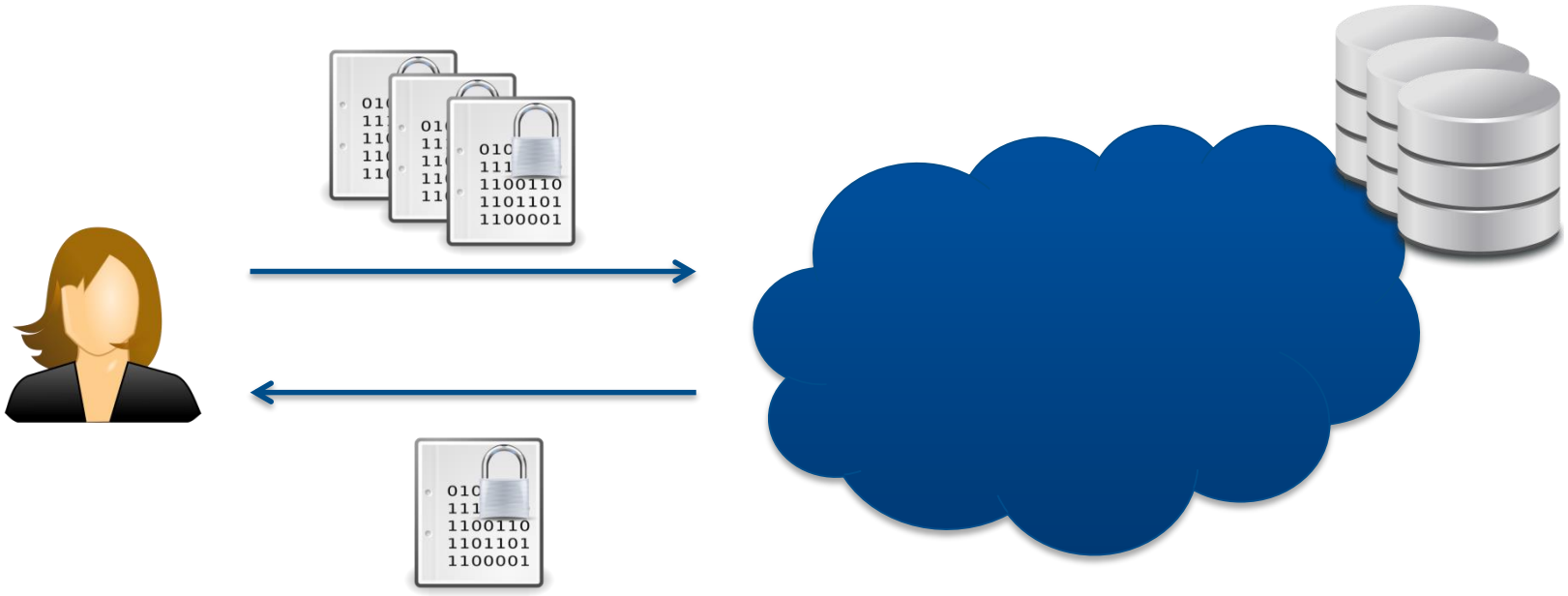
Algorithms for Big Data, Frankfurt, Juni 2014

Marc Fischlin
Alexander May
Arno Mittelbach

Sicheres Outsourcing von Daten **und** Berechnungen



Sicheres Outsourcing von Daten **und** Berechnungen



Ansätze

allgemeine Lösung

fully homomorphic encryption, code obfuscation,…

deterministische Verschlüsselung, spezielle Unterschriftenverfahren,…

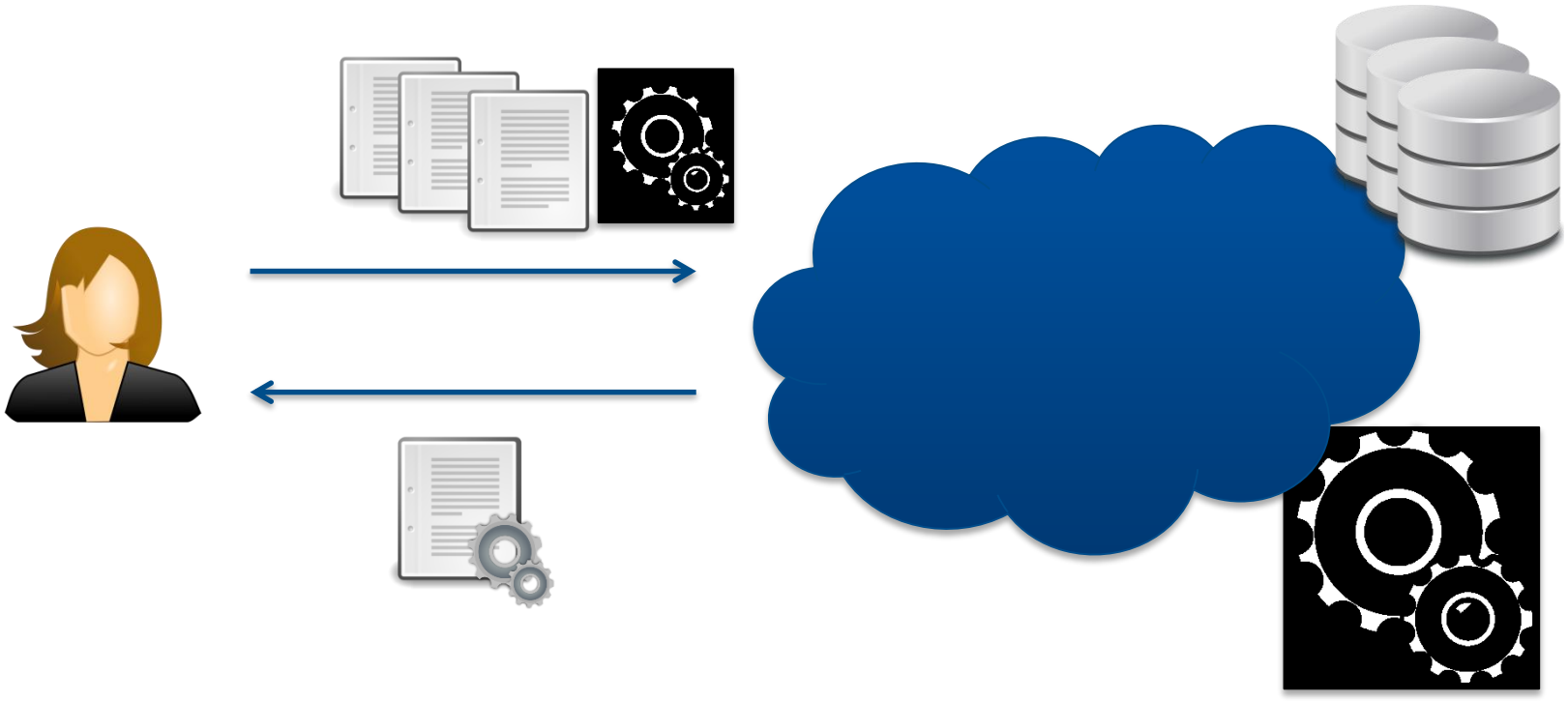
spezielle, effizientere Lösung

Code Obfuscation

```
alert("hello world")
```

```
eval(function(p,a,c,k,e,d){e=function(c){return
c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}
k=[function(e){return d[e]}];e=function(){return'\\w
+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\
\b'+e(c)+'\\b','g'),k[c])}}return p}('0("1 2");',3,3,'alert|
hello|world'.split('|'),0,{}))
```

Sicheres Outsourcing von Daten **und** Berechnungen



Obfuscation in Crypto

- Viele negativ Resultate
- [GGHRSW13]
  - Kandidat für Indistinguishability Obfuscation (IO)

Witness Encryption

Deniable Encryption

Functional Encryption

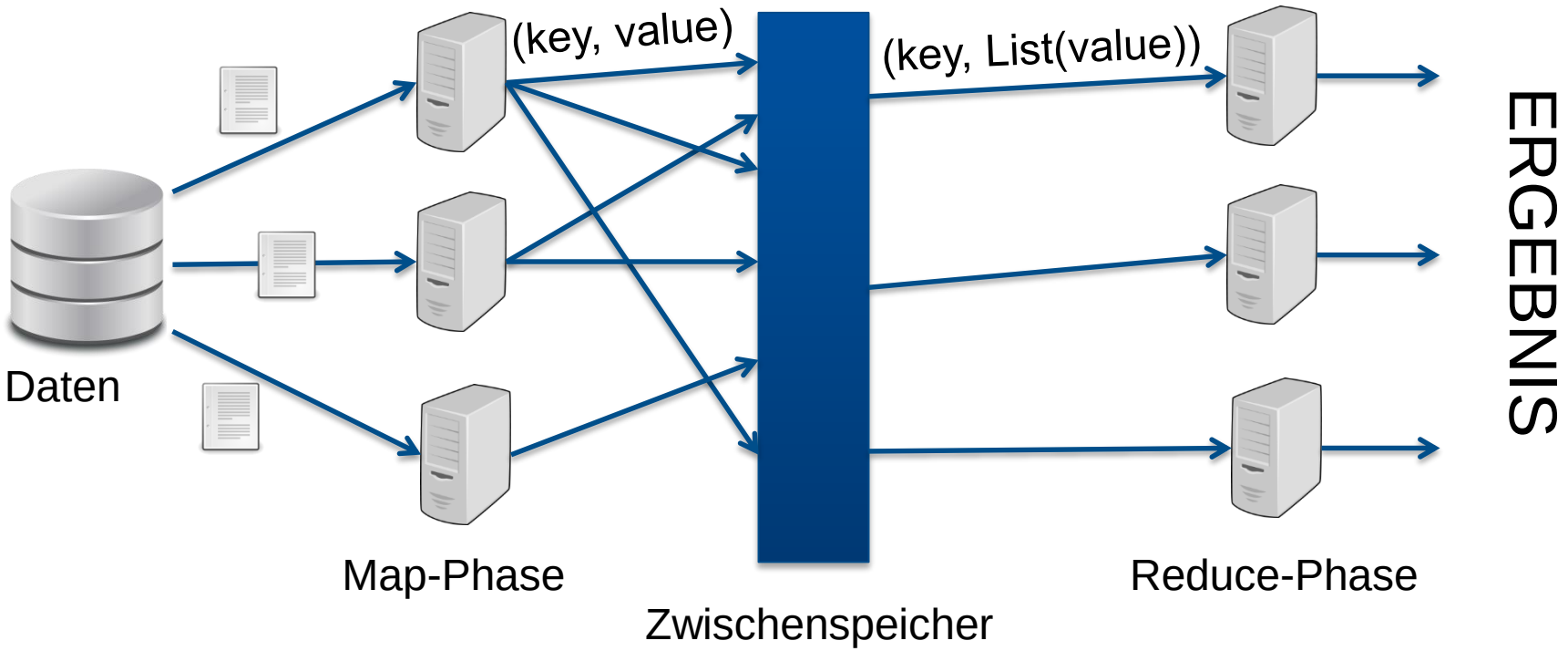
Deterministic Public-key Encryption

Hardcore Functions

Möglichkeiten von IO für Big Data verstehen und voranbringen.

Die direkte Methode: Map Reduce

- Programmiermodell zur parallelen Verarbeitung großer Datenmengen



Map Reduce: Ziele

- Map Reduce sicher (privat und authentisiert) ausführen
- z.B. mittels deterministischer Verschlüsselung
  - Geringe Entropie in aufgeteilten Datenpaketen
  - Handhabung von Integrität und Authentisierung
    - Homomorphic Signatures, Aggregate Signatures

Spezielle Krypto-Verfahren für typische MapReduce-Fälle entwickeln und anwenden