Center for Computational Sciences and Simulation **CCSS**

UNIVERSITÄT DUISBURG ESSEN

*Offen* im Denken

# Verteilte Systeme (Prof. Dr.-Ing. Torben Weis)

**GPU**

## Angriffe auf Hash-Funktion von DNSSEC

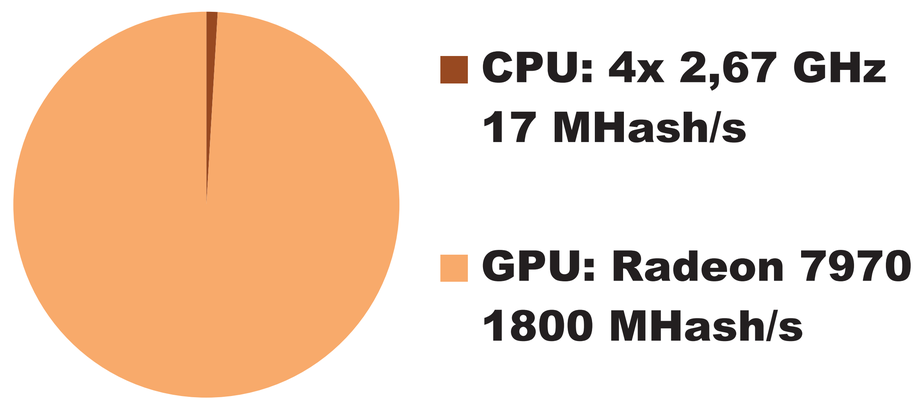
- Sicherheitserweiterung für Domain Name System
- DNSSEC signiert vorhandene Domainnamen
- Negativantwort („not found“) offenbart Namen
- Domaindaten vor Offenlegung schützen
- NSEC3: Hash-Werte statt Klartextnamen


### Schützt NSEC3 vor Offenlegung?

- NSEC3 Hash-Werte vom Server holen
- Brute-Force-Angriff aller Klartextnamen
- Optimierung mit Markov-Ketten erster Ordnung
- Wörterbuchangriff

### GPU Computing

- AMD Radeon 7970: 3,8 TFLOPS (vgl. Cray XT6m: 31 TFLOPS)
- OpenCL (ähnlich zu C)
- Für einfach parallelisierbare Probleme
- Floating Point ⇨ AMD oder NVIDIA
- Integer (z. B. Hash-Berechnung) ⇨ AMD




**CPU**

## Spawn & Merge: Hochparallele Programmierung

- Ziel: Programmiermodell für hochparallele, deterministische Anwendungen
- Zugriff auf gemeinsam genutzte Ressourcen ohne Sperrung (Locking)
- Prozesse werden dupliziert (Spawn) und arbeiten auf Kopie der Ressourcen
- Von Prozessen vorgenommene Änderungen werden zusammengeführt (Merge)
- Cray XT6m für Evaluation auf über 1000 CPU-Kernen