

# Erweiterung des RC2F für einen dynamischen Einsatz in einer flexiblen Cloud-Architektur

## Analyse eines Forschungsthemas

Paul R. Genßler – [paul.genssler@tu-dresden.de](mailto:paul.genssler@tu-dresden.de)

Dresden, 1. Juni 2017

## Ziele des Projekts

- Erweiterung RC2F
- Aufbau Testumgebung
- Messung relevanter Leistungsdaten
- Literaturanalyse für weiterführende Arbeit

1. Motivation
2. Kommunikationsinterface
3. Testumgebung
4. Sicherheit in der Cloud
5. Ausblick und Zusammenfassung

1. Motivation

2. Kommunikationsinterface

3. Testumgebung

4. Sicherheit in der Cloud

5. Ausblick und Zusammenfassung

## 1 Motivation

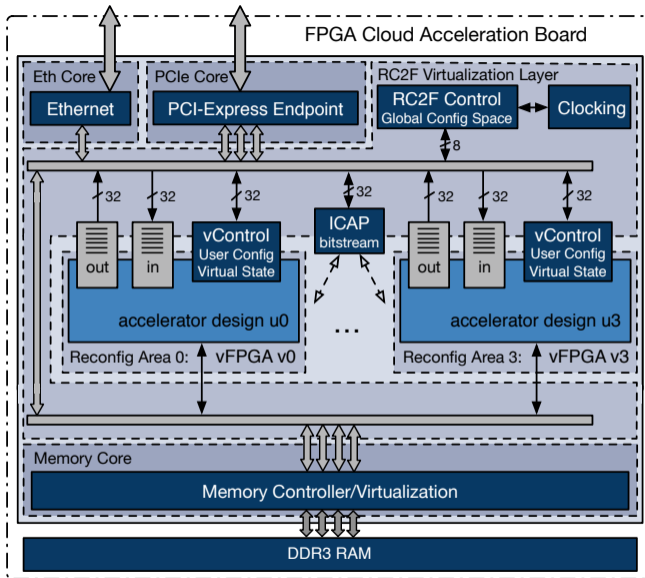
# Field Programmable Gate Array

- Flexibel konfigurierbare Hardware
- Gewinnen an Bedeutung im Data Center
  
- FPGAs in der Cloud
  - Amazon EC2 F1 Instances<sup>1</sup>, Microsoft Catapult<sup>2</sup>
  - Virtualisierung nötig
  - Erhöhung der Auslastung großer Chips
  - Reduzierung des Energieverbrauchs durch Abschaltung

---

<sup>1</sup><https://aws.amazon.com/ec2/instance-types/f1/>

<sup>2</sup>Caulfield u. a., 2016



## 1 Motivation

# Nötige Erweiterungen

- Erweitertes Kommunikationsinterface
  - Einbinden von Ethernet
  - Anbinden des On-Board DDR3 Speichers
  - Beschleunigen der PCIe Schnittstelle

## 1 Motivation

# Nötige Erweiterungen

- Erweitertes Kommunikationsinterface
  - Einbinden von Ethernet
  - Anbinden des On-Board DDR3 Speichers
  - Beschleunigen der PCIe Schnittstelle
- Sicherheit erhöhen
  - Auslesen aller Nutzerdaten möglich
  - Einfacher Diebstahl des Geistigen Eigentums
    - Nicht praktikabel für viele Nutzer



1. Motivation
2. Kommunikationsinterface
3. Testumgebung
4. Sicherheit in der Cloud
5. Ausblick und Zusammenfassung

## 2 Kommunikationsinterface

# Interface

- PCIe Schnittstelle auf 64 Bit erweitert (128 Bit möglich)
- Ethernet
  - Paketbasiertes Interface abbilden
  - Virtualisierung über verschiedene IPs
- DDR3
  - Streambasiertes Interface
  - Pagetables zur Virtualisierung
- Jeweils verschiedene Service Level Agreements realisierbar

## 2 Kommunikationsinterface

# Ressourcenauslastung

Komponente	Total LUTs	Logic LUTs	LUTRAM	BlockRAM18
PCIe	22053	14296	7682	44
Ethernet	1453	1279	167	0
DDR3	9859	8488	1352	0
Gesamt	34627	25325	9201	46
XC7VX485T	11,4 %	8,56 %	2,84 %	2,2 %

part 0 black scholes15

part 1 black scholes16

part 2 black scholes3

part 3 black scholes3

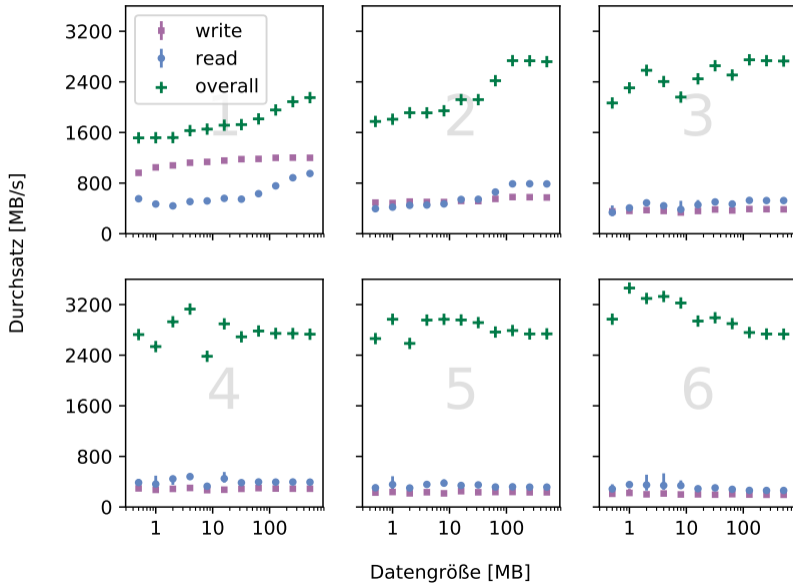
part 4 loophack

pblock static

part 5 black scholes15

pblock static

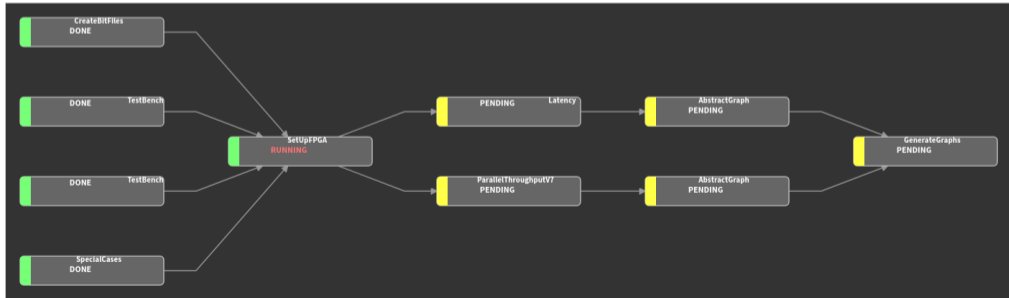
# PCIe Durchsatz mit bis zu 6 Nutzern



1. Motivation
2. Kommunikationsinterface
3. Testumgebung
4. Sicherheit in der Cloud
5. Ausblick und Zusammenfassung

## 3 Testumgebung Aufbau der Testumgebung

- Automatische Synthese, Tests, Benchmarks
- Pipeline realisiert mit Luigi Framework



1. Motivation
2. Kommunikationsinterface
3. Testumgebung
4. Sicherheit in der Cloud
5. Ausblick und Zusammenfassung



## 4 Sicherheit in der Cloud

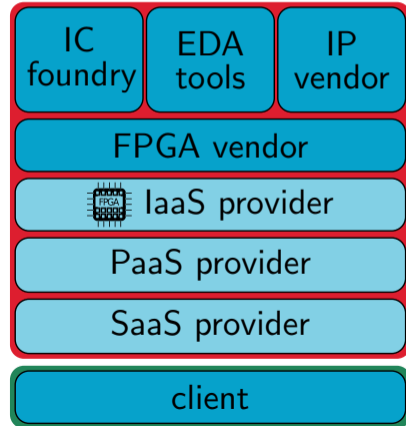
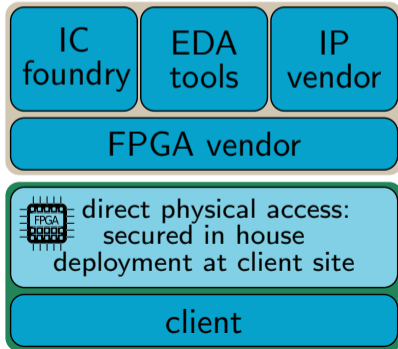
# Sicherheitsbedenken sind größtes Hemmnis

- Verlust der Herrschaft über die Daten (58 % <sup>3</sup>)
- Kein Schutz des geistigen Eigentums
- Vielschichtige Umgebung → Viele Einfallstore
- Kleinere Angriffsfläche von Hardware nutzen

---

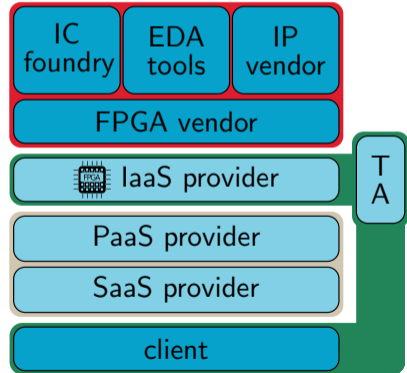
<sup>3</sup>Peter Heidkamp und KPMG AG (2016). *Cloud-Monitor 2016*.

## 4 Sicherheit in der Cloud Stand der Technik



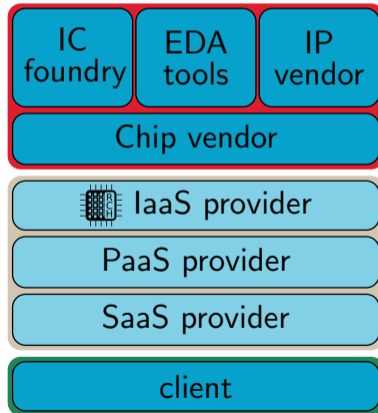
## 4 Sicherheit in der Cloud Literatur

- Trusted Platform Model (TPM)
- Homomorphe Verschlüsselung
- FPGA Sicherheitskonzept vorhanden
- Einbeziehung einer Trusted Authority (TA)
  - Kepa u. a., 2008
  - Devic u. a., 2010
  - Eguro und Venkatesan, 2012



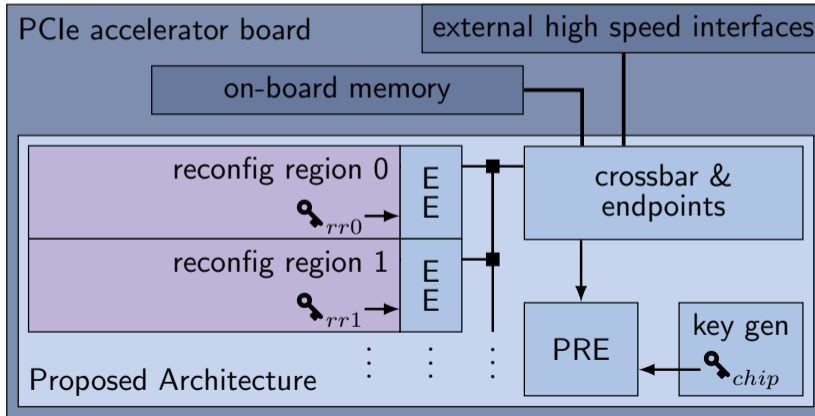
## 4 Sicherheit in der Cloud

# Entwurf einer neuen Architektur (1)



## 4 Sicherheit in der Cloud

### Entwurf einer neuen Architektur (2)



1. Motivation
2. Kommunikationsinterface
3. Testumgebung
4. Sicherheit in der Cloud
5. Ausblick und Zusammenfassung

## 5 Ausblick und Zusammenfassung

# Ausblick und Zusammenfassung

- Ausblick
  - Tiefergehende Evaluierung des Konzepts
  - Implementierung wichtiger Funktionen
  - Notwendige Architekturänderungen aufzeigen
- Zusammenfassung
  - Absolute Sicherheit nicht möglich
  - Verbesserung durch Einsatz teilweise rekonfigurierbarer Hardware
  
  - Aufbau einer automatisierten Test und Benchmark Umgebung
  - Einbindung von weiteren Schnittstellen ins RC2F

- Caulfield, Adrian M u. a. (2016). “A cloud-scale acceleration architecture”. In: *Microarchitecture (MICRO), 2016 49th Annual IEEE/ACM International Symposium on*. IEEE, S. 1–13.
- Devic, Florian, Lionel Torres und Benoit Badrignans (2010). “Secure protocol implementation for remote bitstream update preventing replay attacks on FPGA”. In: *Field Programmable Logic and Applications (FPL), 2010 International Conference on*. IEEE, S. 179–182.
- Eguro, Ken und Ramarathnam Venkatesan (2012). “FPGAs for trusted cloud computinga”. In: *Field Programmable Logic and Applications (FPL), 2012 22nd International Conference on*. IEEE, S. 63–70.
- Kepa, Krzysztof u. a. (2008). “Serecon: A secure dynamic partial reconfiguration controller”. In: *Symposium on VLSI, 2008. ISVLSI'08. IEEE Computer Society Annual*. IEEE, S. 292–297.