

# **Confidential and Privacy-Preserving Computing in Distributed Systems**

Bachelor's Thesis of

Wenzhe Vincent Cui

at the Department of Informatics

KASTEL – Institute of Information Security and Dependability

Reviewer:	Prof. A
Second reviewer:	Prof. B
Advisor:	M.Sc. C
Second advisor:	M.Sc. D

xx. Month 20XX – xx. Month 20XX

Karlsruher Institut für Technologie  
Fakultät für Informatik  
Postfach 6980  
76128 Karlsruhe

---

I declare that I have developed and written the enclosed thesis completely by myself. I have submitted neither parts of nor the complete thesis as an examination elsewhere. I have not used any other than the aids that I have mentioned. I have marked all parts of the thesis that I have included from referenced literature, either in their original wording or paraphrasing their contents. This also applies to figures, sketches, images and similar depictions, as well as sources from the internet.

**PLACE, DATE**

.....  
(Wenzhe Vincent Cui)



# **Abstract**

English abstract.



# **Zusammenfassung**

Deutsche Zusammenfassung





# Contents

<b>Abstract</b>	<b>i</b>
<b>Zusammenfassung</b>	<b>iii</b>
<b>1. Introduction</b>	<b>1</b>
1.1. Background . . . . .	1
1.2. Motivation . . . . .	1
1.3. Research Methodology . . . . .	1
<b>2. First Content Chapter</b>	<b>3</b>
<b>3. Confidential Computing</b>	<b>5</b>
3.1. Trusted Execution Environments (TEEs) . . . . .	5
3.1.1. Properties . . . . .	5
3.1.2. Confidential Computing Environments (CCEs) . . . . .	5
3.2. TEE Flavors . . . . .	5
3.2.1. Virtual-Machine-based TEE . . . . .	5
3.2.2. Process-based TEE . . . . .	6
<b>4. Privacy-Preserving Computing</b>	<b>7</b>
4.1. Multi-Party Computation . . . . .	7
4.2. Homomorphic Encryption . . . . .	7
<b>5. Case Studies</b>	<b>9</b>
5.1. Confidential Containers . . . . .	9
5.2. Marble Run . . . . .	9
5.3. Constellation Kubernetes . . . . .	9
5.4. Sharemind . . . . .	9
5.5. Veracruz . . . . .	9
<b>6. Evaluation</b>	<b>11</b>
<b>7. Conclusion</b>	<b>13</b>
<b>A. Appendix</b>	<b>15</b>
A.1. First Appendix Section . . . . .	15



# List of Figures

A.1. A figure . . . . . 15



## List of Tables



# **1. Introduction**

## **1.1. Background**

## **1.2. Motivation**

## **1.3. Research Methodology**





## **2. First Content Chapter**



## **3. Confidential Computing**

### **3.1. Trusted Execution Environments (TEEs)**

Defined by Confidential Computing Consortium.

#### **3.1.1. Properties**

- Data confidentiality
- Data integrity
- Code integrity

Depending on the specific TEE, it may also provide:

- Code confidentiality
- Authenticated Launch
- Programmability
- Attestation
- Recoverability

#### **3.1.2. Confidential Computing Environments (CCEs)**

Defined by Edgeless Systems. Trusted Execution Environment with specific capabilities:

- Runtime encryption (Data confidentiality/integrity)
- Isolation
- Remote attestation

### **3.2. TEE Flavors**

#### **3.2.1. Virtual-Machine-based TEE**

AMD SEV, Intel TDX, IBM Secure Execution and PEF, ...

#### **3.2.2. Process-based TEE**

Intel SGX, ...

Application Splitting:

- Enclave
- Host

## **4. Privacy-Preserving Computing**

### **4.1. Multi-Party Computation**

### **4.2. Homomorphic Encryption**



## **5. Case Studies**

### **5.1. Confidential Containers**

### **5.2. Marble Run**

### **5.3. Constellation Kubernetes**

### **5.4. Sharemind**

### **5.5. Veracruz**





## **6. Evaluation**



## **7. Conclusion**

...



# A. Appendix

## A.1. First Appendix Section



Figure A.1.: A figure

...