Fachhochschule Aachen

Campus Jülich

Fachbereich: Medizintechnik und Technomathematik

Studiengang: Technomathematik

Secure Multi-Party Computation for Decentralized Distributed Systems

Masterarbeit von Frederic Klein

Diese Arbeit wurde betreut von:

1. Prüfer: Prof. Dr. rer. nat. Alexander Voß
2. Prüfer: Dr. Stephan Jonas

Aachen, Oktober, 2016

Diese Arbeit ist von mir selbständig angefertigt und verfasst. Es sind keine anderen als die angegebenen Quellen und Hilfsmittel benutzt worden.

Frederic Klein .....
Unterschrift

Abstract

Abstract...

Contents

List of Figures

Chapter 1

Introduction

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Random citation [1] embeddeed in text.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

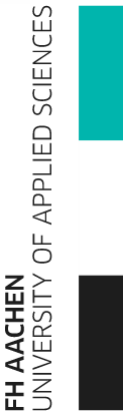

Figure 1.1: The FH Logo

Chapter 2

Foundation

2.1 Gamification and Serious Games

2.2 Distributed Systems

2.3 Secure Multi-Party Computation (SMPC)

Protocols

Frameworks

Differential Privacy

2.4 Wireless network technologies

Wireless Local Area Networks

Wi-Fi/802.11

Wireless Personal Area Networks

Bluetooth

Bluetooth Smart/Bluetooth Low Energy

Wireless Networks in Hospitals

2.5 Case Study: "The Hygiene Games" System

Chapter 3

Research

3.1 Applicability of SMPC Protocols in Decentralised Systems

Analysis of Key Factors: Computing Power, Network Data Rates and Duration of Connection

3.2 Effectiveness of SMPC Protocols in Sparse Networks

Maintaining anonymity

Strategies for Aggregation of Participants in Sparse Networks

3.3 Applicability and Requirements Analysis for the Hygiene Games

Chapter 4

Conclusion

Bibliography

[1] John Doe. *The Book without Title*. Dummy Publisher, 2100.