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

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.

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.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Contents

List of Figures

List of Acronyms

JDK Java Development Kit.

List of Symbols

$\mathbb{R}$ set of real numbers.

Chapter 1

Introduction

Research has found that "this is a direct quotation" (Doe 2100a, p. 1). Doe (2100a, p. 1) found that "this is a direct quotation". On the other hand, if the direct quotation is paraphrased, we don't need the quotes; also we use pp. for multiple, consecutive pages (Doe 2100b, pp. 35-37).

In the above paragraph we used *authoryear* as citation scheme and add a descriptive footnote.[1]

The Corporate Design section on the FH Aachen website, is rather disappointing. Using the website logo, we get a higher resolution (see figure 1.1) and use this logo for the title page.

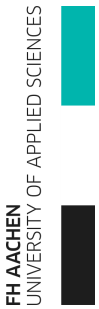

Figure 1.1: The FH Logo (*FH Aachen Logo* 2016)

[1] authoryear complies with the Harvard Reference Style

Simple formulas can be written in-line, e.g. $x^2 + 5x + 6 = 0$. Formulas, which need to be referenced in the text, should be numbered with chapter number and a continuous, 1 based counter per chapter. Let us assume our findings could be summarized as:

$$x^2 + 5x + 6 = 0, x \in \mathbb{R} \tag{1.1}$$

Seeing that our result formula (compare 1.1) is solvable, we determine the solution (see 1.2), though we avoid the automatic numbering for equations that are not referenced by using $\backslash nonumber$:

$$\begin{aligned} & x^2 + 5x + 6 && = 0 \\ \Leftrightarrow \quad & (2 + x)(3 + x) && = 0 \\ \Rightarrow \quad & 2 + x = 0 && \vee \quad 3 + x = 0 \\ \Rightarrow \quad & x = -2 && \vee \quad x = -0 \end{aligned} \tag{1.2}$$

When writing a scientific paper we might need to introduce abbreviations. When we want to use an abbreviation for a phrase, we insert the abbreviation in parentheses directly after the first usage of the phrase. We might for example describe used tools in a development process such as the Java Development Kit (JDK) version. Further references to the JDK will be in form of the acronym.

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.

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.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

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

References

Doe, John (2100a). *The Book without Title*. Dummy Publisher.

— (2100b). *The other Book without Title*. Dummy Publisher.

FH Aachen Logo (2016). URL: https://www.fh-aachen.de/fileadmin/template/pics/fh-logo-right.svg/.

Appendix A

Some name

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.