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, Dezember, 2016

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

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

In recent years gamification has become a part in many areas of our daily routine. In regard to our personal life, companies like Amazon or Runtastic can base their gamification approach on publicly sharing personal achievements and statistics to improve user commitment. In contrast, gamification concerning our work life has to satisfy much higher privacy demands. Since comparison is a key component for gamification, privacy protecting computations of system wide statistical values (for example minimum and maximum) are needed. The solution comes in the form of secure multi-party computation (SMPC), a subfield of cryptography. Existing frameworks for SMPC utilize the Internet Protocol, though access to the Internet or even a local area network (LAN) cannot be provided in all environments. Facilities with sensible measuring systems, e.g. medical devices in hospitals, often avoid Wi-Fi to reduce the risk of electromagnetic interference. To be able to utilize SMPC in environments with Wi-Fi restrictions, this thesis studies the characteristics of mobile ad hoc networks (MANET) and proposes the design of a SMPC framework for MANET, especially based on Bluetooth technology, and the implementation as a C library.

Since MANETs have a high probability for network partition, a centralized architecture for the computation and data preservation is unfavorable. Therefor a blockchain based distributed database is implemented in the framework. Typical problems of distributed systems are addressed with the implementation of algorithms for clock synchronization and coordinator election as well as protocols for the detection of computation partners and data distribution. Since the framework aims to provide distributed computations of comparable values, protocols for secure addition and secure comparison are implemented, enabling the computation of minimum, maximum and average.

bad word high acceptable here?

Devices of diverse computational power will be used to verify the applicability for wearables and Internet of Things (IoT) grade devices. Also field-tests with a smart phone ad hoc network (SPAN)(20-50 nodes) will be conducted to evaluated real life use cases. In contrast, the security of the framework and attack scenarios will be discussed. In summary, this thesis proposes a framework for SMPC for decentralized, distributed systems.

Contents

List of Figures

List of Tables

List of Acronyms

IoT Internet of Things.

LAN local area network.

MANET mobile ad hoc networks.

SMPC secure multi-party computation.

SPAN smart phone ad hoc network.

Chapter 1

Introduction

5-10%, including motivation, general audience

In the last couple of years gamification has found it's way into many areas of our daily life. In regard to our personal life, companies like Amazon or Runtastic can base their gamification approach on publicly sharing personal achievements and statistics to improve user commitment. In contrast, gamification concerning our work life can have much higher privacy demands. Since comparison is a key component for the gamification approach, privacy protecting computations of system wide statistical values (for example minimum and maximum) are needed. The solution comes in the form of SMPC, a subfield of cryptography.

Existing frameworks for SMPC utilize the Internet protocol, though access to the Internet or even a LAN cannot be provided in all environments. Especially many hospitals tend to avoid Wi-Fi to reduce the risk of electromagnetic interference with medical devices.

To be able to utilize SMPC in environments with Wi-Fi restrictions, this thesis studies the characteristics of mesh-networks and proposes describes the design of a SMPC framework for mesh-networks.

Context

Restatement of the problem

Restatement of the response

Roadmap

1.1 Case Study: "The Hygiene Games"

Gamification

Wireless Networks in Hospitals

Chapter 2

Background

10-15%; thorough review of the state of the art; informed audience

In this chapter a general understanding of SMPC and the key features of MANETs is established.

First the general idea for SMPC is introduced. Since secret sharing is used for the development of SMPC protocols, Shamir's secret sharing scheme is presented, as well as random numbers. Before protocols for secure addition and secure comparison with passive security are introduced, the term security is defined and existing framework for SMPC are discussed.

To be able to define requirements for the new framework, the key features of MANETs are identified, with a focus on the wireless technology standards Bluetooth and Wi-Fi.

2.1 Secure Multi-Party Computation

SMPC is a subfield of cryptography. general idea

For SMPC two types of adversaries have to be considered: semi-honest adversaries and malicious adversaries. Semi-honest adversaries "follow the protocol specification, yet may attempt to learn additional information by analyzing the transcript of messages received during the execution" (Aumann and Lindell 2007). Malicious adversaries "are not bound in any way to following the instructions of the specified protocol" (Aumann and Lindell 2007). SMPC protocols that can tolerate semi-honest parties (up to a specific threshold) provide semi-honest or passive security. SMPC protocols that are secure against malicious adversaries achieve malicious or active security. Cramer, Damgard, and Nielsen (2015, p.) also differentiate between unconditional or perfect security and computational security:

discuss passive and active security

4.3.4

if security can be proven for an adversary with unlimited computation power a protocol has unconditional security. In contrast, computational security can only be proven for a polytime adversary.

simple example

Secret Sharing

Cramer, Damgard, and Nielsen (2015, p.) describe secret sharing schemes as the main tool to build a SMPC protocol with passive security. In 1979 Adi Shamir described a (k, n) threshold scheme for sharing secret data D: "Our goal is to divide D into n pieces D_i, ..., D_n in such a way that: (1) knowledge of any k or more D_i pieces makes D easily computable; (2) knowledge of any $k-1$ or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely)." (Shamir 1979) Shamir's secret sharing scheme is based on polynomials of degree $k-1$ with $a_0 = D$ (compare 2.1).

compare to book version

$$q(x) = D + a_1 \cdot x + ... + a_{k-1} \cdot x^{k-1} \tag{2.1}$$

To divide D into n pieces the polynomial is evaluated: $D_i = q(i),\ i = 1, ..., n$.

recombination with Lagrange

For cryptographic protocols it is not practical to work with real arithmetic, instead a finite field is used. Shamir (1979) specifies that modular instead of real arithmetic is used. A prime p with $p > D, p > n$ is selected and used to define the set $[0, p)$. "The coefficients $a_1, ..., a_{k-1}$ in $q(x)$ are randomly chosen from a uniform distribution over the integers in $[0, p)$, and the values $D_1, ..., D_n$ are computed modulo p." (Shamir 1979, p. 613) (compare 2.2)

$$q(x) = D + a_1 \cdot x + ... + a_{k-1} \cdot x^{k-1} \mod p \qquad D,\ a_i \in [0, p)\ , \quad p \in \mathbb{P} \tag{2.2}$$

Cramer, Damgard, and Nielsen (2015, p.) declare the set restricted by p as $\mathbb{Z}_p = \{0, 1, ..., p-1\}$. They also use the notion *secret* S for the data to be shared and *shares* s_i for the computed pieces of the secret.

compare to book version 1.3.1

The reconstruction of a secret S can be done using Lagrange interpolation (compare

describe number off messages, usage of threshold as trade-off between security and performance

2.3).

$$S = \sum_i s_i \prod_{i \neq j} \frac{-x_j}{x_i - x_j} \mod p \tag{2.3}$$

k shares s_i are needed to reconstruct S, so only the associated values for i are used in the Lagrange interpolation.

Example Computation

Consider the following task: a secret $S = 8$ is supposed to be shared among $n = 4$ parties P_i. The threshold for the number of needed shares for the reconstruction of the secret shall be $k = 3$ (public).

First a prime p has to be chosen, which has to be larger than the secret ($p > S$) and the number of parties ($p > n$): $p = 17$ (public)

Since $k = 3$, the polynomial has a degree of $k - 1 = 2$ (compare 2.4).

$$f(x) = S + a_1 \cdot x + a_2 \cdot x^2 \mod p \tag{2.4}$$

The coefficients are selected randomly uniformly out of $\mathbb{Z}_p = \{0, 1, ..., p - 1\} = \{0, 1, ..., 16\}$: $a_1 = 13$ and $a_2 = 4$ and the shares s_i are computed (compare 2.5).

$$f(x) = 8 + 13 \cdot x + 4 \cdot x^2 \mod 17 \tag{2.5}$$

$$\Downarrow$$

$$f(x_1) = f(1) = 25 \mod 17 = 8 = s_1$$

$$f(x_2) = f(2) = 50 \mod 17 = 16 = s_2$$

$$f(x_3) = f(3) = 83 \mod 17 = 15 = s_3$$

$$f(x_4) = f(4) = 124 \mod 17 = 5 = s_4$$

If parties P_2, P_3 and P_4 pool their shares, they can reconstruct the secret S using

Lagrange interpolation (using also the public information: $p = 17$):

$$
\begin{aligned}
S &= \sum_i s_i \prod_{i \neq j} \frac{-x_j}{x_i - x_j} \mod 17 \qquad \textit{with } i, j \in \{2, 3, 4\} && (2.6) \\
&= s_2 \cdot \frac{-x_3}{x_2 - x_3} \cdot \frac{-x_4}{x_2 - x_4} + s_3 \cdot \frac{-x_2}{x_3 - x_2} \cdot \frac{-x_4}{x_3 - x_4} + s_4 \cdot \frac{-x_2}{x_4 - x_2} \cdot \frac{-x_3}{x_4 - x_3} \mod 17 \\
&= 16 \cdot \frac{-3}{2-3} \cdot \frac{-4}{2-4} + 15 \cdot \frac{-2}{3-2} \cdot \frac{-4}{3-4} + 5 \cdot \frac{-2}{4-2} \cdot \frac{-3}{4-3} \mod 17 \\
&= 96 - 120 + 15 \mod 17 \\
&= -9 \mod 17 && (2.7) \\
&= 8
\end{aligned}
$$

Note: in cryptography $a \mod n$ for $a < 0$ (negative dividend) is calculated by adding a multiple of n, so that $m * n + a > 0$: e.g. $-9 \mod 17 = (17 - 9) \mod 17$ (compare 2.7).

Random Numbers

random numbers important for cryptography: selection of coefficients in secret sharing, public key generation, ...; RNG in different environments; entropy

lib will require a callback for random number generator -¿ maybe mention with outlook for requirements

Differential Privacy

Secure Addition Protocol

keep this? definition of security

extended ring (Sheikh, Kumar, and Mishra 2009); number of messages

secure addition (Cramer, Damgard, and Nielsen 2015); number of messages

secure addition with verification (Cramer, Damgard, and Nielsen 2015); number of mes-

Secure Comparison Protocol

Existing Frameworks

2.2 Mobile Ad Hoc Networks

- continuously self-configuring

- self-forming
- self-healing
- infrastructure-less
- peer-to-peer
- Difference to mesh: mobility of nodes

Example: firechat in SPAN

Comparison to Wi-Fi Direct

- SPAN support multi-hop relays
- Wi-Fi Direct since Android 4.0
- Wi-Fi Direct: Soft AP

Bluetooth Based MANET

Wi-Fi Based MANET

Chapter 3

Design

15-20%; explains complete processing chain; explains what methods are used; for someone that wants to know what was done in detail

3.1 Requirements

use cases, process description, resulting requirements

3.2 Distributed Computing

Coordinator Election

Clock Synchronization

Distributed Databases

3.3 Applicability of SMPC Protocols in MANETs

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

Effectiveness of SMPC Protocols in Sparse Networks

Maintaining anonymity

Strategies for Aggregation of Participants in Sparse Networks

3.4 Architecture

UML; module structure

Chapter 4

Implementation

15-20%; details on the implementation; for someone who wants to continue the work

4.1 Communication Layer

Pairing-less Connection

Secure Channel

https://developer

4.2 SMPC Module

4.3 Data Storage and Distribution

4.4 Interfacing the Library

Configuration

Usage in C

Usage in Android

Chapter 5

Evaluation

5-15%; outcome; how was it tested; for supervisor

5.1 Testing Tools

CUnit; JUnit; Simulation?

centralized client-server test app for android: trigger test runs, report results (measured execution time, correctness)

5.2 Examination of Computation Time Dependent on Computing Power

5.3 Examination of Computation Time Dependent on Number of Participants

Chapter 6

Discussion

5-15%; outcome for a design-reader

Chapter 7

Conclusion

5-10%; outcome for a introduction-reader

References

Aumann, Yonatan and Yehuda Lindell (2007). "Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries". In: *Theory of Cryptography: 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007. Proceedings*. Ed. by Salil P. Vadhan. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 137–156. ISBN: 978-3-540-70936-7. DOI: 10.1007/978-3-540-70936-7_8. URL: http://dx.doi.org/10.1007/978-3-540-70936-7_8.

Cramer, Ronald, Ivan Bjerre Damgard, and Jesper Buus Nielsen (2015). *Secure Multiparty Computation and Secret Sharion*. Cambridge University Press.

Shamir, Adi (1979). "How to Share a Secret". In: *Communications of the ACM*.

Sheikh, Rashid, Beerendra Kumar, and Durgesh Kumar Mishra (2009). "Privacy Preserving k Secure Sum Protocol". In: *CoRR* abs/0912.0956. URL: http://arxiv.org/abs/0912.0956.

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.