

Designing a secure messaging application with biometric identification computing on homomorphic encrypted data.

Table of contents.

Alexander Stæhr Johansen, 201905865@post.au.dk
Henrik Tambo Buhl, 201905590@post.au.dk

16/02/2022

Introduction

The purpose of this document is to introduce the second draft of the table of contents. Prior to the table of contents is the cover page and the abstract.

Tentative table of contents

1. Introduction

Purpose

Problem definition

Related work

2. Methodology

Software development process

Eigenfaces

PCA

Power method

Eigen shift procedure

Goldschmidt's algorithm

Eigenface facial recognition

Vector operations

Homomorphic encryption and CKKS

Homomorphic Eigenfaces

HPCA

Homomorphic power method

Homomorphic eigen shift procedure

Homomorphic Goldschmidt's algorithm

Homomorphic Eigenface facial recognition

Homomorphic vector operations

R2 score

Signal protocol

XEdDSA and VEdDSA

X3DH

Double Ratchet

Sesame

3. Implementation

Homomorphic Eigenfaces

Server application

Client application

4. Results

5. Conclusive remarks

6. Future work

7. References