

# A Secure and Privacy-Friendly Logging Scheme

Cloud Cyber Security and Privacy: Readiness for the Next Decade

---

Andreas Aßmuth<sup>1</sup>, Robert Duncan<sup>3</sup>, Simon Lieb<sup>1,2</sup>, and Matthias Söllner<sup>1</sup>



<sup>1</sup> Technical University of Applied Sciences  
OTH Amberg-Weiden, Amberg, Germany

<sup>2</sup> PhD Student at Abertay University, Dundee, UK

<sup>3</sup> University of Aberdeen, Aberdeen, UK



1495



UNIVERSITY OF  
ABERDEEN

April 18, 2021 to April 22, 2021

# About me

Professor of Computer Networks and Mathematics

Dean of Studies (Department of Electrical Engineering, Media and Computer Science)

Teaching:

Mathematics, Computer Networks, Cryptography, Coding Theory, Information Security

Research:

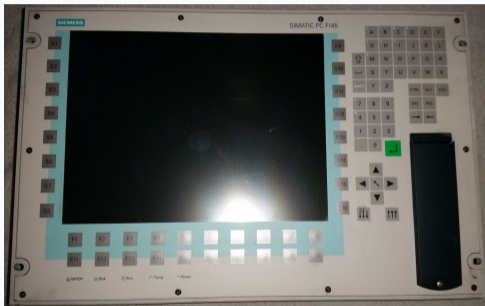
Applied Cryptography, Information Security, Ethical Hacking

IARIA Fellow



- 1 Introduction
- 2 Logging Strategies
- 3 Proposed Logging System
- 4 Conclusion and Future Work

# Introduction Authentication Required



Authentication ensures that only authorised persons may use computers or machines.

## Microsoft productivity score feature criticised as workplace surveillance

Tool allows managers to use Microsoft 365 to track their employees' activity



**The Guardian**

Source:

A. Hern, "Microsoft productivity score feature criticised as workplace surveillance", The Guardian, [Online], 2020-11-26.

Features and services that are used to track individual actions to single employees can violate their privacy.

**PRESS RELEASE**

The Hamburg Commissioner for  
Data Protection and Freedom of Information

October 1st, 2020

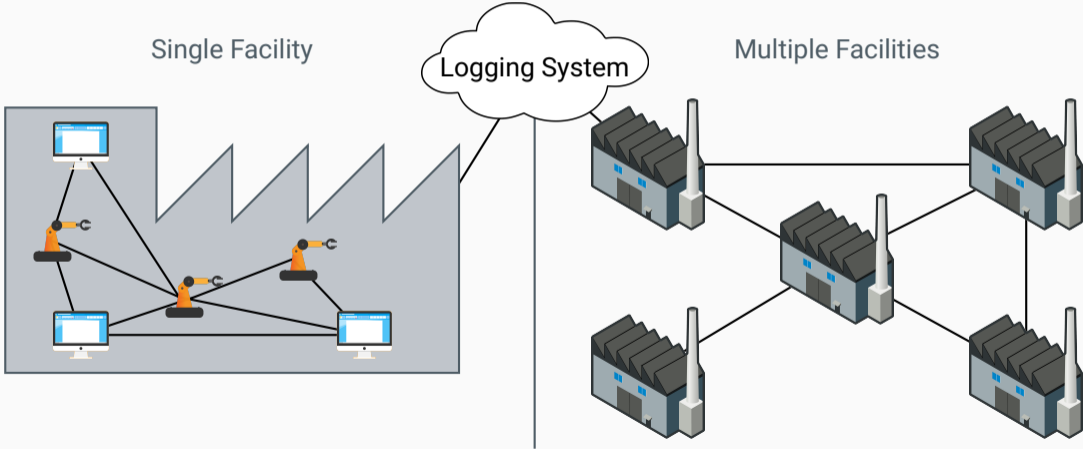
**35.3 Million Euro Fine for Data Protection Violations in  
H&M's Service Center**

Source:

Hamburg Commissioner, Ed., "35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center", Datenschutz-Hamburg GDPR fine for GDPR employee data breach, Press Release [Online], 2020.

# Introduction

**Goal:** Find a solution to this problem, to be capable of tracking down individuals without violating their privacy.



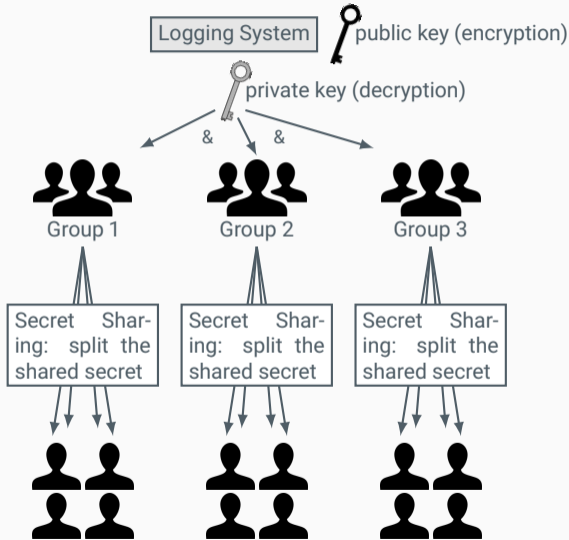
- Logging is carried out to provide an audit trail of all activities involved in running the system. In the event of a disaster, the audit trail may be used to restore the records.
- Logging system is a high-value target for attackers.
- Ensure that logging data cannot be manipulated or deleted!

- Basic idea is to ensure that we can only ever add new records to the database.
- Database entries are permanent records which store any information related to the authentication of employees.
- Goal: retain permanency of all such transactions ➡ audit trail of all transactions
- Data is encrypted to fulfil the demanded privacy constraints.

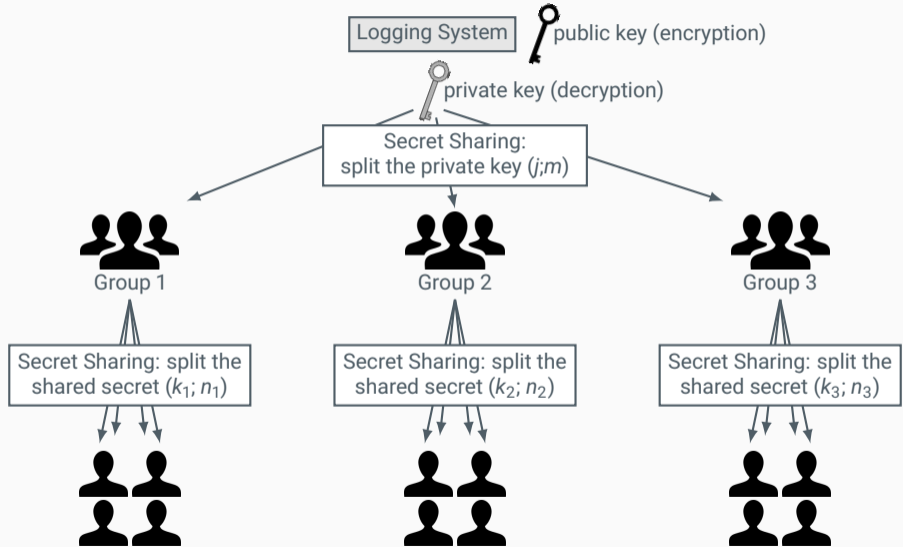


SageMath Demo!

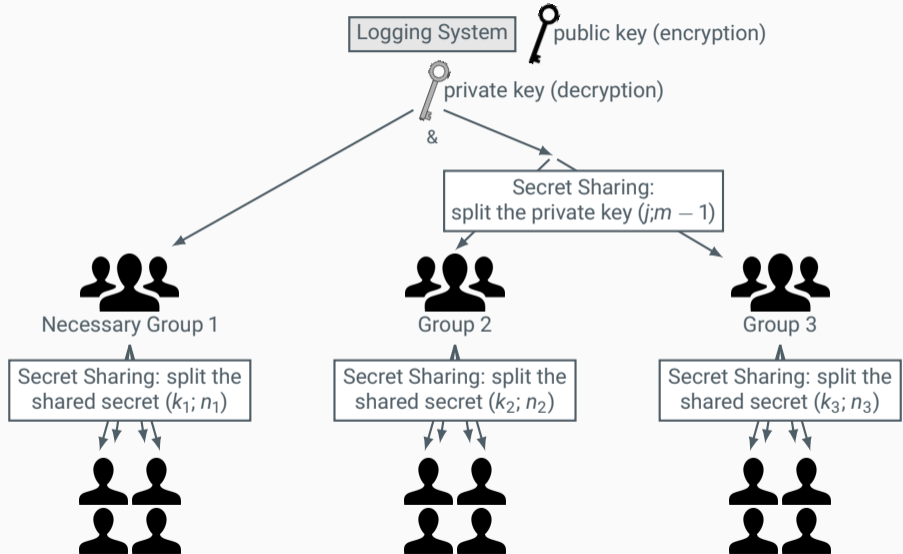
# Proposed Logging System



# Proposed Logging System Adaptability (1)



# Proposed Logging System Adaptability (2)



# Conclusion and Future Work

- Proposed logging approach is highly secure and provides privacy.
- Works for companies with only one, but also for those with multiple facilities
  - ☞ Cloud-ready solution
- Next step: proof-of-concept implementation as a collaboration between the two universities
- Performance? Immutable database? Secret Sharing Scheme?
- Key-related issues: distribution, revocation, etc.

