Kick-off: Applied Cryptography

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

Georg Bramm
georg.bramm@aisec.fraunhofer.de

Mark Gall
mark.gall@aisec.fraunhofer.de

Martin Schanzenbach
martin.schanzenbach@aisec.fraunhofer.de

January 30, 2018

Outline

1. Organization

2. Requirements

3. Grading

4. Time Table

5. Topics

6. Literature Research

7. Next Steps

Organization

The seminar will be organized as a scientific conference:

1. Familiarization phase (3 Weeks)
2. Writing phase (7 Weeks)
3. Review phase (2 Weeks)
4. Improvement phase (2 Weeks)
5. Talk preparation (1 Week)
6. Talk and Discussion

Requirements

- Report Elaboration
  - Delivery of a scientific paper with 10-12 pages in length
  - Usage of LaTeX is mandatory
  - Formatting with the LaTeX-Style of Springer (LNCS)
- Review
  - Each one of you creates two anonymous reviews
  - Review template will be provided
  - Approximately one page in LaTeX
- Presentation
  - Preparing of the presentation
  - 30-45 minutes presentation
  - 15 minutes discussion

Grading

The Grading is comprised of all contributions to this seminar and is composed of:

1. Report (50%)
2. Presentation (30%)
3. Delivered reviews (15%)
4. Participation and discussion (5%)

Time Table

30.01.18	Kick-off meeting (today)
01.03.18	Send email with three topic choices (ranked)
06.03.18	Anouncement of topic assignment
23.04.18	Deadline for report outline submission
27.04.18	Status report (attendance mandatory)
15.06.18	Deadline for report (pre-final) submission
18.06.18	Review Assignments
29.06.18	Deadline for review submission
13.07.18	Deadline for final report submission
18.07.18	Deadline for presentation submission
19+20.07.18	Presentations and discussion

Before we go on....

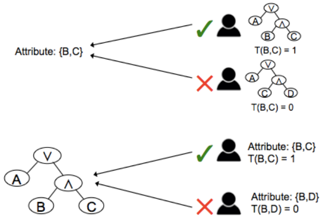
... any questions so far?

Topics

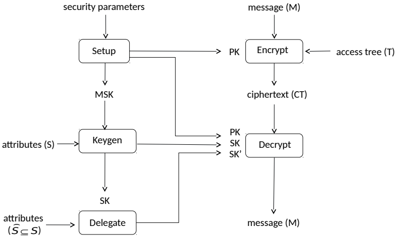
- Pairing-Based Cryptography
  - Decentralized Attribute-Based Encryption (ABE) Schemes
  - Revocation Techniques in ABE (e.g. Proxy Re-encryption)
- Property-preserving Encryption on unstructured data
  - Graph Privacy
  - NoSQL Encryption
- Applications of zero-knowledge techniques
  - Secure cloud computing (Verifiable computation)
  - Identity and Access Management (Privacy-preserving attribute-based credentials)
  - Blockchains (zkSNARKS, Bulletproofs)
- Secure Multiparty Computation
  - Oblivious Transfer und Oblivious Transfer Extensions
  - optimizing Yaos Garbled Circuits
  - MPC with Malicious Adversaries
- Methods and applications of Differential Privacy
- Similarity Search and Wildcards in Searchable Encryption

Applied PBC: ABE

- Attribute Based Encryption (ABE)
  - ABE is a type of public-key encryption based upon PBC.
  - Keys and ciphertexts are dependent upon attributes matching a policy.
  - Mostly two flavors: KP-ABE and CP-ABE



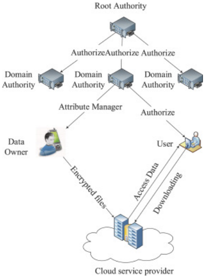
KP-ABE and CP-ABE matching



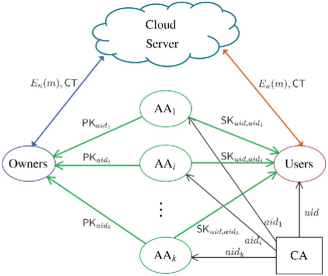
CP-ABE high level

Applied PBC: ABE

- Decentralized ABE Schemes
  - ABE systems are usually centralized.
  - The topic here is to research existing decentralized approaches.
  - How is attribute handling managed ?
  - Do ABE Authorities need to coordinate ?
  - Does this affect the universe of attributes ?
  - Can attributes be "mixed" ?
  - and so on...



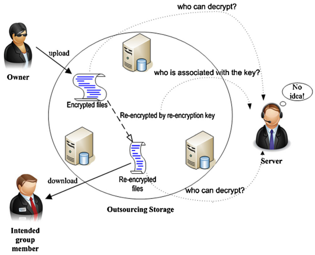
decentral ABE



decentral ABE

Applied PBC: ABE

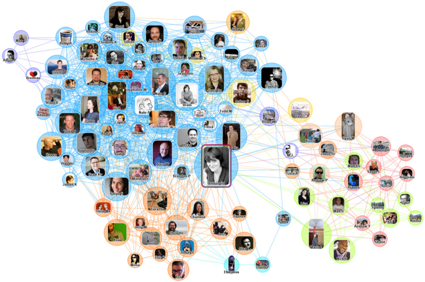
- Revocation Techniques in ABE (e.g. Proxy Re-encryption)
  - ABE suffers from the non-existence of key/attribute revocation mechanisms.
  - Revocation is a well-studied but nontrivial problem, and even more challenging in ABE systems.
  - Different approaches exist: time attribute, broadcast encryption, proxy re-encryption
  - The goal here is to research and compare existing approaches.



Proxy re-encryption

Property-preserving Encryption on unstructured data

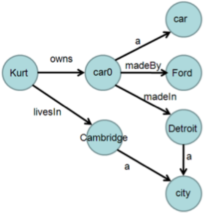
- Graph privacy
  - This topic is about Graphs.
  - Graphs are used for example in social networks, maps, cell biology, and so on...
  - Graph privacy focuses on performing (encrypted) graph queries on encrypted graphs.
  - Which queries are possible ?
  - What is leaked ?
  - Research the current state of the art and compare the current innovations.



Social graph

Property-preserving Encryption on unstructured data

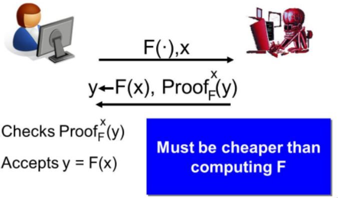
- NoSQL privacy
  - The previous topic was about Graphs.
  - But there are also other types of NoSQL data stores:
    - Wide colum stores
    - Triplestore or RDF
    - Multi modal databases
    - and so on...
  - Research the current state of art and the potential regarding encryption in those kinds of NoSQL databases.



directed graph from a Triplestore

Applications of ZK: Verifiable Computation

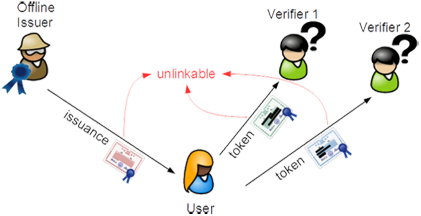
- Useful for Cloud computing
- Allows to offload a computation to an untrusted client
- Result of computation(s) are still verifiable
- Goals:
  - Research current state of the art
  - Get an understanding of the proposed systems
  - Discussion of systems and comparison



Verifiable Computation

Applications of ZK protocols: IAM

- Use-case IAM: Authorization using attribute-based credentials (ABC) where the holder of credentials must disclose the credential (e.g. age, sex, ...)
- Privacy-preserving ABCs (PP-ABC) use ZK proofs to allow authorization without disclosing actual information
- Goals:
  - Research current state of the art (uProve, Idemix)
  - Get an understanding of the proposed systems
  - Discussion and comparison



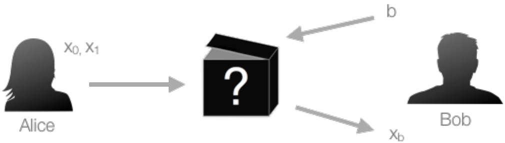
Idemix authentication

Applications of ZK protocols: Blockchains

- Blockchains do not inherently provide data confidentiality
- Contracts in the blockchain are not executed interactively between two parties, the ledger is an indirection layer
- Classical interactive ZK-proofs are not usable due to resource restrictions in blockchains
- Succinct non-interactive arguments of knowledge (SNARKS) can be used non-interactively
- SNARKS can be (more or less trivially) used for ZK proofs ⇒ zkSNARKS
- Goals:
  - Research the current state of art and its applications (zkSNARKS, Bulletproofs, zCash, Ethereum)
  - Get an understanding of the proposed systems
  - Discussion of practicality and viability for e.g. PP-ABCs

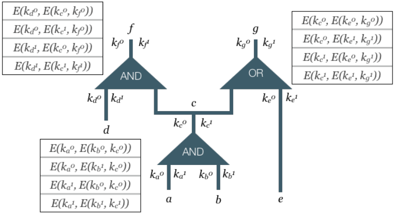
Secure Multiparty Computation

- Oblivious Transfer and OT Extensions
  - Used to exchange information with certain restrictions
  - Basis for 2 important MPC protocols:
    - Yao's Garbled Circuits
    - GMW protocol
  - OT extension allows to compute several OTs at once
  - Research and Compare different OT protocols and OT extensions according to adversary model, performance and capabilities



Secure Multiparty Computation

- Optimizing Yao's Garbled Circuits
  - (Probably) most famous MPC protocol
  - Original protocol is not very efficient
  - Since then lots of optimizations have been developed
  - Research which optimizations exist
  - Compare them and describe their influence on performace of GC
  - Check which optimizations work well together and which don't.

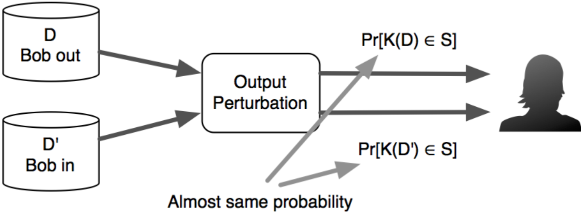

$E(k_d^0, E(k_c^0, k_f^0))$
$E(k_d^0, E(k_c^1, k_f^0))$
$E(k_d^1, E(k_c^0, k_f^0))$
$E(k_d^1, E(k_c^1, k_f^1))$
f
k_f^0
k_f^1
AND
k_d^0
k_d^1
d
g
k_g^0
k_g^1
OR
$E(k_c^0, E(k_e^0, k_g^0))$
$E(k_c^0, E(k_e^1, k_g^1))$
$E(k_c^1, E(k_e^0, k_g^1))$
$E(k_c^1, E(k_e^1, k_g^1))$
k_e^0
k_e^1
c
k_c^0
k_c^1
AND
$E(k_a^0, E(k_b^0, k_c^0))$
$E(k_a^0, E(k_b^1, k_c^0))$
$E(k_a^1, E(k_b^0, k_c^0))$
$E(k_a^1, E(k_b^1, k_c^1))$
k_a^0
k_a^1
k_b^0
k_b^1
a
b
e

Secure Multiparty Computation

- MPC with Malicious Adversaries
  - MPC protocols usually assume honest but curious adversaries
  - Handling malicious adversaries is more difficult
  - Research MPC protocols that can handle malicious adversaries and describe the techniques used to achieve this
  - Compare the protocols and the techniques used

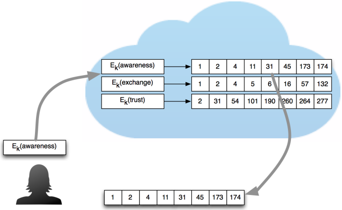
Differential Privacy

- Methods and Applications of Differential Privacy
  - Not really Cryptography
  - Privacy-preserving Data analysis
  - Allow learning statistics about the population from a dataset but not about the individual
  - Research the current state of the art, the methods used to achieve Differential Privacy and its potential application



Searchable Encryption

- Similarity Search and Wildcards in Searchable Encryption
  - Searchable Encryption allows searching in encrypted data
  - SE Protocols started out with single keyword searches
  - Protocols for more complex queries have been developed (Boolean Queries, Range Queries, etc.)
  - Research the current state of the art of similarity search and wildcard searches in Searchable Encryption and compare the protocols



E_k(awareness) → 1 | 2 | 4 | 11 | 31 | 45 | 173 | 174

E_k(exchange) → 1 | 2 | 4 | 5 | 6 | 16 | 57 | 132

E_k(trust) → 2 | 31 | 54 | 101 | 190 | 260 | 264 | 277

E_k(awareness)

1 | 2 | 4 | 11 | 31 | 45 | 173 | 174

Topic assignment

After matching phase we’ll ask you to send your 3 top choices via email

Literature Research

- Objective: Get a comprehensive overview of the topic
  - You'll get initial literature from your supervisor
  - Initial literature serves as basis for **your own** literature research
  - Good Strategy: Check sources and follow-up work of relevant papers
  - Priorize the literature you've found, including the initial literature. You might even omit or replace some of it
  - Keep in touch with your supervisor

- Find more literature
  - Books, Library
  - Citeseer, Springerlink, ACM Digital Library, IEEE Digital Library
  - Google Scholar, Scientific Commons, CiteULike
  - Use the LRZ proxy in order to gain access

Next Steps

- Matching and Topic assignment
  - Matching concludes 21.02.2018. After that we'll get in touch with the participants
  - Participants send top 3 topics via email, we'll assign the topics
- Familiarization phase
  - Literature research
  - Get an overview of your topic
  - Create report structure
- Intermediate meeting (27.04.2018)
  - Participants present the status of their research

Q&A

Q&A ?