M.Sc.-Thesis: Asymmetric DC-Nets versus Other Algorithms to Preserve Users' Privacy

Telecooperation Lab

TECHNISCHE UNIVERSITÄT DARMSTADT

Motivation

Asymmetric DC-Nets have the following technical features:

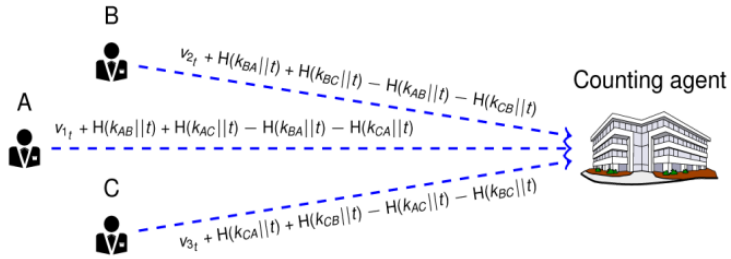
1) all properties of symmetric DC-Nets, with exception of unconditional security; 2) scalable ; 3) security is based on trapdoor function; 4) processing time has complexity at most polynomial; 5) participants can use permanent keys; 6) participants send the minimal number of messages; 7) they do not need to rely on TTP; 8) they can sign their messages; 9) verifiable.

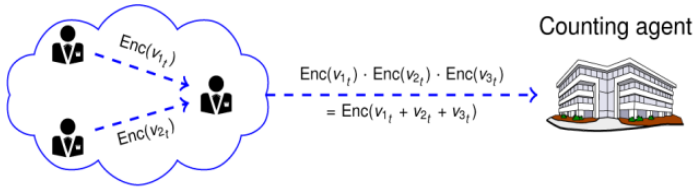
Goals

In general, asymmetric DC-Nets are more efficient than symmetric DC-Nets and even more efficient than additive homomorphic encryption.
Moreover, similarly to commitments, participants using asymmetric DC-Nets can prove their messages sent.
The main goal is to compare asymmetric DC-Nets with other algorithms used in privacy-preserving protocols and survey the differences between them.

Abstract

In 1988, David Chaum introduced the dining cryptographers problem and the so-called symmetric DC-Net protocol, which enables participants to keep their privacy and to reveal information of them. This year, we expanded the concept and introduced the asymmetric DC-Nets.





Type

Analysis	■■■■■
Empiricism	■■■□□
Implementation	■■□□□
Literature Research	■■■■□

Vision

Asymmetric DC-Nets may be used in many areas of application.

This work will make a fundamental contribution to the theoretical basis of privacy and security in many areas of application.

Fábio Borges | Telekooperation | Raum: S2|02 A 121 | Tel: (6151)16 - 2259| fabio.borges@cased.de

23.10.2014