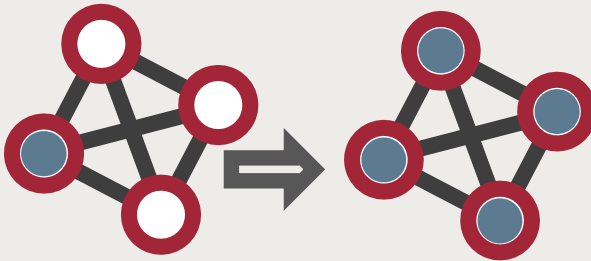


Evaluation von Threshold Cryptography für k-anonyme Dining Cryptographer Netzwerke



Bachelorarbeit	12 LP
Masterarbeit	30 LP

Dining Cryptographer Netzwerke bieten eine Möglichkeit um in einer Gruppe anonym eine Nachricht an alle zu verbreiten. Diese Konstruktion benötigt jedoch sehr viele Nachrichten und erzeugt daher viel Overhead.

Um die Effizienz dieser Netzwerke zu verbessern, haben von Ahn, et al. das Konzept der k -Anonymität auf sie angewandt: Kleinere Gruppen im Gesamtnetzwerk erlauben eine Einschränkung der Anonymität, erzeugen jedoch deutlich weniger Overhead.

Um die k -Anonymitätsgarantie zu stärken, bietet die Kryptografie das Konzept der Threshold-Kryptografie an: Nur wenn ausreichend Nutzer sich beteiligen, kann die Nachricht entschlüsselt werden.

Ziel dieser Arbeit ist es, die Umsetzung dieser Technik für k -DC Netze zu untersuchen.

Erfahrung in C++, Python und Netzwerkprogrammierung kann hilfreich sein.

This project can also be completed in English. Please contact me for further details.

David Mödinger | david.moedinger@uni-ulm.de | 027-3211

Bei Interesse und für weitere Details kontaktieren Sie mich oder kommen einfach unverbindlich vorbei.

