Fakultät für Informatik
Institut für Anthropomatik
Lehrstuhl für Intelligente Sensor-Aktor-Systeme (ISAS)
Prof. Dr.-Ing. Uwe D. Hanebeck

Masterarbeit:

Endgültiges Universalfilter

Die moderne Welt verlässt sich immer mehr auf durchgehend verfügbare Informationstechnologien, und dadurch steigt der Bedarf nach Informationssicherheit und v.a. Datenschutz kontinuierlich an. Sowohl Privatpersonen, als auch Unternehmen sind daran interessiert, kostenintensive Verarbeitung großer Datenmengen, u.a. von Messwerten, in die „Cloud“ auszulagern, ohne dabei ihre Firmengeheimnisse an ihre Betreiber bzw. an die Behörden preiszugeben.

Das Kalman-Filter ist einer der grundlegenden Bausteine der modernen Signalverarbeitung, und eine beweisbar sichere Implementierung davon würde einen großen Fortschritt auf dem interdisziplinären Forschungsgebiet der sicheren Signalverarbeitung darstellen. 2014 hatten Gonzalez-Serano et al. bereits eine ebensolche Implementierung vorgeschlagen, die auf der sog. teilhomomorphen Verschlüsselung basierte, allerdings ohne eine formale Analyse der Sicherheit und der Komplexität ihres Protokolls vorzunehmen.

Das Ziel dieser Masterarbeit ist es, die bisherige Erkenntnisse zu den datenschutzerhaltenden Umsetzungen des Kalman-Filters zu sammeln und sie in Bezug auf Datensicherheit, Genauigkeitsverlust, und Rechen-, Speicher- und Netzwerkeffizienz zu analysieren. Da das Protokoll von Gonzalez-Serano et al. sich nur bedingt für den Cloud-Einsatz eignet, ist außerdem eine neue Lösung für den ebensolchen Einsatz, ggf. mit schwächeren Sicherheitsgarantien, zu erarbeiten und prototypisch umzusetzen. Dabei sollen v.a. Synergien zwischen den Randbedingungen der Signalverarbeitung und der formalen Kryptographie gesucht und verwertet werden.

Aufgaben:

- Überblick der aktuellen Literatur zu der datenschutzerhaltenden Signalverarbeitung.
- Analyse der Effekte der Umwandlung (Quantisierung) der reellen Messdaten in die kryptographische Domäne (Bitstrings, Integer) und zurück.
- Formale Definition eines Sicherheitsmodells für verteilte Signalverarbeitung.
- Formale Sicherheits- und Komplexitätsanalyse des Protokolls von Gonzalez-Serano et al. und die Evaluation davon in Bezug auf Cloud-Einsatz.
- Erarbeitung und prototypische Implementierung eines neuen Protokolls zur datenschutzerhaltender Filterung der verschlüsselten Messdaten, das nur auf effizient berechenbaren homomorphen Operationen (z.B. Addition) aufbaut.

Bearbeiter:	**B.Sc. Susi Studiergut**	**Matrikelnummer: 12345678**
Betr. Mitarbeiter:	**Dr.-Ing. Benjamin Noack**,	
Referent:	**Prof. Dr.-Ing. Uwe D. Hanebeck**	
Beginn:	**1. Februar 2018**	
Zwischenvortrag:	**≈1. Mai 2018**	
Abgabe:	**31. Juli 2018**	

Karlsruhe, den 13. März 2018

Susi Studiergut	*Benjamin Noack*	*Uwe D. Hanebeck*