

Thema für Bachelor-/Masterarbeit

## Verfahren zur Verschlüsselung und Authentifizierung von eingebetteten Sensorknoten

Cyber-Sicherheit im Zuge der wachsenden Digitalisierung (Industrie 4.0) und dem Vorranschreiten des Internets der Dinge wird aufgrund sich öffnender Infrastruktur zunehmend wichtiger. Während in der Vergangenheit vorwiegend klassische IT-Systeme Angriffen ausgesetzt waren, werden es in Zukunft die mobilen Sensor- und Netzwerkknoten sein, die auf Basis von Klein- und Kleinstrechnern arbeiten. Diese eingebetteten Systeme, die meistens ohne Betriebssystem auskommen, zeichnen sich vor allem durch ihren sehr geringen Stromverbrauch und langen Lebenszyklus aus. Klassische Verschlüsselungsverfahren können auf diesen Systemen aufgrund ihrer begrenzten Ressourcen nur begrenzt eingesetzt werden.

Im Rahmen der Arbeit sollen Verfahren weiterentwickelt werden, um Verschlüsselungs- und Authentifizierungsmethoden möglichst stromsparend und kostengünstig in netzwerkfähige Controller zu implementieren.

Zu den Aufgaben zählen:

- Recherche und Auswahl von geeigneten Verfahren (Public-Key-Kryptographie, Forward Secrecy), Standards (X.509, etc.) und ggf. externer Crypto-Hardware;
- Aufbau eines Demonstrators und Implementierung notwendiger Softwarekomponenten;
- Validierung und Optimierung hinsichtlich Stromverbrauch.

### Unser Profil

Das Laboratory for Biosignal Processing (LaBP) arbeitet im Rahmen biomedizinischer Themen schwerpunktmäßig an der Erfassung, Verarbeitung und Analyse von Biosignalen. In interdisziplinären Forschungsprojekten entwickeln wir gemeinsam mit Partnern aus Wirtschaft und Wissenschaft innovative und anwendungsnahe Lösungen für vielfältige Problemstellungen in der Biotechnologie und Medizintechnik.

**Fragen und Bewerbungsunterlagen richten Sie bitte an:**

Gerold Bausch

E-Mail: [gerold.bausch@htwk-leipzig.de](mailto:gerold.bausch@htwk-leipzig.de)

Tel. 0341-3076 3103

