Masterarbeit Vorschlag

Titel: *Untersuchung und Erweiterung von Privacy Amplification Methoden für drahtlose Physical Layer Security Anwendungen*.

Beschreibung: Im Rahmen dieser Masterarbeit soll zunächst eine Literaturrecherche über Methoden zur Erhöhung der Informationsentropie in kryptografischen Schlüsseln (asym. und sym.) durchgeführt werden. Das generelle Ziel dabei ist die nachweislich sichere Generierung von kryptografischem Schlüsselmaterial, welches z.B. für symmetrische Blockchiffren wie den AES genutzt werden kann. Hierbei ist der Ausgangspunkt eine Menge Φ an Input Bits, die eine geringe Informationsentropie besitzt. Ausgehend von Φ soll eine Erweiterung $AMP(\Phi)$ entwickelt werden, die eine Erhöhung der intrinsischen Entropie des Inputs Φ erreicht und zugleich einen Schlüssel $AMP(\Phi) = \alpha$ berechnet, der direkt in einer symmetrischen Blockchiffre verwendet werden kann. Hiermit wird implizit die Stärke des Schlüssels α erhöht. Daher bezeichnet man diesen Vorgang in der Literatur als *Privacy Amplification.*
Eingesetzt werden kann dieser Funktionsbaustein unter anderem in der Physical Layer Security (PLS) und der damit verbundenen Secret Key Generation (SKG). Die Idee dabei ist die Ableitung von symmetrischem Schlüsselmaterial aus den reziproken Funkkanaleigenschaften auf beiden Seiten eines (Funk-)Kommunikationskanals. Dieses erspart in der Praxis den asymmetrischen Schlüsselaustausch da beide Kommunikationsteilnehmer das geteilte Geheimnis aus dem Funkkanal generieren können. Durch auftretende Dämpfungs-, Abschattungs-, Reflexionseffekte oder Mehrwegeausbreitung bilden Funkkanäle ein intrinsisches Kanalprofil zwischen zwei Teilnehmern ab, das eine hohe Entropie besitzt. Um dieses Kanalprofil nutzbar zu machen, wurden fünf wesentliche Bausteine in der Literatur entwickelt: „Channel Measurement“, „Reciprocity Enhancement“, „Quantization“, „Information Reconciliation“ und die „Privacy Amplification“ [1, 3]. Lipps et al. haben den Vorgang grafisch wie folgt zusammengefasst:

Abbildung 1: SKG-Blöcke nach [1]

Bisher ist der letzte Block (Privacy Amplification) nur wenig beleuchtet worden. Zumeist verwenden SKG-Konzepte als letzten Block die simple SHA256 Hash Funktion, um die Verstärkung der Entropie zu erreichen. Im Rahmen dieser Masterarbeit sollen hierbei jedoch Alternativen aufgezeigt und mittels eines Demonstrators auf die reale Umsetzbarkeit hin evaluiert werden.

Aufgaben

Die anvisierten Aufgaben und Probleme, die es im Rahmen dieses Projektes zu lösen gilt, sind die folgenden:

- Literaturrecherche zu bestehenden Privacy Amplification Konzepten
- Entwicklung und Ableitung von alternativen Konzepten für die Privacy Amplification
- Erprobung und reale Umsetzung eines Konzepts am Demonstrator
    - Leistungsbewertung ausgehend von dem SHA-256 Referenzfall
    - Einschätzung der Umsetzbarkeit für ressourcenbeschränkte Geräte

Ressourcen/Literatur

[1]	C. Lipps, S. B. Mallikarjun, M. Strufe, C. Heinz, C. Grimm and H. D. Schotten, "Keep Private Networks Private: Secure Channel-PUFs, and Physical Layer Security by Linear Regression Enhanced Channel Profiles," *2020 3rd International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, 2020, pp. 93-100, doi: 10.1109/ICDIS50059.2020.00019.
[2]	P. Walther *et al.*, "Improving Quantization for Channel Reciprocity based Key Generation," *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*, Chicago, IL, USA, 2018, pp. 545-552, doi: 10.1109/LCN.2018.8638248.
[3]	Lipps, Christoph & Schotten, Hans. (2022). Physical Layer Security: About Humans, Machines and the Transmission Channel. European Conference on Cyber Warfare and Security. 21. 160-169. 10.34190/eccws.21.1.403.
[4]	H. Chamkhia, A. Erbad, A. Al-Ali, A. Mohamed, A. Refaey and M. Guizani, "PLS Performance Analysis of a Hybrid NOMA-OMA based IoT System with Mobile Sensors," *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, Austin, TX, USA, 2022, pp. 1419-1424, doi: 10.1109/WCNC51071.2022.9771872.
[5]	C. Lipps, D. Krummacker and H. D. Schotten, "Securing Industrial Wireless Networks: Enhancing SDN with PhySec," *2019 Conference on Next Generation Computing Applications (NextComp)*, Mauritius, 2019, pp. 1-7, doi: 10.1109/NEXTCOMP.2019.8883600.

Betreuung durch:

	JULIAN DREYER, M.SC.	**PROF. DR-ING. RALF TÖNJES**
RAUM:	UA0309	UA0308
E-MAIL:	j.dreyer@hs-osnabrueck.de	r.toenjes@hs-osnabrueck.de
TELEFON:	0541 969 7317	0541 969 2941