

Duale Hochschule Baden-Württemberg Mannheim



Studienarbeit

# Programmierung einer SIM-Authentifizierung

Irgend ein Untertitel

Name: **Marco Heumann**  
Matrikelnummer: 4188528  
Kurs: TINF13AI-BI  
Studiengang: Angewandte Informatik  
Studiengangsleiter: Prof. Dr. C. Bürgy  
Betreuer:  
Semester: 5. - 6. Semester  
Datum:



## Ehrenwörtliche Erklärung

Gemäß § 5 Abs. 3 der Studien- und Prüfungsordnung DHBW Technik vom 22.09.2011 versichere ich hiermit, die vorliegende Arbeit selbstständig und nur mit den angegebenen Quellen und Hilfsmitteln verfasst zu haben.

---

Datum

---

Marco Heumann

# Inhaltsverzeichnis

|   |             |
|---|-------------|
| <b>Ehrenwörtliche Erklärung</b>         | <b>III</b>  |
| <b>Inhaltsverzeichnis</b>               | <b>IV</b>   |
| <b>Abkürzungsverzeichnis</b>            | <b>V</b>    |
| <b>Abbildungsverzeichnis</b>            | <b>VI</b>   |
| <b>Tabellenverzeichnis</b>              | <b>VII</b>  |
| <b>Quellcodeverzeichnis</b>             | <b>VIII</b> |
| <b>1 Einleitung</b>                     | <b>1</b>    |
| 1.1 Idee zur Arbeit . . . . .           | 1           |
| 1.2 Geschichte der USIM . . . . .       | 1           |
| <b>2 Theorie</b>                        | <b>2</b>    |
| 2.1 Mobilfunkstandards . . . . .        | 2           |
| 2.2 SIM-Karten . . . . .                | 2           |
| 2.3 Authentifizierungsvorgang . . . . . | 2           |
| 2.4 Milenage Algorithmus . . . . .      | 2           |
| 2.4.1 Funktionsweise . . . . .          | 3           |
| 2.4.2 AES . . . . .                     | 4           |
| 2.5 PPPoE . . . . .                     | 4           |
| 2.6 raspberry pi . . . . .              | 4           |
| 2.7 pysim . . . . .                     | 4           |
| 2.8 Die Sprache C . . . . .             | 4           |
| 2.9 Projektspecs . . . . .              | 4           |
| <b>3 Tätigkeit</b>                      | <b>5</b>    |
| <b>4 Ergebnis</b>                       | <b>6</b>    |
| <b>5 Diskussion</b>                     | <b>7</b>    |
| <b>Literatur</b>                        | <b>i</b>    |

## Abkürzungsverzeichnis

|             |  |
|-------------|--|
| <b>3GPP</b> | 3rd Generation Partnership Project             |
| <b>SIM</b>  | Subscriber Identity Module                     |
| <b>USIM</b> | Universal Subscriber Identity Module           |
| <b>IMSI</b> | International Mobile Subscriber Identity       |
| <b>GSM</b>  | Global System for Mobile communications        |
| <b>UMTS</b> | Universal Mobile Telecommunications System -   |
| <b>PIN</b>  | Personal Identification Number                 |
| <b>EF</b>   | Elementary File                                |
| <b>AuC</b>  | Authentication Center                          |
| <b>UE</b>   | User Equipment                                 |
| <b>RES</b>  | Response to Challenge                          |
| <b>AMF</b>  | Authentication Management Field                |
| <b>SN</b>   | Sequence Number                                |
| <b>AES</b>  | Advanced Encryption Standard                   |
| <b>OP</b>   | Operator Variant Algorithm Configuration Field |
| <b>K</b>    | Subscriber Key                                 |

## Abbildungsverzeichnis

|   |   |   |
|---|---|---|
| 1 | Übersicht über die Generierung der Authentifizierungsvektoren . . . . . | 3 |
|---|---|---|

## Tabellenverzeichnis

## Listings



---

# **1 Einleitung**

## **1.1 Idee zur Arbeit**

## **1.2 Geschichte der USIM**

## 2 Theorie

### 2.1 Mobilfunkstandards

### 2.2 SIM-Karten

### 2.3 Authentifizierungsvorgang

### 2.4 Milenage Algorithmus

Zwischen SIM<sup>1</sup>-Karte und Netzprovider muss eine sichere Authentifizierung und Kommunikation gewährleistet werden können. Dies war wie in Kapitel 1.2 bereits beschrieben mit dem ersten entwickelten Algorithmus des 3GPP<sup>2</sup> nicht mehr gewährleistet, weshalb mit der Entwicklung des neuen Netzstandards auch ein neuer Algorithmus entwickelt wurde, namentlich der Milenage Algorithmus.

Dieser verfügt über die sieben Funktionen  $f1, f1^*, f2, f3, f4, f5, f5^*$  mit Hilfe derer eine sichere Authentifizierung und Schlüsselgenerierung ermöglicht wird. 3GPP hat allerdings wie auch beim Vorgänger diese Funktionen nicht näher spezifiziert und ermöglicht den Netz Providern eigenen Lösungen zu implementieren. Stattdessen beschrieben sie den Kontext in dem diese Funktionen Anwendung finden und definieren generelle Anforderungen an diese Algorithmen [1].

Der Milenage Algorithmus hat wie erwähnt zwei Hauptaufgaben, nämlich einerseits die Authentifizierung, als auch die Generierung eines Schlüssel, um die versendeten Nachrichten zu ver- und entschlüsseln. Wenn es um die Authentifizierung geht muss sich einerseits die SIM-Karte, bzw. das UE<sup>3</sup>, gegenüber dem Netzprovider authentifizieren, aber andererseits muss sich auch das Netzwerk gegenüber der SIM-Karte authentifizieren. Damit soll die Möglichkeit der Man-in-the-Middle Attacken reduziert werden, die es einem Außenstehenden erlauben die Kommunikation mitzulesen. Auch so genannte Replay-Attacken, bei denen zuvor aufgezeichnete Daten genutzt werden, sind nicht möglich, auf Grund der Sequence Number [2].

---

<sup>1</sup>Subscriber Identity Module

<sup>2</sup>3rd Generation Partnership Project

<sup>3</sup>User Equipment

In den nachfolgenden Unterkapiteln wird die Funktionsweise des Algorithmus, sowie die Funktionsweise der eingesetzten Blockschiffrierung AES<sup>4</sup> erläutert.

### 2.4.1 Funktionsweise

In Kapitel 2.3 wurde beschrieben, welche Daten zwischen AuC<sup>5</sup> und UE verschickt werden, jedoch nicht wie diese Daten generiert werden. Es gibt einige Werte, die auf der USIM<sup>6</sup> und der Datenbank des AuC fest eingespeichert sind. Diese sind der OP<sup>7</sup> und K<sup>8</sup>, sowie jeweils fünf Rotations- und XOR-Konstanten (r1, ..., r5 und c1, ... c5). Welche Funktion welche Werte benötigt und generiert zeigt dabei Abbildung 1.

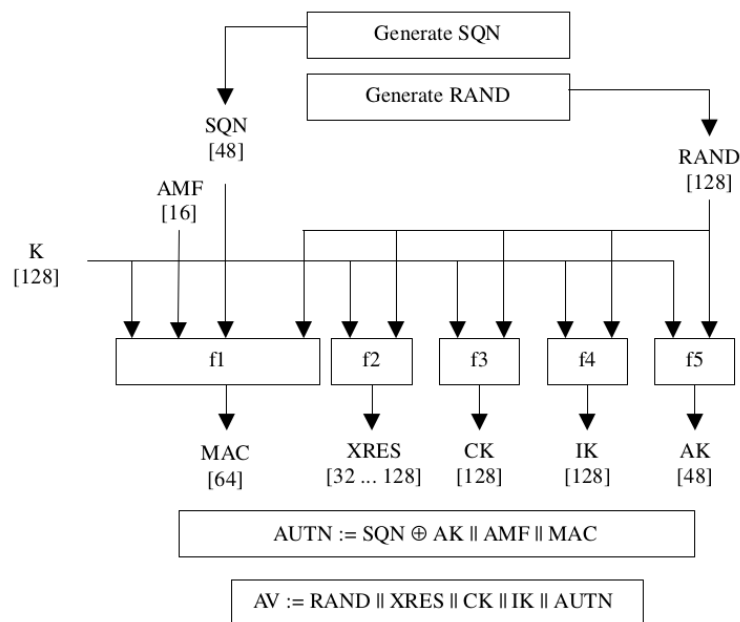


Abbildung 1: Übersicht über die Generierung der Authentifizierungsvektoren

Die Abbildung 1 zeigt, dass zu Beginn die SQN<sup>9</sup> generiert wird. Diese besteht aus den beiden Teilen SEQ und IND, mit SEQ als der die eigentliche Sequenznummer und IND als Arrayindex. Auf der SIM-Karte sind nämlich die letzten SQNs in einem Array gespeichert. Die empfohlene Größe ist 32, was für IND eine Länge von fünf Bits bedeutet. Mit

<sup>4</sup>Advanced Encryption Standard

<sup>5</sup>Authentication Center

<sup>6</sup>Universal Subscriber Identity Module

<sup>7</sup>Operator Variant Algorithm Configuration Field

<sup>8</sup>Subscriber Key

<sup>9</sup>Sequence Number

diesem Index kann nachher die Aktualität der SEQ überprüft werden. Für die Bildung der SEQ selbst gibt es drei verschiedene Möglichkeiten:

- teilweise zeitbasiert
- nicht zeitbasiert
- komplett zeitbasiert

### **2.4.2 AES**

## **2.5 PPPoE**

## **2.6 raspberry pi**

## **2.7 pysim**

## **2.8 Die Sprache C**

## **2.9 Projektspecs**

---

## 3 Tätigkeit

## 4 Ergebnis

---

## 5 Diskussion

## Literatur

- [1] Walker, M., 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*; Document 1: General, TS 35.205, 3rd Generation Partnership Project (3GPP), 2015.
- [2] Spitz, S., Pramateftakis, M. und Swoboda, J., *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*, Studium : IT-Sicherheit und Datenschutz, Vieweg+Teubner Verlag, 2011.



# Studienarbeit

**Titel:** Programmierung einer SIM-Authentifizierung  
**Subtitel:** Irgend ein Untertitel  
**Autor:** Marco Heumann  
**Hochschule:** Duale Hochschule Baden-Württemberg Mannheim  
**Datum:**  
**Bearbeitungszeitraum:**  
**Studiengang:** Angewandte Informatik  
**Matrikelnummer, Kurs:** 4188528, TINF13AI-BI  
**Betreuer:**  
**Gutachter:** Prof. Dr. C. Bürgy

## Abstract

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

# Studienarbeit

**Title:** Programmierung einer SIM-Authentifizierung  
**Subtitle:** Irgend ein Untertitel  
**Author:** Marco Heumann  
**University:** Duale Hochschule Baden-Württemberg Mannheim  
**Date:**  
**Time of Project:**  
**Study Course:** Angewandte Informatik  
**Student ID, Course:** 4188528, TINF13AI-BI  
**Supervisor in the Company:**  
**Reviewer:** Prof. Dr. C. Bürgy

## Abstract

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.