

Vorwort

Wer das kryptographische Verfahren AES implementieren will oder soll, kann es sich sehr einfach machen, denn das Buch [DaRi] der beiden Erfinder des Verfahrens enthält eine komplette Realisierung. Soll die Implementierung jedoch für Mikrocontroller am unteren Ende des Leistungsspektrums durchgeführt werden, kommt man schnell in Schwierigkeiten, denn die Realisierung in [DaRi] ist ein C-Programm, das in die Mikrocontroller nicht hineinpasst.

Nun wäre es wohl möglich gewesen, an besagtem C-Programm so lange herumzubasteln, bis es doch passte, aber solch eine — kann man hier sagen — Strategie wäre doch sehr risikvoll gewesen: Änderungen an einem Programm vorzunehmen, dessen Funktion nicht genau bekannt ist war noch selten von Erfolg gekrönt. Der bessere Weg war sicherlich, vorab volles Verständnis des Verfahren zu erlangen und erst dann zu implementieren, und zwar direkt in die Assemblersprache der Mikrocontroller, um die speziellen Eigenschaften ihrer Befehlssätze ausnützen zu können und so auch Mikrocontroller mit geringen Ressourcen einsetzen zu können.

Allerdings verlangt ein „volles Verständnis des Verfahrens“ ein beträchtliches Mehr an Verständnis komplexer Mathematik als bei Programmieren von Mikrocontrollern gemeinhin vermutet werden kann. Aus diesem Grund hat das Buch in großen Teilen eine geschichtete Struktur. Und zwar sind drei Schichten vorhanden:

- Die obere Schicht enthält die Theorie des Verfahrens. Hier wird noch keine Rücksicht auf eine Implementierung genommen, im Gegenteil, das Verfahren wird in reiner abstrakter Form in mathematischer Terminologie dargestellt.
- Die mittlere Schicht stellt eine praktische Formulierung des Verfahrens dar, welche die Realisierung als Computerprogramm berücksichtigt. Beispielsweise werden Vektorraumhomomorphismen der oberen Schicht durch der Rechnung unmittelbar zugängliche Matrizen ersetzt.
- Die untere Schicht endlich enthält die Umsetzung in Programmcode mitsamt einer ausführlichen Erläuterung der gewählten Umsetzungsstrategien.

Die Umsetzung in Programmcode hängt natürlich stark davon ab, welcher Mikrocontroller das Ziel darstellt. Um diesen Effekt etwas zu mildern werden deshalb Programme für zwei Mikrocontroller vorgestellt, die sehr verschiedenen Welten angehören, nämlich AVR und dsPIC. Überraschenderweise ist der dsPIC, mit einer 16-Bit-CPU und einem großartigen Befehlssatz, dem 8-Bit-AVR-Controller mit seinem wenig Enthusiasmus hervorrufenden Befehlssatz nicht so weit überlegen wie man wohl annehmen konnte. Der Grund liegt darin, daß die beiden umgesetzten kryptographischen Verfahren auf der Maschinenbefehlsebene eine relativ einfache Struktur besitzen, bei der die Vorteile eines überlegenen Befehlssatzes nicht groß ausgespielt werden können.

Es sei an dieser Stelle vermerkt, daß die C-Programme in [DaRi] **keine** Grundlage für die Implementierung von AES gewesen sind.

Kein Thema des Buches sind die kryptographischen Aspekte von Verschlüsselungssystemen, also etwa ob es möglich ist, einen Geheimtext zu dechiffrieren, ohne den zur Chiffrierung verwendeten Schlüssel zu kennen, oder, falls es möglich sein sollte, welcher Aufwand dazu wohl nötig wäre. Allerdings reichen die Darstellung und Implementierung von AES für ein Buch mit anständigem Umfang nicht aus.

Hier bot sich an, zusätzlich ein Verfahren mit öffentlichem Schlüssel darzustellen und zu implementieren. Damit wäre dann auch allein auf der Mikrocontrollerebene die sichere Versendung von AES-Schlüsseln möglich.

Jedoch erfordern sowohl RSA und ähnliche Systeme als auch solche, die auf elliptischen Funktionen basieren, einen solch großen rechnerischen Aufwand, daß eine brauchbare Implementierung für die kleinen Mikrocontroller praktisch ausgeschlossen ist. Das bleibt selbst dann richtig, wenn die effizientesten Rechenverfahren eingesetzt werden, etwa die Durchführung von modularer Multiplikation mit Montgomery-Multiplikation. Das gilt nun nicht nur für die Verschlüsselung an sich, sondern beispielsweise auch für die Bereitstellung von Schlüsseln. So muß beispielsweise ein Paar von großen Primzahlen mit gewissen Eigenschaften erzeugt werden. Wie das Sprichwort es so schön sagt: Die Teufelchen verstecken sich in den Details.

Einige der Verfahren mit einem öffentlichen Schlüssel sind jedoch rechentechnisch noch praxisgeeignet zu bewältigen, und zwar sind das Verfahren, die auf dem Rucksackproblem basieren. Hier bereitet auch die Schlüsselerzeugung keine großen Probleme. Leider sind diese Chiffriersysteme nicht sicher (siehe z.B. [Sha]). Allerdings ist die Dechiffrierung eines Geheimtextes ohne den eingesetzten Schlüssel zu besitzen sehr aufwendig, und das gilt nicht nur für den Einsatz des Verfahrens, sondern auch für sein Verständnis. Zieht man daher den Einsatzzweck der im Buch behandelten Systeme in Betracht, nämlich die Verhinderung nicht autorisierten Gebrauches von Mikrocontrollersoftware, dann kann dieses Problem sicherlich ignoriert werden: Einem Raubkopierer von Mikrocontrollersoftware werden die benötigten Ressourcen wohl kaum zur Verfügung stehen.

Zum Schluss sei noch angemerkt, daß die Autoren bemüht waren, auch Querlesern einen leichten Zugang zu den verschiedenen Buchabteilungen zu ermöglichen, also etwa solchen Lesern, die an der theoretischen Darstellung nicht interessiert sind oder umgekehrt (wenn auch sehr unwahrscheinlich) nur an der Theorie interessiert sind. Das Buch enthält deshalb einiges an Redundanz, um das möglich zu machen.

Herrad Schmidt
Manfred Schwabl-Schmidt

Boppard, im Mai 2017

AES und Rucksackverfahren

Theorie und Praxis mit AVR- und dsPIC-Mikrocontrollern

Schmidt, H.; Schwabl-Schmidt, M.

2017, IX, 241 S., Softcover

ISBN: 978-3-658-19703-2