Kryptografie in UHF Tags: Aktueller DIN-Vorschlag zur Standardisierung einer Crypto Suite

Klaus Finkenzeller[1], Walter Hinz[1], Katharina Schulz[1]

Kurzfassung:
Der vorliegende Beitrag beschreibt einen von uns eingereichten Normungsvorschlag für ISO/IEC 29167 [2], der eine Crypto Suite basierend auf dem Rabin-Montgomery Verfahren für UHF Tags definiert. Das Verfahren ermöglicht eine sichere Identifikation des Tags, um zum Beispiel ein auf der UHF-Technologie gestütztes „hands-free“ Ticketingsystem für den öffentlichen Verkehr zu implementieren. Hierbei sollen handelsübliche RFID-Leser unverändert verwendet werden können. Träger derartiger Tags sollen mit normalen, nicht zum System gehörenden Lesern nicht verfolgt werden können. Dies ist mit handelsüblichen Tags problemlos möglich, da bei diesen die Tag-ID (EPC) aus einer eindeutigen, konstanten Zahl gebildet und im Klartext übertragen wird.

Stichworte: UHF, RFID, Public Key Cryptosystem, Rabin, Montgomery

1 Einleitung

UHF Tags sind passive RFID Transponder gemäß dem Standard ISO/IEC 18000-63 [1] (ehemals ISO/IEC 18000-6C, äquivalent zu EPC Class-1 Generation-2), die über eine Distanz von mehreren Metern im Frequenzbereich 860 MHz bis 960 MHz kontaktlos kommunizieren können. Solche Tags werden heute vor allem zur Identifikation und Verfolgung von Waren und Gütern in der Handelslogistik eingesetzt. Hierzu besitzen die Tags als eindeutige Kennzeichnung einen elektronischen Produktcode (EPC).

Bei UHF RFID wird das sogenannte RADAR-Backscatter Verfahren zur Datenübertragung vom Tag zum Lesegerät eingesetzt. Dieses Funktionsprinzip ist in Abbildung 1 veranschaulicht. Die UHF-Technologie zeichnet sich durch große Lesereichweiten von typischerweise 3 m bis 12 m aus. Einerseits ergeben sich durch die große Leseentfernung zahlreiche Anwendungsszenarien, die mit induktiv gekoppelten RFID Systemen, welche nur kurze Distanzen von bis zu einigen 10 cm erlauben, nicht realisiert werden können. Andererseits verlangen viele dieser Anwendungen gerade aufgrund der größeren Reichweite den Einsatz kryptografischer Maßnahmen für abhörsichere Kommunikation, Authentisierung und Prüfung der Identität der beteiligten Kommunikationsendpunkte.

[1] Giesecke & Devrient GmbH, München

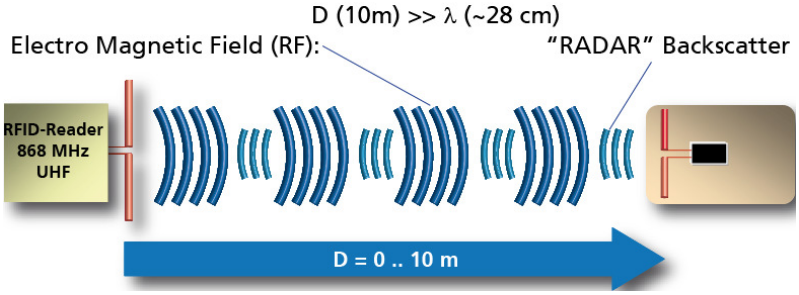

Abbildung 1 Funktionsprinzip von UHF RFID

Handelsübliche UHF Tags verfügen heute noch nicht über kryptografische Funktionen. Somit ist eine sichere Authentisierung wie bei kontaktbehafteten Chipkarten, beispielsweise mittels eines Public-Key-Verfahrens, mit UHF Chips heute nicht möglich. Die in großer Distanz nur sehr geringe zur Verfügung stehende Energie stellt eine der Schwierigkeiten beim Einsatz kryptografischer Funktionen in UHF Chips dar. Besitzt der Chip keine eigene Energiequelle, erfolgt demnach die Energieversorgung über das elektromagnetische Feld, reicht die durch den Leser bereit gestellte Energie nicht zur Ausführung der Operation aus, oder die Energie steht nicht für die Durchführung der Operation benötigte Dauer der zur Verfügung.

Da also passive Tags ihre Energie aus dem elektromagnetischen Feld beziehen müssen, ist ein Verfahren auszuwählen, das möglichst wenige Rechenoperationen und folglich möglichst wenig Energie erfordert. In diesem Beitrag stellen wir ein Verfahren vor, bei dem der Rabin-Algorithmus mit der Montgomery-Multiplikation kombiniert und der Funktionsumfang eines UHF Tags geeignet erweitert wird, um solchen Anforderungen zu genügen.

1.1 Zum Stand der Technik

UHF Tags speichern einen Unique Item Identifier (UII), eine statische weltweit eindeutige Nummer, über welche das Tag und dadurch auch das Trägerobjekt, an dem das Tag befestigt ist, identifiziert wird. In den meisten Anwendungen kommt heute als UII ein EPC zur Anwendung. Der UII eines UHF-Tags kann ohne Einschränkungen mit einem beliebigen UHF Leser ausgelesen werden und wird im Klartext übertragen. UHF Tag und Leser (*interrogator*) kommunizieren über einen nicht-abhörsicheren Kanal, was das Tag anfällig für Cloning- und Emulation-Angriffe und unerwünschten Informationsabfluss macht. Der Leser erkennt die Gültigkeit eines UHF Tags uneingeschränkt lediglich anhand des gelesenen Wertes an. Der UII kann ferner durch passives Abhören der Kommunikation zwischen Leser und Tag über die Luftschnittstelle über Entfernungen von bis zu 100 m und mehr ermittelt werden. Aktiver und passiver Zugriff sind demnach ohne vorausgehende Authentisierung oder Prüfung der Zugriffsberechtigung und unbemerkt (etwa durch die Person, welche den gekennzeichneten Gegenstand trägt) möglich. Der ermittelte UII kann von einem Angreifer dazu verwendet werden, die Identität eines echten UHF Tags vorzutäuschen, indem er ein Duplikat des Originals herstellt, oder durch Tag-Emulation mittels

einer geeigneten Vorrichtung (die nicht notwendigerweise selbst ein UHF Tag ist).

Zu den Sicherheitsfunktionen von ISO/IEC 18000-63 gehören ein nur-lese UII, ein optionaler Schreibschutz für einzelne Speicherbereiche, ein optionaler Passwortschutz für die Schreib- und Lesefunktion, ein passwort-geschütztes „Kill“ Kommando sowie 16-bit Prüfsummen (CRC) für fast alle Kommandos. Erweiterte, insbesondere kryptografische Schutzmaßnahmen für z.B. sichere Kommunikation sind nicht vorgesehen und heute nur mit proprietären Lösungen möglich. Um diese Lücke zu schließen wurde in dem Standardisierungsgremium SC31/WG7 mit der Entwicklung von sogenannten Crypto Suites begonnen, die in ISO/IEC 29167 spezifiziert werden sollen. In diesem Artikel beschreiben wir den von uns eingereichten Normenvorschlag für eine Crypto Suite, dem das Rabin-Montogmery Verfahren zugrunde gelegt ist.

2 Rabin-Montgomery Kryptosystem für UHF Tags

2.1 Das Rabin-Verfahren

Das Rabin-Verfahren [3] ist eines der ältesten bekannten Authentifizierungs- und Verschlüsselungsverfahren, das als Grundlage die modulare Exponentiation nutzt. Es war das erste asymmetrische Kryptosystem, bei dem auf mathematischen Weg bewiesen werden konnte, dass es zumindest gleich schwierig zu lösen ist wie das Faktorisierungsproblem, von welchem angenommen wird, das es nicht effizient lösbar ist. Wie alle asymmetrischen Kryptosysteme verwendet auch das Rabin-Kryptosystem einen öffentlichen Schlüssel (*public key*) und einen geheimen Schlüssel (*private key*).

Es beruht auf zwei großen, geheim zu haltenden Primzahlen, p und q (d.h. der geheime Schlüssel ist das Paar (p, q)), für die die Kongruenzbedingung $p \equiv q \equiv 3 \pmod 4$ gilt und deren Produkt

$$n = p \cdot q \tag{1}$$

den Modulus des Verfahrens darstellt und gleichzeitig als öffentlicher Schlüssel n bekannt gegeben wird. Anders ausgedrückt: Wer nur n kennt, kann verschlüsseln aber nicht entschlüsseln, wer dagegen p und q kennt, kann damit auch entschlüsseln. Wären p und q keine Primzahlen, so ließe sich das Verfahren nicht anwenden.

Zweckmäßigerweise werden die ursprünglichen Primzahlen p und q in etwa gleich groß gewählt.

Gemäß dem Rabin-Verfahren wird die zu übertragende Klartextnachricht M, die beispielsweise eine die Identität und Authentizität des Tags nachweisende geheime Information (z.B. eine eindeutige Tag-ID) beinhalten kann, durch modulares Quadrieren verschlüsselt, also

$$C = M^2 \bmod n \tag{2}$$

Die Sicherheit des Verfahrens beruht darauf, dass die Berechnung der modularen Quadratwurzel aus dem Chiffretext C ohne Kenntnis der Primzahlen p und q schwierig ist. Dies ist aber nur dann der Fall, wenn M nicht wesentlich kleiner als n ist. Durch die auf die Quadrierung folgende Modulo-Operation wird verhindert, dass eine Entschlüsselung durch einfaches Wurzelziehen aus einer natürlichen Zahl möglich ist.

Um einen Angriff durch Wiederholung einer abgefangenen authentischen Nachricht zu erschweren, ist es ferner erforderlich, eine ausreichende Anzahl zufälliger Daten, die vom Lesegerät und dem Tag unabhängig voneinander erzeugt werden, in den Klartext M einzufügen.

Nachdem die Nachricht C vom RFID-Leser empfangen wurde, muss sie wieder entschlüsselt werden, um den Inhalt überprüfen zu können. Da die Verschlüsselung einer modularen Quadrierung entspricht, muss der Leser dazu also eine modulare Quadratwurzel berechnen. Unter den anfangs dargestellten Voraussetzungen gelingt dies verhältnismäßig einfach:

Seien allgemein C und n bekannt, so wird $M \in \{0,...,n-1\}$ gesucht mit

$$M^2 \equiv C \bmod n \tag{3}$$

Wenn, wie in unserem Fall, n das Produkt von zwei Primzahlen p und q ist, lässt sich der chinesische Restsatz ausnutzen.

Gesucht sind die Quadratwurzeln $M_p = \sqrt{C} \bmod p$ und $M_q = \sqrt{C} \bmod q$, wobei C ein quadratischer Rest modulo p und q ist. Im Fall p, q = 3 (mod 4) gilt

$$M_p = \pm C^{\frac{p+1}{4}} \bmod p \tag{4}$$

$$M_q = \pm C^{\frac{q+1}{4}} \bmod q \tag{5}$$

Falls p oder q gleich 1 (mod 4) gilt, ist die Berechnung der entsprechenden Quadratwurzel zwar auch möglich, aber komplizierter.

Es werden nun yp und yq mit

$$y_p \cdot p + y_q \cdot q = 1 \tag{6}$$

bestimmt. Hierfür kann z.B. der erweiterte euklidische Algorithmus verwendet werden. Unter Ausnutzung des chinesischen Restsatzes können jetzt die vier Quadratwurzeln +r, -r, +s und –s von C bestimmt werden:

$$\begin{aligned} +r &= (y_p \cdot p \cdot M_q + y_q \cdot q \cdot M_p) \bmod n \\ -r &= n - r \\ +s &= (y_p \cdot p \cdot M_q - y_q \cdot q \cdot M_p) \bmod n \\ -s &= n - s \end{aligned} \tag{7}$$

Eine dieser vier Quadratwurzeln ergibt den gewünschten Klartext; die anderen drei sind zu verwerfen. Daher ist es erforderlich, den „richtigen“ Klartext durch eine Kennung, Prüfsumme oder Ähnliches kenntlich zu machen.

2.2 Modulare Montgomery Multiplikation

Die modulare Montgomery-Multiplikation [4] bezeichnet ein alternatives Verfahren zur Berechnung des Produktes $C = a \cdot b$ (mod n). Anstatt direkt mit ganzen Zahlen modulo n zu rechnen, definieren wir für eine beliebige ganze Zahl x das Residuum $\overline{x} = xR$ (mod n), und ersetzen die Operanden und Ergebnisse der Berechung durch deren Residuen. Die Zahl R wird dabei so gewählt, dass sie sowohl größer als n als auch teilerfremd zu n ist, so dass die Division durch R modulo n möglich ist. Im Allgemeinen wird für R eine Zweierpotenz gewählt, so dass diese Rechenoperationen durch bitweise Maskierung und Verschiebung erreicht werden. Die Eigenschaft der Teilerfremdheit ist immer garantiert, wenn n ungerade und R eine Potenz von 2 ist, was für kryptografische Probleme typischerweise zutrifft.

Es existiert eine 1:1-Abbildung zwischen den Zahlen $a, b, \ldots$ und deren Residuen $\overline{a}, \overline{b}, \ldots$. Addition und Subtraktion sind gleich

$$x\,R \pm y\,R \equiv z\,R \,(\mathrm{mod}\, n) \tag{8}$$

genau dann, wenn $x \pm y \equiv z (\mathrm{mod}\, n)$. Dies ist wichtig, denn die Konvertierung zwischen der natürlichen und der residualen Darstellung einer Zahl ist kostspielig und man sollte so lange wie möglich in einer Darstellungsform arbeiten können und Konversionen minimieren. Es wird sich zeigen, dass unser Verfahren überhaupt nur eine einzige Konvertierung erfordert, und zwar auf Seiten des Lesers.

Um die Multiplikation zu definieren, benötigen wir das modulare Inverse R^{-1} von R, so dass

$$y_p \cdot p + y_q \cdot q = 1 \tag{9}$$

oder, anders ausgedrückt

$$R\,R^{-1} = 1 \,(\mathrm{mod}\, n) \tag{10}$$

wobei k eine ganze Zahl ist. Ist nun $C = a \cdot b$ (mod n), so gilt

$$\overline{C} \equiv (a \cdot b)\ R \equiv (aR \cdot bR)\ R^{-1} \equiv (\overline{a} \cdot \overline{b})\ R^{-1} \pmod{n} \qquad (11)$$

Es erweist sich, dass man den Ausdruck $(\overline{a} \cdot \overline{b})\ R^{-1} \pmod{n}$, im Vergleich zu einer normalen modularen Multiplikation, kostengünstiger (ohne Division) berechnen kann, weil die Division durch R bei geschickter Wahl von R durch eine wortweise Verschiebung erledigt werden kann.

2.3 Kombination zu Rabin-Montgomery

Das Rabin-Verfahren birgt den Nachteil, dass zur modularen Reduktion eine kostspielige Division mit Rest ausgeführt werden muss und weiterhin, dass vor Abschluss dieser Division noch kein Teilergebnis zur Verfügung steht. Der Ablauf stellt sich also in der seriellen Abfolge „Quadrierung" – „modulare Reduktion" – „Datenübertragung (Ergebnis senden)" dar.

In unserem Ansatz wird auf dem Tag die Rabin-Verschlüsselung derart mit der Montgomery-Methode kombiniert, dass keine modulare Reduktion, also keine Division benötigt wird und nicht mehr Daten erzeugt werden, als der Länge des Modulus n entspricht. Das Tag berechnet und sendet das inverse Residuum $M^2\ R^{-1}$ (mod n) der verschlüsselten Nachricht M^2 (mod n).

Das Verfahren bietet den Vorteil, dass das Tag mit der Berechnung der Verschlüsselung beginnen kann, bevor alle in die Rechnung eingehenden Daten vollständig vorliegen (z.B. bevor sie vollständig empfangen wurden). Auch das Senden des Ergebnisses (als eine Folge von Teilergebnissen) an den Leser kann beginnen, bevor die Berechnung abgeschlossen ist. Weil hierbei Datenübertragung und Berechnung parallel ausgeführt werden, wird die Transaktionszeit verkürzt. Ist das UHF-Tag also eingerichtet, dass die Übertragung der Teilergebnisse unabhängig von der Berechnung des Algorithmus durchgeführt werden kann, so können die beiden Prozesse „Verschlüsselung" und „Datenübertragung" parallel ausgeführt werden, was zu einer deutlichen Verbesserung der Leistung des Gesamtsystems führt.

Im RFID-Leser wird zunächst der empfangene Datensatz, der ja aufgrund des Montgomery-Algorithmus das inverse Residuum $M^2\ R^{-1}$ (mod n) des eigentlichen Chiffretextes M^2 (mod n) darstellt, in die Normaldarstellung umgewandelt. Dazu wird er mit R multipliziert und anschließend modular reduziert, wobei in diesem Fall eine Langzahldivision zur Anwendung kommt, deren Kosten aber im Vergleich zur nachfolgenden Rabin-Entschlüsselung keine Rolle spielen. Bei dieser Gelegenheit kann auch gleich ein (sehr unwahrscheinlicher) Überlauf der modularen Montgomery-Multiplikation korrigiert werden. Der weitere Ablauf der Entschlüsselung ist identisch mit dem bekannten Ablauf der Rabin-Entschlüsselung, da nunmehr der Datensatz wieder in der Form $C = M^2$ (mod n) vorliegt.

2.4 Struktur des Identifizierungsnachricht

Die Zielsetzung und Hauptanwendungsfall unseres Normenvorschlags ist letztlich eine eindeutige Identifizierung des betreffenden UHF-Tags anhand einer (möglichst authentischen) Identifikationsnummer. Gleichzeitig soll vermieden werden, dass ein derart ausgerüstetes Tag mit einem beliebigen Leser, der nicht über den geheimen Schlüssel verfügt, zu identifizeren und zu verfolgen ist.

Die letzte Forderung ist einfach zu erfüllen: Bei jeder Aktivierung des Tags wird eine ausreichende Anzahl von Stellen der EPC-ID zufällig neu generiert und damit einem einfachen EPC-Leser immer eine andere Identität präsentiert. Der entsprechend ausgestattete Leser jedoch erkennt anhand der festen Stellen der EPC-ID, zu welcher Gruppe dieses Tag gehört und welcher geheime Schlüssel demzufolge anzuwenden ist.

Der Inhalt der Nachricht M besteht also in erster Linie aus einer eindeutigen Kennung, sowie, in optionaler Ausführung, einer Signatur dieser Kennung, die mitttels eines Elliptische Kurven Verfahrens berechnet wurde. Die Anwendung Elliptischer Kurven hat den Vorteil, dass die sich ergebenden Signaturen ohne weiteres innerhalb der maximal zur Verfügung stehenden Nachrichtenlänge (128 Bit, abzüglich einiger Bit Redundanz) untergebracht werden können. Hinzu kommen vom Leser einerseits und vom Tag andererseits erzeugte Zufallsdaten, die die Authentizität und die Frische der Nachricht sicherstellen sollen.

Das Rabin-Kryptosystem weist eine Schwäche gegen Angriffe mit bekanntem Klartext auf, wenn der Angreifer alle vier Wurzeln zur Verfügung hat. Er ist dann nämlich in der Lage die Faktoren von n auszurechnen. Dieser Fall trifft hier allerdings nicht zu, denn zum einen kann der Angreifer nur einen kleinen Teil der zu verschlüsselnden Daten vorgeben, zum anderen wird er vom Leser nur die korrekte Wurzel erhalten, die anderen werden verworfen.

Dennoch ist es sinnvoll, längere Passagen mit bekanntem oder manipulierbarem Klartext innerhalb der Nachricht zu vermeiden. Deshalb werden die darin enthaltenen Komponenten vor der Verschlüsselung miteinander vermischt. Der nachfolgende Pseudocode demonstriert beispielhaft eine derartige MIX-Funktion:

```
for (i=0; i<16;++i) {                          // 112 bytes (7*16)
get next 5 bytes from (signed) ID; if out of data, get random bytes;
  get 1 byte from reader challenge;
  get 1 byte random as Tag challenge;
}
get next 13 bytes from (signed) ID; if out of data, get random bytes;
```

3 Konkrete Umsetzung in UHF Tags

Zur Authentisierung des Tags gegenüber dem Leser wird ein Datensatz mittels Rabin-Montgomery verschlüsselt von dem UHF-Tag an den RFID-Leser übertragen. Der Datensatz setzt sich aus einem vom Leser vorgegebenen zufälligen Teil (*Challenge*), aus einem vom Tag beigesteuerten zufälligen Teil und aus einem extern signierten Teil,

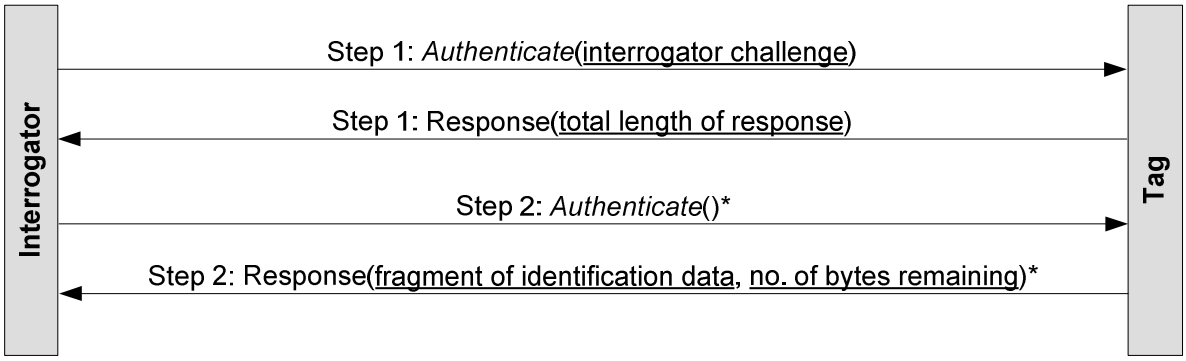

Abbildung 2 Nachrichtenaustausch für Tag-Identifikation

der Sig(UII|…) des Tags zusammen, welcher die Authentizität des Tags anhand der darin enthaltenen eindeutigen Seriennummer UII und weiteren Informationen nachweist. Durch die enthaltenen zufälligen Bestandteile wird erreicht, dass sowohl der Klartext als auch der verschlüsselte Datensatz bei jeder Abfrage unterschiedlich ausfallen. Dabei ist die Rabin-Verschlüsselung so realisiert, dass das Tag schon während des Empfangs des *Challenge* mit der Verschlüsselung beginnen kann. Außerdem kann es die ersten Datenbytes des Ergebnisses der Verschlüsselung bereits ausgeben, während es noch dabei ist die nachfolgenden Datenbytes zu berechnen.

Im Teil 1, *Crypto Suite Framework*, des Standards ISO/IEC 29167-1 [2] wird das Kommando *Authenticate* definiert. Wir bedienen uns dieses Kommandos, um ein Challenge-Response-Protokoll mit dem Ziel der Tag-Authentisierung durchzuführen. Das Protokoll wird vom Leser initiiert, indem im ersten Schritt der *Challenge* des Lesers an das Tag übertragen wird. Die erste Antwort des Tags beinhaltet die Gesamtlänge der Antwortdaten. Im zweiten Schritt werden vom Leser iterativ so viele *Authenticate* Kommandos gesendet wie für die Abholung der Antwortdaten notwendig ist. Dieses Vorgehen liegt u.a. darin begründet, dass UHF Tags über einen begrenzten Sende- und Empfangspuffer verfügen und nicht die gesamten Antwortdaten gleichzeitig zur Verfügung stehen. Wir hatten bereits erwähnt, dass die Verschlüsselung und das Senden der Teilergebnisse überlagert sind. Die beschriebene Überlappung von Eingabe, Verarbeitung und Ausgabe des Rabin-Montgomery-Verfahrens können hier vorteilhaft angewendet werden. Die Kommando-Sequenz ist in Abbildung 2 aus dem Normungsvorschlag dargestellt.

Ein ISO/IEC 18000-63 UHF Tag befindet sich zu jedem Zeitpunkt in einem der Zustände *Ready*, *Arbitrate*, *Reply*, *Acknowledge*, *Open*, *Secured* oder *Killed*, in denen jeweils unterschiedliche Kommandos und daraus resultierende Aktionen erlaubt sind. Beispielsweise versetzen Zugriffkommandos mit korrektem Access-Passwort das Tag vom *Open* in den *Secured*-Status, das Kill-Kommando vom *Secured* in den *Killed*-Status. In den Crypto Suite-spezifischen Teilen des ISO/IEC 27167 Standards wird dieser Zustandsautomat erweitert. Für die Rabin-Montgomery Crpyto Suite ist dieser auszugsweise in Abbildung 3 dargestellt.

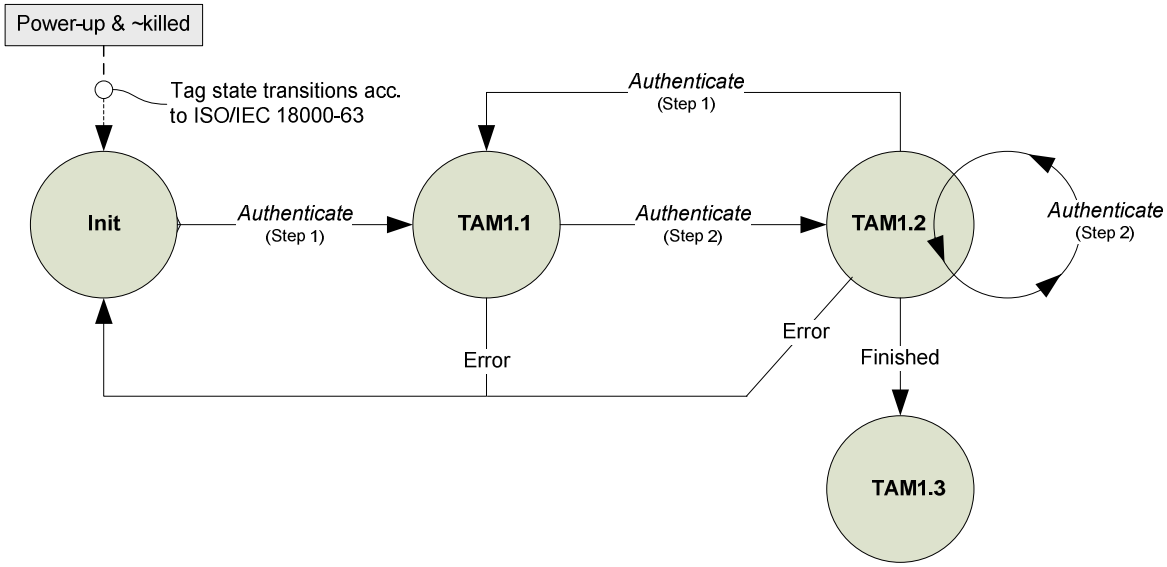

Abbildung 3 Erweiterung des ISO/IEC 18000-63 Zustandsautomaten

Um die Funktionsfähigkeit des Protokolls zu verifizieren haben wir ein UHF Tag mit einem Mikrocontroller ergänzt, der als Softcore in einem FPGA realisiert war. Von dem UHF-Tag wird nur noch der Analogteil verwendet; das demodulierte Basisbandsignal wurde an das FPGA übergeben, wo auch das vollständige UHF-Protokoll nach ISO/IEC 18000-63 abgewickelt wird. Dabei hat der Mikrocontroller Zugriff auf die Speicherbänke des UHF-Tags, somit kann eine Datenübergabe vom UHF-Leser über das Tag an den Mikrocontroller und entgegen gesetzt realisiert werden.

Als Mikrocontroller wird im FPGA ein MSP430X nachgebildet, dessen Vorzug im Rahmen dieser Aufgabenstellung darin besteht, dass er einen 16×16-Bit Multiplizierer enthält, der die bei der Berechnung auftretenden Partialprodukte in einem einzigen Taktzyklus multiplizieren und aufaddieren kann.

Unter den gegebenen Bedingungen werden bei einem Systemtakt von 1,28 MHz zur Berechnung der RAMON-Nachricht ca. 137 ms benötigt (bzw. 171.250 Taktzyklen). Diese Zahl ist zu vergleichen mit einem Aufwand von 336 ms allein zur Übertragung der Daten an den UHF-Leser, welche wegen der begrenzten Pufferkapazitäten auf der Übertragungsstrecke in mindestens zwei Pakete aufgeteilt werden muss.

Es ist zu berücksichtigen, dass die Funktionen des Crypto Suite Frameworks von handelsüblichen UHF-Lesern noch nicht unterstützt werden, daher erwarten wir hier noch Verbesserungspotential, ebenso wie bei der Optimierung der Funktionen innerhalb des Tags.

4 Anwendungsgebiete für sichere UHF Tags

Zu den Anwendungsgebieten sicherer UHF Tags zählen die authentische Identifikation von gekennzeichneten Objekten, jedoch ausdrücklich ohne die Möglichkeit diese mit

einem unberechtigten systemfremden Lesegerät auf Grund der nach dem Stand der Technik statischen UII verfolgen zu können.

Weiterhin ist die authentisierte Zugriffs- bzw. Zutrittsberechtigung mit „hands-free" Funktion wie z.B. an Ski-Liften zu nennen.

Als drittes Beispiel sei schließlich Diebstahlschutz und Aktivierung wertvoller elektronischer Handelsgüter angeführt. Die Tags werden auf die Platine (PCB) z.B. eines Handys aufgebracht. Das PCB stellt gleichzeitig die Antenne des Tags bereit. An der Kasse wird das Handy durch die Verpackung hindurch über den Chip freigeschaltet. Gleichzeitig wird der Diebstahlschutz desaktiviert.

5 Zusammenfassung

Laufende Aktivitäten in nationalen und internationalen Standardisierungsgremien und aktuelle Pressemeldungen bestätigen, dass der Markt für UHF zunehmend wachsen wird. Weil der zugrunde liegende Standard ISO/IEC18000-63 an die Pulkerfassung und hohe Geschwindigkeiten zum Erfassen und Auslesen der Tags angepasst ist, während auf Sicherheitsmechanismen weitgehend verzichtet wird, haben wir es uns zum Ziel gesetzt, kryptografische Sicherheitsfunktionen in Form von geeigneten Algorithmen und Protokollen mit der RFID Technologie im UHF Frequenzbereich (868 MHz) zu verbinden.

Nach einer Analyse der Marktsituation im UHF-Umfeld, der Sicherheitsanforderungen der jeweiligen Zielanwendungen und einer Untersuchung technologiebedingter Rahmenbedingungen wie zu überbrückende Entfernungen, Einsatzumgebung, zur Verfügung stehende Energie und Transaktionszeiten haben wir das Rabin-Montgomery Verfahren für sichere UHF Tags ausgewählt und prototypisch implementiert. Das resultierende Verfahren wurde im Normungsgremium SC31/WG7 zur Standardisierung vorgeschlagen.

Literaturhinweise

[1] ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management* — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C (former Part 6C)

[2] ISO/IEC 29167 (all parts), Information technology — Automatic identification and data capture techniques

[3] Michael O. Rabin: Digitalized Signatures and Public-Key Functions as In-tractable as Factorization. MIT-LCS-TR 212, MIT Laboratory for Computer Science, January 1979

[4] P. Montgomery, Modular Multiplication Without Trial Division (http://jstor.org/stable/2007970), Math. Computation, vol. 44, pp 519-521, 1985