Auswahlkriterien für kryptographische Algorithmen bei Low-Cost-RFID-Systemen

Ulrich Kaiser[1] · Christof Paar[2] · Jan Pelzl[2] · Dörte Rappe[3] · Werner Schindler[3] · André Weimerskirch[4] · Thomas Wollinger[2]

[1]Texas Instruments Deutschland GmbH
Haggertystraße 1, D-85350 Freising
d-kaiser@ti.com

[2]Horst Görtz Institut für IT Sicherheit
Ruhr-Universität Bochum, D-44780 Bochum
{cpaar,pelzl,wollinger}@crypto.rub.de

[3]Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189, D-53175 Bonn
{Doerte.Rappe,Werner.Schindler}@bsi.bund.de

[4]escrypt GmbH
Lise-Meitner-Allee 4, D-44801 Bochum
aweimerskirch@escrypt.com

Zusammenfassung

Die Radio Frequency Identification-Technologie (RFID-Technologie) ermöglicht die kontaktlose Identifikation von Objekten ohne Sichtverbindung zwischen Tag und Reader. Diese Eigenschaft erschließt Anwendungen in den unterschiedlichsten Bereichen. Ob der Einsatz kryptographischer Mechanismen notwendig oder zumindest wünschenswert ist, um die Funktionalität des RFID-Systems auch bei Angriffen zu gewährleisten, hängt von der konkreten Applikation ab.
Es wird ein Kriterienkatalog vorgestellt, der von Anwendern und Entwicklern von Low-Cost-RFID-Systemen genutzt werden kann. Er unterstützt Entwickler, kryptographische Mechanismen auszuwählen, die für eine bestimmte (Klasse von) Anwendung(en) geeignet sind, und er hilft Anwendern bei der Entscheidung zwischen verschiedenen in Frage kommenden Systemen.

1 Einleitung

Die Radio Frequency Identification-Technologie (RFID-Technologie) ermöglicht die kontaktlose Identifikation von Objekten. Im Gegensatz zu Barcodes ist keine Sichtverbindung zwischen Reader und Tag erforderlich. Unter einem RFID-System verstehen wir im Folgenden ein RFID-Lesegerät (Reader) und (viele) Tags. Der Reader eröffnet die Kommunikation mit allen Tags, die sich in seiner Sendereichweite befinden, um zunächst deren Identifikationsnummern abzufragen.

Die Daten des RFID-Tags (kurz: Tag) können geändert werden und viele Objekte im Sendefeld eines Readers können nahezu gleichzeitig identifiziert werden (vgl. z.B. [21]). Der sogenannte RFID-Transponder (synonym: RFID-Tag bzw. Tag) wird an ein Objekt angebracht oder ist in dieses Objekt eingebettet. Nur in Ausnahmefällen existiert kein Träger, etwa bei Tags, die bei der Wahrnehmung eines Sendefelds einen aktiven Transponder mit stärkerer Sendeleistung aktivieren (z.B. Passive Entry System). Solche Systeme werden wir nicht weiter verfolgen. Stattdessen befassen wir uns ausschließlich mit Tags, deren primäre Aufgabe in der Identifizierung von Objekten liegt.

Ein Tag besteht aus einer Antenne, einem Energiespeicher und einer integrierten Schaltung (IC). Das IC enthält eine analoge Schaltung zum Empfang und Senden der Daten, einen nichtflüchtigen Speicher und eine Logik-Schaltung für die Ablaufsteuerung. Im einfachsten Fall sendet das Tag seine Identifikationsnummer.

Man unterscheidet zwischen aktiven und passiven Tags. Aktive Tags werden durch eine eigene Batterie mit Energie versorgt, passive Tags besitzen keine eigene Energiequelle. In dieser Arbeit befassen wir uns ausschließlich mit passiven RFID-Transpondern, die wir kurz als Tags bezeichnen.

1.1 RFID: Technik und Anwendungen

Die Tags beziehen ihre Energie aus dem vom Reader erzeugten elektromagnetischen Feld. Die häufigsten Antennenformen sind Kupferbahnen auf Folien, Ferritstäbchen mit Kupferdrahtwicklung, Luftspulen aus Kupferdraht [13] oder im Mikrowellenbereich nur zwei kurze Leiterstücke (je $\lambda/4$, wobei λ die Wellenlänge bezeichnet). Die ICs haben Größen zwischen 0,25 und 10 mm^2 und sind üblicherweise in EEPROM-CMOS-Technik [11] gefertigt. Zur Kommunikation mit Tags wird normalerweise eines von fünf Frequenzbändern genutzt (vgl. Tabelle 1). Im HF-Bereich, beispielsweise, wurde die Übertragungsrate auf 27 Kbps (ISO 15693) bzw. 106 Kbps (ISO 14443) standardisiert. Zur Zeit werden Tags für den Mikrowellenbereich entwickelt. Tags für LF, HF und UHF sind bereits erhältlich.

Im Vergleich zu anderen Funksystemen ist die Reichweite von RFID-Systemen gering. Sie hängt in erster Line von den verwendeten Antennenquerschnittsflächen, aber auch von den erlaubten Sendeleistungen und der Empfindlichkeit der Lesegeräte (im Folgenden der Einfachheit halber nur 'Reader' genannt) ab. Ein passives Abhören der Kommunikation zwischen Tag und Reader ist unter Umständen selbst in einer großen Entfernung (einem Vielfachen der Kommunikationsreichweite) möglich ([3]). Die Mehrzahl der Tags sendet ihre Informationen im Klartext. Es gibt aber auch Tags, die ihre Daten verschlüsselt übertragen. Die eingesetzten Protokolle sind z.B. in den ISO Standards ISO 14443, ISO 15693 und ISO 18000 festgelegt.

	Frequenz	Typische Reichweite	Datenrate
LF	125 – 135 KHz	20 – 200 cm	niedrig
HF	13,56 MHz	10 – 100 cm	mittel/hoch
UHF	868 – 954 MHz	3 – 10 m	mittel/hoch
Mikrowelle	2,45 GHz	3 – 10 m	mittel/hoch
	5,8 GHz	3 – 10 m	mittel/hoch

Tab. 1: RFID Übersicht

Der Preis pro Tag liegt bei hohen Stückzahlen derzeit bei 30 US Cent für den HF und bei einem US Dollar für den LF Bereich. Allerdings hat das MIT AutoID Center über ein 5 Cent Tag spekuliert [17] und damit sehr hohe Erwartungen geweckt, die zumindest in naher Zukunft kaum erfüllt werden dürften. Dennoch werden Tags aufgrund ihrer geringen Größe und des niedrigen Stückpreises bereits heute in vielen Bereichen verwendet. Beispiele für den Einsatz und Nutzen von (nicht notwendigerweise Low-Cost-) RFID-Systemen sind

- *Objektidentifikation*: Identifikation von Tieren einer Herde, Verwaltung von Bibliotheksbeständen, Textilien- und Wäschereilogistik, Identifikation von Autos und Autoreifen (z.B. Michelin), Mülltonnen, ... [24]
- *Elektronischer Zahlungsverkehr:* Mautbezahlung (z.B. California FasTrak), öffentliche Transportmittel (z.B. Octopus Card in Hong Kong), Skipässe (z.B. SkiData), Tankstellen (z.B. SpeedPass), drahtlose Kreditkarten (z.B. Amex ExpressPay), ... [4]
- *Zugangskontrolle und Diebstahlschutz:* Keyless-Entry Lösungen für Automobile, Wegfahrsperren, Gebäudezugangskontrollen, Diebstahlschutz von Supermarktwaren, Automatisierung auf Parkplätzen (Stammkunden), ...
- *Tracking:* Verfolgung von Lastwagen, Paket-Versandsteuerung, Nachverfolgung von Flugzeuggepäck, Containerverfolgung, Containerhafen (Tags im Boden, Singapur), aber auch Produktionsautomatisierung (z.B. BMW Automobilherstellung, Texas Instruments Waferbox [25]), ...
- *Warenlogistik:* Ersatz des Barcodes von der Produktion über Transport- und Warenlagerlogistik hin zum Bezahlvorgang und Reklamationswesen (Hauptinteressenten zur Zeit z.B. Gillette, Walmart und Metro), Paletten, Bierfässer, ...

Mit Tags kann Warenlogistik erheblich effizienter als in der Vergangenheit gestaltet werden. Es ist (z.B.) möglich, alle Objekte einer voll bepackten Palette zu identifizieren und zu zählen, selbst wenn nur ein kleiner Teil der Tags sichtbar ist. Dies ist ein großer Vorteil gegenüber Barcodes. Daher sind große Firmen wie (z.B.) Walmart und Metro an der RFID-Technologie interessiert. Indem sie ihre Lieferanten verpflichten, RFIDs einzusetzen (vgl. z.B. [26]) treiben sie deren Entwicklung und Verbreitung voran.

1.2 Motivation für diese Arbeit und Zielsetzung

Im einfachsten Fall speichert ein Tag eine feste Identifikationsnummer, die es bei ausreichender Energiezufuhr an den Reader sendet. Technisch höherwertige Tags besitzen überschreibbaren, nichtflüchtigen Speicher und können arithmetische oder kryptographische Operationen durchführen. Es liegt auf der Hand, dass es bei bestimmten Anwendun-

gen (z.B. beim Diebstahlschutz) aus Sicht mancher Beteiligter wünschenswert wäre, wenn die vorgesehene Funktionalität des RFID-Systems vollständig ausgeschaltet oder zumindest manipuliert werden könnte. Mit anderen Worten: In solchen Fällen muss mit Angriffen gegen das RFID-System gerechnet werden. Im einfachsten Fall versucht der Angreifer, das Tag vom Objekt zu entfernen oder durch das Umwickeln mit Alufolie vorübergehend funktionsunfähig zu machen. Fortgeschrittene Angriffe bestehen z.B. im Überlagern der Sendefrequenz durch einen Störsender, im Auslesen oder Manipulieren von Tag-Daten und dem Abhören der Kommunikation zwischen Tag und Reader. Ein Angreifer könnte auch versuchen, ein echtes Tag oder den echten Reader vorzutäuschen. Eine Zusammenstellung möglicher Angriffe und Gegenmaßnahmen findet der interessierte Leser z.B. in [21].

In diesem Aufsatz konzentrieren wir uns ausschließlich auf Auswahlkriterien für kryptographische Mechanismen für Low-Cost-RFID-Systeme; andere Schutzmaßnahmen bleiben hier unberücksichtigt. (Implizit beschränken wir unser Augenmerk damit auf Angriffe, die mit kryptographischen Hilfsmitteln verhindert oder zumindest erschwert werden können.) Anders als z.B. in [6, 10, 12] entwickeln oder empfehlen wir keine konkreten Algorithmen. Stattdessen präsentieren wir eine Kriterienkatalog, der unter Berücksichtigung der avisierten Anwendung die Auswahl geeigneter kryptographischer Algorithmen unterstützt.

Low-Cost Tags werden millionen- oder gar milliardenfach produziert und eingesetzt. Zusätzliche Gatter zur Implementierung kryptographischer Mechanismen erhöhen neben der Sicherheit des Systems jedoch auch die Produktionskosten. Der Stückpreis spielt eine herausragende Rolle, und so wird zur Zeit aus Kostengründen vielfach noch auf kryptographische Mechanismen verzichtet [22]. Da die zukünftige Aufgabe eines Tags schon bei dessen Produktion feststeht, erscheint es sinnvoll, noch mehr als bei Chipkarten die kryptographischen Mechanismen gezielt auf die beabsichtigte Applikation zuzuschneiden. Eine ökonomische Algorithmenauswahl sollte neben der Sicherheit der Algorithmen, den grundsätzlichen Risiken und potentiellen Schäden durch erfolgreiche Angriffe auch die Zusatzkosten (in der Produktion und im Wirkbetrieb) berücksichtigen, die sich durch die kryptographischen Mechanismen ergeben, sowie die Motivation und das Knowhow eines potentiellen Angreifers bedenken. In bestimmten Einsatzszenarien kann es sich als sinnvoll herausstellen, schwächere, aber preisgünstigere Algorithmen einzusetzen, wenn der befürchtete Schaden nur gering ist. Die Motivation eines Angreifers kann monetärer Natur sein, aber vielleicht ist es auch nur ein Gewinn an Ansehen oder Geltungssucht. Überschreitet der zeitliche und finanzielle Aufwand eines Angriffs ein gewisses Maß, dürften monetäre Interessen im Vordergrund stehen.

Dieser Ansatz steht im Gegensatz z.B. zu sensitiven Chipkartenapplikationen, etwa Signaturanwendungen oder elektronische Geldbörsen, bei denen Hochsicherheitsanforderungen erfüllt werden müssen, was insbesondere starke, nach dem aktuellen Know-how unüberwindbare kryptographische Mechanismen erfordert.

Im zweiten Kapitel wird ein Kriterienkatalog vorgestellt, der verschiedene Aspekte anspricht und präzisiert. Er kann von Anwendern und Entwicklern von RFID-Systemen genutzt werden. Er unterstützt Entwickler, zielgerichtet kryptographische Mechanismen auszuwählen, die für eine bestimmte (Klasse von) Anwendungen zugeschnitten sind, ohne dass dabei wichtige Aspekte unberücksichtigt bleiben. Großabnehmer können eventuell

Einfluß auf die Ausgestaltung ihrer Systeme nehmen. Abnehmern kleinerer Mengen an Tags bietet der Kriterienkatalog eine Entscheidungshilfe beim Kaufentscheid.

Wir stellen die grundsätzliche Herangehensweise in den Vordergrund und nicht konkrete kryptographische Algorithmen, da deren Einsatz entscheidend von der zur Verfügung stehenden Technik abhängt und sich diese in den kommenden Jahren sicher weiterentwickeln wird. Die Kriterien werden in Kapitel 3 auf ein Beispiel angewandt. Direkte Angriffe gegen den Reader (z.B. Hardwareangriffe) und gegen das Hintergrundsystem werden im Folgenden nicht berücksichtigt.

2 Kriterien zur Auswahl kryptographischer Mechanismen

Es werden verschiedene Aspekte angesprochen, die zur applikationsabhängigen Auswahl geeigneter kryptographischer Mechanismen und beim Kaufentscheid eines RFID-Systems relevant sind.

2.1 Angriffsziele

Dieser Abschnitt spricht mögliche Ziele eines Angreifers an, die (zumindest auch) durch kryptographische Mechanismen und / oder Eigenschaften der Tags verhindert oder zumindest erschwert werden können. Das unerlaubte Entfernen von Tags oder das Abschirmen durch Alufolie gehören beispielsweise nicht dazu. Man beachte, dass nicht für jede Anwendung alle Aspekte relevant sind.

- Angriffe gegen den Tag bzw. dessen Daten
  - Auslesen von Tag-Daten
  - Ändern von Tag-Daten
  - Klonen existierender Tags, Erstellen neuer Tags
- Angriffe gegen die Kommunikation zwischen Tag und Reader
  - Kommunikation mitlesen
  - Man-in-the-Middle Attack
  - Vortäuschen eines echten Tags
  - Vortäuschen des authentischen Readers

2.2 Angriffsarten

'Logische' Angriffe nutzen fehlende oder unzureichende algorithmische (kryptographische) Schutzmechanismen aus. Das Auslesen, Mitlesen oder Verändern von Daten erfolgt auf dem hierfür (wenngleich nicht für den Angreifer) vorgesehenen Weg. Daneben gibt es Angriffe, die (auch) die Eigenschaften der Tag-Hardware explizit berücksichtigen. Man darf vermuten, dass Low-Cost Tags im Allgemeinen anfällig gegen Hardwareangriffe, Seitenkanalangriffe und Fault Attacken sind. Da solche Angriffe neben großer Expertise auch einen nicht zu unterschätzenden Aufwand erfordern, dürften sie aus Sicht eines

Angreifers nur dann interessant sein, falls die Kompromittierung eines einzelnen Tag-Schlüssels Auswirkungen auf eine große Anzahl weiterer Tags hat oder die Daten des kompromittierten Tags besonders sensitiv sind.

- 'logische' Angriffe gegen Daten im Tag oder im Rahmen der Kommunikation
- Hardwareangriffe, Seitenkanalangriffe, Fault-Attacken gegen das Tag

2.3 Angreifermodell

Um die Wahrscheinlichkeit für erfolgreiche Angriffe einschätzen zu können, sollte man sich zunächst ein Bild über die Motivation des Angreifers, seinen potentiellen Nutzen (vgl. Abschnitt 2.6), seine Expertise und seine finanziellen Mittel machen. Der Einsatz von ASICS, die speziell zu diesem Zweck gefertigt werden, dürfte sich höchstens in sehr speziellen Szenarien lohnen. Innerhalb der einzelnen Spiegelpunkte trennen Kommata alternative Ausprägungen eines Merkmals.

- Außentäter, Innentäter
- Einzeltäter, kriminelle Organisation
- Systemkenntnis: keine Kenntnisse, Kenntnis der Algorithmen und Eigenschaften der genutzten Tags, Kenntnis der verwendeten kryptographischen Schlüssel
- vermutetes Equipment des Angreifers: Laptop oder Standard-PC mit kommerziellem Computeralgebrasystem, Workstation, FPGAs, ASICs
- vermutete Expertise: IT-Laie, IT-Fachmann, Experte Kryptographie und RFID-Technik

2.4 Daten im Tag, Kommunikationsdaten, kryptographische Absicherung

Mit kryptographischen Mechanismen kann man Tag-Daten und die Kommunikation zwischen Tag und Reader gegen Auslesen, Fälschung und Verfälschung sichern. Der Angriff auf einen Schlüssel oder ein Passwort kann die erste Stufe eines komplexeren Angriffs darstellen.

Am Ende dieses Abschnitts werden verschiedene sicherheitsrelevante Eigenschaften der im Tag gespeicherten Daten und der Kommunikation zwischen Tag und Reader angesprochen. Diese Eigenschaften sind für eine Sicherheitsbewertung relevant. Sie haben Einfluss darauf, wie schwierig ein Angriff ist und welchen Aufwand er erfordert. Auch der erwartete Schaden durch einen erfolgreichen Angriff und die Zusatzkosten, den die kryptographischen Mechanismen bei der Produktion und im Einsatz verursachen, hängen hiervon ab.

Einheitsschlüssel oder gruppenspezifische Schlüssel für große Mengen an Tags (z.B. für die gesamte Jahresproduktion eines großen Abnehmers) bergen gegenüber Angreifern mit Expertise auf dem Feld der Kryptographie und der RFID-Technologie Risiken, selbst wenn starke kryptographische Algorithmen eingesetzt werden. Dies liegt darin begründet, dass Low-cost Tags vermutlich nur geringen Schutz gegen Hardware-, Fault- und Seitenkanalangriffe bieten.

Grundsätzlich kann man diese Risiken durch Tag-individuelle Schlüssel (oder gruppenspezifische Schlüssel für kleine Gruppen) mindern. Applikationsabhängig kann man sogar

über schwächere kryptographische Mechanismen (mit preisgünstiger Implementierung!) nachdenken. Allerdings erfordern Tag-individuelle Schlüssel auch Mehrkosten bei der Produktion. Werden die Tag-Schlüssel mit einem Masterkey abgeleitet, muss der Schlüsselableitungsmechanismus (z.B. die AES-Verschlüsselung der Tag-ID bzw. Teile hiervon, falls Gruppen von RFIDs identische Schlüssel besitzen sollen) für jedes einzelne Tag ausgewertet werden. Dies könnte einen nicht zu unterschätzenden 'Flaschenhals' darstellen. Es liegt auf der Hand, dass der Schlüsselableitungsmechanismus auf jeden Fall stark sein sollte, selbst wenn dies auf die von den Tags genutzten Algorithmen nicht zutrifft. Ferner muss der Masterkey zuverlässig verwaltet werden, und der Reader muss vor jeder Kommunikation mit einem Tag ebenfalls einmal den Schlüsselableitungsmechanismus auswerten.

Bei gruppenspezifischen Schlüsseln oder Passwörten ist die Größe der Gruppe von Interesse. Sie beeinflusst sowohl den Aufwand für die Produktion als auch die Sicherheit. Können Tag-Daten verändert werden, spielen die Zugriffsrechte eine wichtige Rolle. (Zur Notation: 'Authentisierung: Tag $\mapsto$ Reader' bedeutet, dass sich der Tag gegenüber dem Reader authentisiert, nicht aber umgekehrt.)

- im Tag gespeicherte Daten
  - identische Nutzdaten für alle Tags, gruppenspezifische Nutzdaten, Tag-individuelle Nutzdaten
  - Nutzdaten: nicht verschlüsselt, verschüsselt
  - kein Passwort, identisches Passwort für alle Tags, gruppenspezifisches Passwort, Tag-individuelles Passwort
  - keine kryptographischen Schlüssel, identische Schlüssel für alle Tags, gruppenspezifische Schlüssel, Tag-individuelle Schlüssel
  - Read-only-Tag, Nutzdaten können hinzugefügt werden, Nutzdaten können hinzugefügt oder überschrieben werden
- übertragene Daten
  - Einheitsantwort (z.B. Produktname), Tag-individuelle Antwort (z.B. Verfallsdatum)
  - Länge der übertragenen Nachrichten: Tag $\rightarrow$ Reader, Tag $\leftarrow$ Reader
  - Verschlüsselung: keine Verschlüsselung, Tag $\rightarrow$ Reader, Tag $\leftarrow$ Reader, Tag $\leftrightarrow$ Reader
  - Authentisierung: keine Authentisierung, Tag $\rightarrow$ Reader, Tag $\leftarrow$ Reader, Tag $\leftrightarrow$ Reader
  - Integritätssicherung: keine Integritätssicherung, Tag $\rightarrow$ Reader, Tag $\leftarrow$ Reader, Tag $\leftrightarrow$ Reader

2.5 Schaden durch einen erfolgreichen Angriff

Der Schaden, den ein erfolgreicher Angriff verursacht, hängt insbesondere davon ab, wie viele Tags durch einen kompromittierten Schlüssel bzw. durch ein kompromittiertes Passwort gefährdet sind.

- Anzahl der gefährdeten Tags pro kompromittiertem kryptographischen Schlüssel bzw. Passwort

- finanzieller Schaden pro Tag
- erwarteter Gesamtschaden: (Schaden pro Tag) * (Anzahl gefährdeter Tags pro kompromittiertem Schlüssel bzw. Passwort) + Folgeschäden durch Imageverlust

2.6 Angreifer: Aufwand und Nutzen

Der Nutzen, den ein erfolgreicher Angriff verspricht, beeinflußt die Motivation und das Interesse potentieller Angreifer und damit insbesondere den Aufwand an Zeit und Geld, den sie zu investieren bereit ist (vgl. auch Abschnitt 2.3).

- Nutzen / Motivation des Angreifers: finanzieller Gewinn, Prestige (z.B. Hacker), Sabotage (z.B. frustrierter Mitarbeiter, Konkurrenz)
- Zeitaufwand für einen erfolgreichen Angriff: Setup-Time (Informationsgewinnung, Implementierung von Angriffsprogrammen, ggf. Programmierung von FPGAs etc.), Zeit für Schlüsselbestimmung, ggf. Zeit zur Durchführung weiterer Attacken (etwa nach Ermittlung eines globalen oder gruppenspezifischen Schlüssels)
- Kosten für das technische Equipment

2.7 Zusatzkosten durch Kryptographie

Wir unterscheiden zwischen Zusatzkosten in der Produktion und im Einsatz. Aus Sicht des Anwenders bedingen zusätzliche Produktionskosten auch höhere Anschaffungskosten.

- Implementierung:
  - Aufwand in Gattern und Speicherbits
  - Produktionszusatzkosten durch kryptographische Mechanismen
- Zusatzkosten im Wirkbetrieb:
  - zusätzliche Energiekosten
  - Performanceverlust durch kryptographische Operationen
  - (bei langlebigen Tags:) ggf. Kosten für einen Schlüsselwechsel

2.8 Kryptographische Mechanismen

Dieser Abschnitt befasst sich mit Kenngrößen kryptographischer Algorithmen und Protokolle. Algorithmus, Schlüssellänge und Implementierung beeinflussen die Kenngrößen und sind daher als Einheit zu sehen und sollten unter Berücksichtigung der avisierten Applikationen und der vorgesehenen Hardware ausgewählt werden. Eine vollständige und umfassende Untersuchung aller in Frage kommenden Algorithmen würde den Rahmen dieser Veröffentlichung weit übersteigen. Vielmehr soll in diesem Abschnitt das grundsätzliche Vorgehen illustriert werden. Die Kenngrößen der berücksichtigten Algorithmen sollen einen groben Überblick über deren Komplexität vermitteln. Bei einer konkreten Implementierung eines Algorithmus müssen die Komplexität und die hieraus entstehenden Mehrkosten unter Berücksichtigung der zur Verfügung stehenden Technologie ermittelt werden. Bei der Anschaffung eines RFID-Systems schlagen die Kenngrößen indirekt über den Anschaffungspreis und ggf. über höhere Betriebskosten oder Performanceverluste des Systems zu Buche. Da die technologische Entwicklung der Tags in den kommenden Jahren sicherlich voranschreiten wird, könnte sich die Algorithmenwahl für den gleichem

Einsatzzweck im Lauf der Jahre ändern. Aus diesem Grund berücksichtigen wir neben mehreren symmetrischen Verfahren auch aufwendigere asymmetrische Verfahren.

In der Literatur findet man eine Vielzahl von Veröffentlichungen über Implementierungen symmetrischer Algorithmen und Hashfunktionen. Es besteht zudem die Möglichkeit, IP Cores dieser Algorithmen von verschiedenen Firmen zu erwerben (z.B. Amphion, Helion Technologies, SiWorks, Barco-Silex, Elliptic Semiconductor, sci-worx GmbH). Die in der nachfolgenden Liste aufgeführten Leistungskenngrößen beziehen sich hauptsächlich auf diese kommerziellen Produkte. Grundsätzlich kann man mit größeren Hardwareressourcen den Durchsatz erhöhen. Allerdings wird man für Tags normalerweise Implementierungen bevorzugen, die wenige Gatter benötigen, da man i.d.R. keine großen Datenmengen verschlüsseln muss. Daher haben wir in unserer Aufstellung Implementierungen mit sehr geringem Ressourcenbedarf berücksichtigt.

Für asymmetrische Algorithmen steht vergleichsweise wenig Literatur zur Verfügung und kommerziell erhältliche Produkte sind hauptsächlich auf einen hohen Datendurchsatz optimiert und daher für unsere Zwecke ungeeignet. Wir haben daher eine Methodik entwickelt, die eine zuverlässige Aufwandsabschätzung für low-cost Applikationen ermöglicht. Die zentralen Ideen werden im folgenden grob skizziert.

Wir betrachten die Dekomposition der ausgewählten Algorithmen über elementaren Einheiten wie z.B. Speicher, Arithmetik für Addition, Multiplikation, etc. Für die Beschreibung dieser Einheiten verwenden wir Resultate aus der Literatur, um den Bedarf an Gattern und die Laufzeit zu erhalten (z.B. [1]). Der Fokus liegt hierbei insbesondere auf AT (Fläche-Zeit) optimalen Implementierungen. So nehmen wir beispielsweise bei der modulare Addition und Multiplikation von großen Operanden eine wortweise (sequentielle) Durchführung an, welche flächensparend ist. Für die modulare Multiplikation, welches i.A. die zeitkritische Operation ist, verwenden wir Kenngrößen aus der Referenz [19], in welcher eine effiziente und skalierbare Architektur hierfür vorgestellt wird. Alle elementaren Operationen sollen mit aus der Literatur bekannten Standard-Verfahren (siehe [14]) berechnet werden. Letztlich steht es hier dem RFID-Entwickler frei, in Spezialfällen auf besonders effiziente Algorithmen auszuweichen (z.B. bei speziellen Primkörpern für ECC).

Die verwendeten Algorithmen benötigen meist (schnelle) Speicher für Zwischenergebnisse. Wir gehen hierbei einheitlich von einer Realisierung mittels D-FlipFlops aus (5 Gatter pro Bit). Bedingt durch die Applikation und die Hardware-Plattform kann evtl. auch ein anderer Speichertyp (z.B. SRAM, DRAM) verwendet werden.

Sind die Kenngrößen der elementaren Operationen bekannt, kann die Laufzeit und der Bedarf an Transistoren abgschätzt werden. Für wichtige asymmetrische Verfahren haben wir mehrere für RFID in Frage kommende Alternativen angegeben, um die Abwägung zwischen Ressourcenverbrauch und Rechenzeit zu verdeutlichen. Hierbei kann letztlich der RFID-Entwickler aufgrund seiner Vorgaben die für ihn optimale Wahl treffen.

Die nachfolgende Aufstellung gibt einen Überblick über die Geschwindigkeit und den schaltungstechnischen Aufwand einiger ausgewählter symmetrischer und asymmetrischer Verfahren. Unter einem *GE (gate equivalent)* verstehen wir ein NAND Gatter mit 2 Eingängen, welches sich in Standard CMOS Technologie mit 4 Transistoren realisieren lässt. Wie bereits erwähnt, ist die Liste der untersuchten Algorithmen keineswegs vollständig. Tatsächlich wurden in der Vergangenheit immer wieder asymmetrische Algo-

rithmen vorgeschlagen, die zumindest in Bezug auf einige Kenngrößen performanter als RSA oder elliptische Kurven sind (vgl. z.B. [8, 5]). Mit diesen Vorschlägen sollte oftmals (u.a.) den eingeschränkten Ressourcen von Chipkarten Rechnung getragen werden. Eine zuverlässige Sicherheitsbewertung ist in vielen Fällen schwierig, da die Algorithmen noch nicht hinreichend untersucht worden sind oder sich bereits bestimmte Parametersätze als schwach erwiesen haben. Es würde weit über die Zielsetzung dieser Publikation hinausgehen, wenn wir uns dieser Fragestellung auch nur ansatzweise nachgingen. Dass 256-Bit-RSA selbst gegenüber Angreifern mit geringen Ressourcen nur äußerst kurzfristige Sicherheit gewährleisten kann, ist allgemein bekannt. Wir haben trotzdem diese Modulgröße berücksichtigt, um der Rechenleistung sehr kleiner Schaltungen Rechnung zu tragen und um einen Eindruck des Zusammenhangs von Schlüssellänge und Leistungskenngrößen zu vermitteln.

Verwendet man asymmetrische Algorithmen und Mechanismen, erfordert dies normalerweise zusätzlich Zertifikate (insofern der öffentliche Schlüssel des Readers nicht fest im Tag gespeichert ist etc.) und ggf. das Berechnen eines Hashwertes (Signaturanwendung). Zumindest derzeit erscheint dies für Low-Cost-Tags (zu) aufwendig, zumal normalerweise nur sehr kurze Nachrichten zwischen Tag und Reader ausgetauscht werden. Verschiedene Autoren haben Algorithmen und Protokolle vorgeschlagen, die auf die Bedürfnisse spezieller Anwendungen zugeschnitten sind und den technischen Möglichkeiten von Low-Cost-Tags Rechnung tragen sollen ([7, 10, 12] etc.).

Dass die Ressourcen eines Tags beschränkt sind und nur kurze Datensätze ausgetauscht werden, sollte man stets im Auge behalten. Anders als bei der Verschlüsselung oder Signatur großer Datenmengen spielt hier der Initialisierungsaufwand des Algorithmus keine untergeordnete Rolle. Bei geschlossenen RFID-Systemen bietet sich der Einsatz symmetrischer Algorithmen an, bzw. Protokolle, welche symmetrischen Algorithmen verwenden. Besitzen die Tags individuelle Schlüssel, bietet sich eine Schlüsselableitung mit einem Masterkey an, der im Reader gespeichert ist. Ein solches Vorgehen ist von geschlossenen Chipkartensystemen bekannt. Tag-individuelle Schlüssel erfordern dann keine zusätzliche Speicher- oder Rechenleistung im Tag.

Symmetrische Algorithmen

- AES
  - Leistungskenngrößen:a)100 Mbps, 8.000 KGE [CLP-11 von Elliptic Semiconductor];
    b) IP Cores: AES core mit 2.9 KGE;
    c) [2] (Zahlenwerte speziell auf Tags zugeschnitten): Stromverbrauch 8.15 μA, 1.25 Mbps bei 10 MHz, 3.595 KGE.
  - Sicherheitsniveau: gilt derzeit als uneingeschränkt sicher
- DES
  - Leistungskenngrößen: a) [18]: 1.1 - 3.2 Gbps, 6 - 17 KGE
    b) sci-worx GmbH: IPcore TSMC13 mit 3.8 Mbps, 3.4 KGE
  - Sicherheitsniveau: mit entsprechendem Aufwand überwindbar; zum Schutz sicherheitskritischer Daten nicht mehr geeignet
- Triple-DES
  - Leistungskenngrößen: ca. Verschlüsselungsrate(DES)/3 bei gleicher GE-Anzahl [18]

  - Sicherheitsniveau: gilt derzeit als uneingeschränkt sicher
- k lineare Schieberegister über GF(2) mit nichtlinearer Combinerfunktion (Stromchiffre)
  - Leistungskenngrößen: z.B. 10 Mbps bei 10MHz; $(n_1 + \cdots + n_k) \cdot 12$ GE für k Schieberegister der Länge $n_1, \ldots, n_k$; Tabelle für Combinerfunktion (max. 40 GE für z.B. $k = 3$)
  - Sicherheitsniveau: Einzelfallbetrachtung (siehe z.B. [16], einführende Literatur)

Asymmetrische Algorithmen

- RSA
  - Leistungskenngrößen: Laufzeit z.B. 4Kbps bei 100MHz mit 5.3KGE (256 Bit), 1Kbps bei 100MHz mit 10KGE (512 Bit), 256bps bei 100MHz mit 67KGE (1024 Bit).
  - Sicherheitsniveau: 1024 Bit: gilt als derzeit sicher; 512 Bit: Modul kann mit großem Aufwand und Expertise faktorisiert werden; 256 Bit: Modul kann mit geringem Aufwand in kurzer Zeit faktorisiert werden.
- Elliptische Kurven über Primkörpern
  - Leistungskenngrößen: a) Laufzeit: 19.2Kbps bei 100MHz mit 20KGE (192 Bit). b) [15]: 5Kbps bei 0.99mW Leistungsverbrauch bei 20MHz mit 30KGE.
  - Sicherheitsniveau (192-Bit ECC, Signaturfunktionalität): wird in [23] mit Skipjack (symmetrischer Algorithmus mit 80-Bit-Schlüssel) verglichen
  - Anmerkung: Signaturerzeugung deutlich schneller, Signatur und Signaturschlüssel kürzer als bei RSA; Signaturprüfung langsamer als RSA mit kleinem öffentlichen Exponenten
- Vorschlag von Girault und Lefranc [7]
  - Funktionalität: einseitige RFID-Authentikation
  - Anmerkung: berechnet pro Authentikation eine Langzahladdition online; basiert auf GPS-Verfahren von Girault ([6])
  - Leistungskenngrößen: (z.B.) 1920-Bit-Integer-Addition (effektiv; S=160) bitseriell mit Volladdierer in 190 μsec bei 10MHz mit ca. 1 KGE; + zusätzlicher Speicher
  - Nachteile (Effizienz): benötigt vorausberechnete Werte ($\rightarrow$ insbes. zusätzlicher Speicher), relativ großer Kommunikationsaufwand

Hashfunktionen

- SHA-1
  - Leistungskenngrößen: 1264 Mbps, 17 KGE [Amphion IP core, 180 nm]

3 Fallbeispiel

Wir erläutern an einem Beispiel die Bedeutung und die Anwendung der Kriterien, die im zweiten Kapitel erarbeitet wurden. Wir nehmen an, dass die Bücher einer Bibliothek mit RFID-Tags ausgestattet werden sollen. Die Tags sollen Diebstahl verhindern und das Wiederfinden fehlerhaft einsortierter Bücher erleichtern. Handelt es sich um eine

Leihbibliothek, soll zudem die Verwaltung der ausgeliehenen Bücher vereinfacht werden. Der Wert der Bücher bewegt sich zwischen wenigen Euro und mehreren hundert Euro.

Einsatzszenarien:

a) Präsenzbibliothek mit Reader am Ausgang: reiner Diebstahlschutz; Tag enthält keine individuellen (Nutz-)Daten

b) Das RFID-System soll das Auffinden (versehentlich oder bewusst) fehlerhaft einsortierter Bücher erleichtern, um diese den übrigen Besuchern der Bibliothek wieder zugänglich zu machen. Neben seiner Identifikationsnummer speichert das Tag Nutzdaten. Ein Bibliotheksmitarbeiter kann mit Hilfe eines speziell programmierten Readers fehlende Bücher aufspüren.

c) Leihbibliothek: Ein Reader am Ausgang stellt fest, ob nur ordnungsgemäß entliehene Bücher mitgenommen werden. Ein negatives Prüfergebnis könnte z.B. durch ein akustisches Signal angezeigt werden. Das Tag enthält eine Identifikationsnummer, die das System eindeutig dem zugehörigen Buch und damit weiteren Nutzdaten zuordnet. Der Bibliotheksangestellte kann beim Entleihen Daten in das Tag schreiben (z.B. das Rückgabedatum, Name des Entleihers).

Da selbst alle Bibliotheken einer großen Universität zusammen keine exorbitant großen Mengen an Tags benötigen, bedeutet dies, dass der für die Beschaffung Verantwortliche nicht die Entwicklung eines speziell für seine Bedürfnisse zugeschnittenen Systems initiieren kann, sondern sich für ein auf dem Markt befindliches RFID-System entscheiden muss. Insbesondere muss er die Frage klären, ob kryptographische Mechanismen notwendig sind, um die vorgesehene Funktionalität des Systems sicherzustellen. Wird dies bejaht, ist zu klären, welches System für die vorgesehene Anwendung am geeignetsten ist. Der Kriterienkatalog unterstützt die Entscheidungsfindung.

Am Anfang steht die Auswertung von Erfahrungswerten aus den vergangenen Jahren, was die Schäden durch Diebstahl oder fehlerhaft einsortierte Bücher betrifft. Unter anderem auf Grundlage dieser Daten erstellt der Verantwortliche eine Prognose über die voraussichtliche Lebensdauer der Tags.

In allen Szenarien besteht ein nahe liegendes Ziel eines Angreifers darin, den Tag funktionsunfähig zu machen. Wir verfolgen diesen Aspekt nicht weiter und verweisen z.B. auf [21]. Weitere Zielsetzungen sind das gezielte Verändern von Tag-Daten (Szenarien b) und c)) oder (in Kombination mit dem Angriffsziel, den Tag unbrauchbar zu machen) den Reader durch ein gefälschtes Tag zu täuschen.

Die Annahmen über die Motivation, die Fähigkeiten und das technische Equipment potentieller Angreifer sollten eigene Erfahrungen und die Erfahrungen anderer Bibliotheken (welche ggf. bereits mit einem RFID-System ausgestattet sind) berücksichtigen. Da es sich nach obiger Annahme um keine sehr teuren Bücher handelt und sich der Verkauf gestohlener Fachbücher mit Bibliotheksstempel schwierig gestalten dürfte, kann man von IT-Laien (Normalfall), unter Umständen aber auch IT-Fachleute oder Experten auf dem Feld der Kryptographie und RFID-Technik (z.B. bei einer Bibliothek im Fachbereich Informatik) ausgehen, die für den 'Eigenbedarf' stehlen, aber kaum von bandenmäßig organisiertem Diebstahl. Aus dem Verstellen von Büchern lässt sich ohnehin kein finanzieller Gewinn erzielen.

Innerhalb der Bibliothek verfügt der Angreifer vermutlich bestenfalls über einen Laptop. Zur Vorbereitung des Angriffs stehen unter Umständen mehr Ressourcen zur Verfügung, etwa eine Workstation oder ein leistungsstarker Universitäts-Großrechner. Vom Einsatz von Spezialhardware ist dagegen kaum auszugehen. Die Zeit, die ein Angreifer bereit ist, für einen erfolgreichen Angriff aufzuwenden, hängt eng mit seinem Nutzen zusammen. Vermutlich wird ein Angreifer nicht mehr als einige Tage für einen erfolgreichen Angriff aufwenden wollen.

Müssen die Tag-Daten während der Lebensdauer des Tags nicht verändert werden, bietet sich ein Read-Only-Tags an, was ein Verändern dieser Daten verhindert. Speichert der Tag veränderbare Nutzdaten, kann einem unbefugten Verändern dieser Daten entgegengewirkt werden, indem sich der Reader gegenüber dem Tag authentisiert. Eine Authentikation der Tags gegenüber dem Reader wirkt Totalfälschungen von Tags entgegen. Ob die übertragenen Daten zusätzlich verschlüsselt werden müssen, hängt von der dem Authentikationsmechanismus und ggf. von der Natur dieser Daten ab. Eine einseitige Reader – Tag-Authentikation oder eine gegenseitige Reader – Tag-Authentikation kann durch symmetrische Mechanismen gewährleistet werden, falls Reader und Tag über einen gemeinsamen Schlüssel verfügen (vgl. Abschnitt 2.8).

Wie bereits in Kapitel 2 erläutert, ist für eine Risikoabschätzung nicht nur relevant, wie schwierig ein Angriff ist, sondern auch, wie groß der erwartete Schaden ist. Wie groß der Schaden durch einen kompromittierten Tag-Schlüssel ist, hängt davon ab, ob (i) alle Tags denselben Schlüssel besitzen oder (ii) jedes Tag über einen individuellen Schlüssel verfügt. Die Folgen eines Angriffs bei (i) können weitaus gravierender sein als bei (ii), da die kryptographischen Mechanismen gegenüber diesem Angreifer keinen Schutz mehr bieten. (Bei (ii) kommt natürlich dem Schutz des Masterkeys eine besondere Bedeutung zu. Dieser ist allerdings nicht in den Tags, sondern im Reader gespeichert.) Umgekehrt beeinflußt der Nutzen für den Angreifer dessen Interesse an einem Angriff.

Der Bibliotheksverantwortliche muss sich zwischen verschiedenen RFID-Systemen entscheiden. Die preiswerteste Variante ist vermutlich diejenige, die vollständig auf kryptographische Algorithmen verzichtet. Möglicherweise kann er zwischen weiteren RFID-Systemen auswählen, deren kryptographische Funktionalität (einseitige bzw. beidseitige Authentikation, ggf. Verschlüsselung) für den Einsatzzweck geeignet ist. Er vergleicht die jeweiligen Beschaffungs- und Betriebskosten mit den zu erwartenden Schäden (vgl. Abschnitt 2.5) und den Ersparnissen (Verringerung von Verwaltungskosten) im Lebenszyklus der Tags. Hierbei geht die Stärke der kryptographischen Mechanismen ebenso ein wie die Annahmen über die Möglichkeiten und das Verhalten eines typischen Angreifer und die Konsequenzen eines erfolgreichen Angriffs.

Um eine konkrete Rangfolge zu erstellen, benötigt man (hier: der Bibliotheksverantwortliche) konkretes Zahlenmaterial. Wir belassen es daher bei allgemeinen Hinweisen zum grundsätzlichen Vorgehen.

4 Resümee

Die Verbreitung und die Bedeutung von Low-Cost RFID-Tags wird in den kommenden Jahren weiter zunehmen. Derzeit wird auf kryptographische Mechanismen noch weitestgehend verzichtet. Abhängig von der konkreten Applikation und den damit verbundenen

Missbrauchsrisiken kann der Einsatz kryptographischer Mechanismen ratsam sein. Da die Aufgaben eines Tags bei dessen Produktion schon feststehen, liegt es nahe, gerade bei Low-Cost Tags eine ökonomische Auswahl der kryptographischen Mechanismen vorzunehmen, die Kosten und Risiken berücksichtigt und abwägt. Die vorliegende Arbeit präsentiert einen Kriterienkatalog, der Entwickler und Systembetreiber bei ihren Entscheidungen unterstützen soll.

Literatur

[1] L. Batina, J. Lano, N. Mentens, B. Preneel, I. Verbauwhede: Energy, Performance, Area versus Security Trade-offs for Stream Ciphers. In: *P*roceedings of SASC 2004 – The State of the Art of Stream Ciphers (ECRYPT Workshop), 302–310.

[2] M. Feldhofer, S. Domenikus, J. Wolkerstorfer: Strong Authentication for RFID-Systems Using the AES Algorithm. In: M. Joye, J.-J. Quisquater (Hrsg.): *Cryptographic Hardware in Embedded Systems — CHES 2004*, Springer, LNCS 3156, Berlin 2004, 357–370.

[3] T. Finke, H. Kelter: Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. http://www.bsi.de/fachthem/rfid/index.htm

[4] K. Finkenzeller, Kontaktlose Chipkarten, *Funkschau* 19, 1998, http://www.rfid-handbook.de/downloads/fs9819040.pdf

[5] G. Gaubatz, J.-P. Kapsa, Berk Sunar: Public Key Cryptography in Sensor Networks–Revisited. Erscheint in: C. Casteluccia, H. Hartenstein, C. Paar, D. Westhoff (Hrsg.): *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, Springer, LNCS 3313, Berlin 2005.

[6] M. Girault: Self-certified Public Keys. In: D.W. Davies (Hrsg.): Eurocrypt '91, Springer, LNCS 547, Berlin 1991, 491–497.

[7] M. Girault, D. Lefranc: Public Key Authentication with One (Online) Single Addition. In: M. Joye, J.-J. Quisquater (Hrsg.): *Cryptographic Hardware in Embedded Systems — CHES 2004*, Springer, LNCS 3156, Berlin 2004, 413–427.

[8] J. Hoffstein, J. Pipher, J.H. Silverman: NTRU: A Ring-Based Public Key Cryptosystem. In: J.P. Buhler (Hrsg.): *Algorithmic Number Theory — ANTS III*, Springer, LNCS 1423, Berlin 1998, 267–288.

[9] M. Jakobsson and D. Pointcheval. Mutual Authentication for Low-Power Mobile Devices. In: P. Syverson (Hrsg.): *Proceedings of Financial Cryptography 2001*, LNCS 2339, Springer 2001, 178–195.

[10] A. Juels: Minimalist Cryptography for Low-Cost RFID Tags. Erscheint in: C. Blundo, S. Cimato (Hrsg.): *S*ecurity in Communication Networks — SCN 2004, Springer, LNCS 3352, Berlin 2005.

[11] U. Kaiser, W. Steinhagen: A Low Power Transponder IC for High Performance Identification Systems. *IEEE Journal of Solid-State Circuits*, JSSC 30, 1995, 306–310.

[12] U. Kaiser: Universal Immobilizer Crypto Engine, UICE, the Little Brother of AES. In: *AES4 Conference*, Bonn 2004. Folien: http://www.aes4.org/english/events/aes4/downloads/AES4_UICE_slides.pdf

[13] C. Kern: RFID-Technology - Recent Development and Future Requirements. In: C. Beccari (Hrsg.): *European Conference on Circuit Theory and Design*, ECCTD'99, Workshop Proceedings, 25–28.

[14] A.J. Menezes, P.C. van Oorschot und S.A. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, USA, 1997.

[15] E. Öztürk, V. Sunar und E. Savaş: Low-Power Elliptic Curve Cryptography Using Scaled Modular Arithmetic. In: M. Joye u. J.-J. Quisquater (Hrsg.): *C*ryptographic Hardware and Embedded Systems - CHES 2004, Springer, LNCS 3156, Berlin 2004, 92–106.

[16] R. Rueppel: Analysis and Design of Stream Ciphers. Springer, New York, 1986.

[17] S. Sarma: Towards the 5 Cent Tag. *Auto-ID Center*, White paper, Feb. 2002. http://www.autoidlabs.org/whitepapers/MIT-AUTOID-WH-006.pdf

[18] S. Shimizu, H. Ishikawa, A. Satoh, T. Aihara: On-demand design service innovations. IBM Journal Research and Development 48 (no. 5/6), 2004.

[19] A.F. Tenca and Ç.K. Koç: A Scalable Architecture for Modular Multiplication Based on Montgomery's Algorithm. *IEEE Transactions on Computers* 52 (no.9), 2003, 1215 – 1221.

[20] D.S. Wong and A.H. Chan: Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices. In: Boyd (Hrsg.): *Asiacrypt 2001*, Springer, LNCS 2248, Berlin 2001, 272–289.

[21] Risiken und Chancen des Einsatzes von RFID-Systemen. Studie, Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Secumedia-Verlag, Ingelheim 2004. Auch: http://www.bsi.bund.de/fachthem/rfid/studie.htm

[22] EPCglobal, Class-1, Generation-2, UHF RFID, Specification 1.0.6

[23] NIST: Digital Signature Standard (DSS). FIPS PUB 186-2 (27.01.2000) with Change Notice 1 (5.10.2001). csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[24] Texas Instruments: http://www.ti.com/tiris/docs/applications/applications.shtml

[25] Texas Instruments: http://www.ti.com/tiris/docs/manuals/RFIDNews/Tiris_NL16.pdf

[26] Wal-Mart (Pressrelease vom 30. April 2004) http://www.walmartstores.com/wmstore/wmstores/Mainsupplier.jsp