(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. September 2013 (19.09.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/135337 A1

(51) Internationale Patentklassifikation:
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/000421

(22) Internationales Anmeldedatum:
13. Februar 2013 (13.02.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102012005427.0 16. März 2012 (16.03.2012) DE

(71) Anmelder: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder: **HINZ, Walter**; Zugspitzweg 3, 85748 Garching (DE). **FINKENZELLER, Klaus**; Ahornstraße 19, 85774 Unterföhring (DE).

(74) Anwalt: **GIESECKE & DEVRIENT GMBH**; Patent- und Lizenzabteilung, Prinzregentenstrasse 159, 81677 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHODS AND SYSTEM FOR SECURE COMMUNICATION BETWEEN AN RFID TAG AND A READER

(54) **Bezeichnung** : VERFAHREN UND SYSTEM ZUR GESICHERTEN KOMMUNIKATION ZWISCHEN EINEM RFID-TAG UND EINEM LESEGERÄT

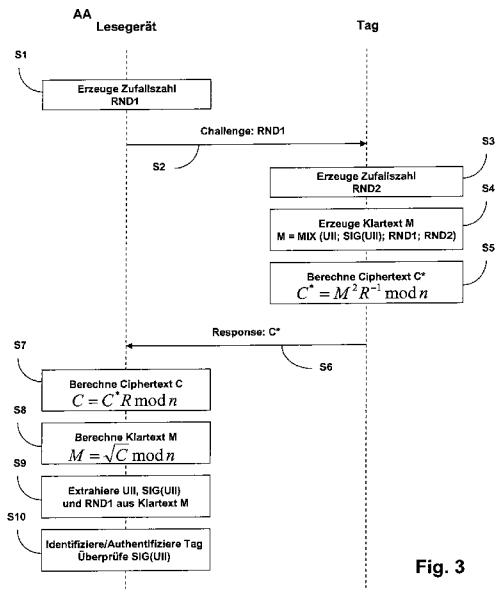


Fig. 3

AA... Reader
S1... Generate random number RND1
S3... Generate random number RND2
S4... Generate plain text M
S5... Calculate ciphertext C*
S7... Calculate ciphertext C
S8... Calculate plain text M
S9... Extract UII, SIG(UII) and RND1 from plain text M
S10... Identify/authenticate tag
Check SIG(UII)

(57) **Abstract**: The invention relates to methods and a system for secure communication between an RFID tag and a reader via the air interface and to corresponding RFID tags and corresponding readers. The invention is based on the fundamental idea that, for the purpose of secure communication between an RFID tag and a reader, a modification of Rabin's method is used, in which, within the scope of encrypting plain text M, which includes an identification element of the RFID tag or of an object provided with the latter, the Montgomery residual ("Montgomery reduction") of the square of the plain text M modulo n with respect to a Montgomery base R, that is to say $C^* = M^2 R^{-1} \bmod n$, is calculated from the RFID tag instead of the square of the plain text M modulo n, that is to say $M^2 \bmod n$, and the resultant ciphertext C* is used to authenticate the RFID tag. In this case the modulus n = p.q is the public key of the reader, the prime numbers p, q are the private key of the reader and the Montgomery base R is an integer greater than the modulus n.

(57) **Zusammenfassung**: Die Erfindung betrifft Verfahren und ein System zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät über die Luftschnittstelle sowie entsprechende RFID-Tags und entsprechende Lesegeräte. Die Erfindung

[Fortsetzung auf der nächsten Seite]

WO 2013/135337 A1

RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

geht von dem Grundgedanken aus, dass zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät eine Abwandlung des Rabin-Verfahrens verwendet wird, bei der im Rahmen der Verschlüsselung eines Klartextes M, in den ein Identifizierungselement des RFID-Tags oder eines damit versehenen Objekts einfließt, vom RFID-Tag statt des Quadrats des Klartextes M modulo n, d.h. M^2 mod n, das Montgomery-Residuum ("Montgomery reduction") des Quadrats des Klartextes M modulo n hinsichtlich einer Montgomery-Basis R, d.h. $C^* = M^2 R^{-1} \bmod n$, berechnet wird und der daraus resultierende Ciphertext C^* zur Authentisierung des RFID-Tags verwendet wird. Dabei handelt es sich bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts, bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts und bei der Montgomery- Basis R um eine ganze Zahl, die größer als der Modulus n ist.

Verfahren und System zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät

Die Erfindung betrifft Verfahren und ein System zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät über die Luftschnittstelle sowie entsprechende RFID-Tags und entsprechende Lesegeräte.

Die RFID-Technologie ("radio frequency identification") ermöglicht insbesondere die automatische Identifizierung von Personen und Objekten und findet zunehmend Verbreitung bei einer Vielzahl von Anwendungen, wie beispielsweise beim Supply Chain Management, bei Zugangskontrollsystemen, bei Systemen zur Diebstahlsicherung von Waren, beim elektronischen Ticketing und dergleichen. Ein RFID-System besteht in der Regel aus einem portablen Datenträger in Form eines RFID-Tags (auch Transponder genannt), das eine Person mit sich führt bzw. an einem Objekt angebracht ist und in dem ein das RFID-Tag und/oder das Objekt eindeutig identifizierender Identifizierungscode (dem Fachmann auch als Unique-ID (UID), Tag-ID (TID) oder "Unique Item Identifier" (UII) bekannt) gespeichert ist, sowie einem Lesegerät zum kontaktlosen Auslesen des Identifizierungscodes des RFID-Tags. Dabei ist das Lesegerät üblicherweise nur ein Lesegerät einer Vielzahl von Lesegeräten, die an unterschiedlichen Orten installiert sind und über ein Hintergrundsystem auf dort hinterlegte Daten einer Vielzahl von RFID-Tags zugreifen können.

Insbesondere für Logistikanwendungen und für das Supply Chain Management vorgesehene kostengünstige RFID-Tags, bei denen es sich in der Regel um passive RFID-Tags handelt, welche die für den Betrieb benötigte Energie aus dem elektromagnetischen Feld eines Lesegeräts beziehen, bieten häufig

keine kryptographischen Funktionen, so dass eine Authentifizierung eines RFID-Tags gegenüber einem Lesegerät bei derartigen RFID-Tags nicht möglich ist. Dies ist beispielsweise bei UHF-RFID-Tags der Fall, die dem Fachmann unter dem Namen Class-1 Gen-2 EPC-Tags bekannt sind, d.h. RFID-Tags, die gemäß dem Standard EPC Class 1 Generation 2 bzw. dem neueren Standard ISO/IEC 18000-63 ausgebildet sind. Wie dies dem Fachmann bekannt ist, umfasst der Begriff "Class-1 Gen-2 EPC-Tags" auch Tags nach dem Standard ISO/IEC 18000-63. Bei derartigen RFID-Tags wird der eindeutige Identifizierungscode als EPC ("Electronic Product Code") bezeichnet, bei dem es sich üblicherweise um eine aus 96 Bits bestehende, in einem jeweiligen RFID-Tag hinterlegte Bitfolge handelt. Der EPC wird bei einem Auslesevorgang eines RFID-Tags im Klartext ohne Authentisierung an ein Lesegerät übertragen und kann somit sowohl aktiv durch ein Lesegerät eines unberechtigten Dritten als auch passiv abgegriffen werden, indem ein Dritter den ungesicherten Kommunikationskanal, d.h. die Luftschnittstelle, zwischen dem RFID-Tag und einem Lesegerät abhört.

Dies führt zu zwei potentiellen Problemen, nämlich zum einen dazu, dass die Anwesenheit und die Position eines RFID-Tags durch einen unberechtigten Dritten erfasst und verfolgt werden können, was auch als Tracking eines RFID-Tags bezeichnet wird, und zum anderen dazu, dass ein Dritter den ausgelesenen EPC in ein neues, gefälschtes RFID-Tag kopieren kann und sich somit das neue, gefälschte RFID-Tag als das Tag ausgeben kann, aus dem der EPC ursprünglich ausgelesen worden ist, was auch als Klonen eines RFID-Tags bezeichnet wird.

Zur Sicherung der Kommunikation zwischen einem RFID-Tag und einem Lesegerät bieten sich kryptographische Verfahren an, die zum einem eine einseitige oder gegenseitige Authentifizierung zwischen dem RFID-Tag und

dem Lesegerät und zum anderen eine Verschlüsselung der Kommunikation über die Luftschnittstelle ermöglichen. Kryptographische Verfahren werden in symmetrische Verfahren, bei denen Sender und Empfänger denselben geheimen Schlüssel verwenden, und Public-Key- bzw. asymmetrische Verfahren unterteilt, bei denen der Sender einen öffentlichen Schlüssel ("public key") und der Empfänger einen geheimen Schlüssel ("private key") verwendet. Bei symmetrischen Verfahren besteht jedoch bekanntermaßen das Problem, dass sowohl in einem RFID-Tag als auch in einem Lesegerät bzw. einem damit verbundenen Hintergrundsystem der gemeinsame geheime Schlüssel sicher hinterlegt sein muss, was bei Systemen mit einer Vielzahl von RFID-Tags und einer Vielzahl von Lesegeräten eine aufwändige Schlüsselverwaltung erforderlich macht, die bei Public-Key- bzw. asymmetrischen Verfahren entfällt. Eine derartige Schlüsselverwaltung kann auch bei Systemen entfallen, die ein symmetrisches Verfahren verwenden, falls in allen RFID-Tags und im Hintergrundsystem derselbe Generalschlüssel hinterlegt wird. Dies birgt jedoch die Gefahr, dass sobald der Generalschlüssel eines RFID-Tags ermittelt worden ist, das ganze System gebrochen ist. Diese Gefahr besteht bei Public-Key-Verfahren nicht.

Ein bekanntes Public-Key-Verfahren ist das Rabin-Verfahren, das wie das häufig eingesetzte RSA-Verfahren als Grundlage die modulare Exponentiation nutzt. Da beim Rabin-Verfahren die Berechnung der Verschlüsselung wesentlich einfacher, d.h. weniger rechenintensiv als beim RSA-Verfahren ist, bietet sich das Rabin-Verfahren gegenüber dem RSA-Verfahren insbesondere dort an, wo die Instanz, welche die Verschlüsselung durchführt, d.h. der Sender einer verschlüsselten Nachricht, nur über eine begrenzte Prozessorleistung verfügt, wie dies beispielsweise bei einem ressourcenbeschränkten RFID-Tag der Fall ist, das sicher mit einem an ein Hintergrundsystem angebundenes Lesegerät kommunizieren soll.

Beim Rabin-Verfahren besteht der geheime Schlüssel aus zwei in der Praxis hinreichend groß gewählten Primzahlen p und q, die über eine bestimmte Kongruenzbedingung miteinander verknüpft sind. Das Produkt $n = p \cdot q$ der beiden Primzahlen p und q definiert den Modulus oder das Modul n und stellt gleichzeitig den öffentlichen Schlüssel dar. Zweckmäßigerweise sind die Primzahlen p und q in etwa gleich groß. Gemäß dem Rabin-Verfahren wird ein zu übermittelnder Klartext M durch modulares Quadrieren und Anwenden der Modulo-Operation verschlüsselt, d.h. der Ciphertext C ergibt sich aus dem Klartext M gemäß der folgenden Formel: $C = M^2 \bmod n$.

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

Da beim Rabin-Verfahren die Verschlüsselung durch den Sender eine modulare Quadrierung beinhaltet, muss der Empfänger zur Entschlüsselung die modulare Quadratwurzel des Ciphertextes C berechnen. Hierbei kann bekanntermaßen der Chinesische Restklassensatz (CRT; "chinese remainder theorem") ausgenutzt werden. Wie dies der Fachmann weiß, ergeben sich dabei vier Quadratwurzeln, aus denen eine als der ursprüngliche Klartext M ausgewählt werden muss. Hierzu kann der "richtige" Klartext M beispielsweise mittels einer geeigneten Kennung, Prüfsumme oder dergleichen dem Empfänger kenntlich gemacht werden.

Wie sich dies aus der vorstehend beschriebenen Formel für die Berechnung des Ciphertextes C beim Rabin-Verfahren ergibt, muss der Sender zur

Durchführung der Modulo-Operation in der Regel eine Langzahldivision durchführen. Eine derartige Langzahldivision kann jedoch insbesondere auf einfachen Mikroprozessoren, wie diese bei RFID-Tags zum Einsatz kommen, nur sehr aufwändig realisiert werden.

In der Publikation "A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes" von Y. Oren und M. Feldhofer in D.A. Basin, S. Capkun, and W.Lee, editors, *WISEC*, Seiten 59-68, ACM 2009 wird unter dem Namen WIPR-Verfahren eine Abwandlung des herkömmlichen Rabin-Verfahrens vorgeschlagen, die insbesondere für die Sicherung der Kommunikation zwischen einem resourcenbeschränkten RFID-Tag mit einem einfachen Prozessor und einem Lesegerät vorgesehen ist. Gegenüber dem vorstehend beschriebenen herkömmlichen Rabin-Verfahren weist das WIPR-Verfahren den Vorteil auf, dass zur Berechnung des Ciphertextes anstatt einer aufwändigen Langzahl-Division, die sehr rechenintensiv ist und somit auf einfachen Mikroprozessoren, wie sie auf RFID-Tags üblicherweise zu finden sind, kaum implementiert werden kann, Langzahl-Multiplikationen zum Einsatz kommen, die wesentlich schneller ausführbar sind als Divisionen und sich auch hardwaremäßig einfacher realisieren lassen.

Gemäß dem WIPR-Verfahren wird der Ciphertext C' berechnet, indem der Sender, z.B. ein RFID-Tag, eine Zufallszahl r erzeugt, diese mit dem Modulus n multipliziert und das Ergebnis zum Quadrat des Klartextes M hinzu addiert, also $C' = M^2 + r \cdot n$. Dabei fließt ein Identifizierungscode des RFID-Tags in den Klartext M ein und die Größe der Zufallszahl r wird so gewählt, dass das Produkt $r \cdot n$ mehr als doppelt so groß wie der Modulus n ist. Im Gegensatz zum herkömmlichen Rabin-Verfahren wird beim WIPR-Verfahren das Quadrat des Klartextes M also nicht durch die Durchführung der Modulo-Operation, die eine Langzahldivision beinhaltet, sondern durch

die Addition des Produkts $r \cdot n$ mit der geeignet gewählten Zufallszahl r maskiert.

In der Publikation A. Shamir, "Memory Efficient Variants of Public-Key Schemes for Smart Card Applications", in A. D. Santis, editor, Advances in Cryptology - EUROCRYPT '94, Springer LNCS, Band 950, Seiten 445-449 ist gezeigt worden, dass ein Verfahren wie das WIPR-Verfahren ebenso sicher wie das herkömmliche Rabin-Verfahren ist, sofern die Zufallszahl r aus einem hinreichend großen Zahlenbereich zufällig gewählt wird.

Jedoch wird beim WIPR-Verfahren der Vorteil der Vermeidung einer Langzahldivision dadurch erkauft, dass der Ciphertext C' aufgrund des Wegfallens der Modulo-Operation beim Quadrieren des Klartextes M und aufgrund des Produkts des Modulus n mit der hinreichend groß gewählten Zufallszahl r in der Regel sehr lang sein wird, was den Authentisierungsvorgang zwischen einem RFID-Tag und einem Lesegerät verlangsamt, da eine größere Datenmenge vom RFID-Tag zum Lesegerät übertragen werden muss.

Vor diesem Hintergrund stellt sich der vorliegenden Erfindung das Problem, verbesserte Verfahren und ein verbessertes System zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät über die Luftschnittstelle bereitzustellen, die das RFID-Tag insbesondere davor schützen, getrackt und/oder geklont zu werden. Ferner sollen ein entsprechend ausgestaltetes RFID-Tag sowie ein entsprechend ausgestaltetes Lesegerät bereitgestellt werden.

Diese Aufgabe wird erfindungsgemäß durch den Gegenstand der unabhängigen Ansprüche gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen definiert.

Die Erfindung geht von dem Grundgedanken aus, dass zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät eine Abwandlung des Rabin-Verfahrens verwendet wird, bei der im Rahmen der Verschlüsselung eines Klartextes M, in den ein Identifizierungselement des RFID-Tags oder eines damit versehenen Objekts einfließt, vom RFID-Tag statt des Quadrats des Klartextes M modulo n, d.h. $M^2 \bmod n$, das Montgomery-Residuum ("Montgomery reduction") des Quadrats des Klartextes M modulo n hinsichtlich einer Montgomery-Basis R, d.h. $C^* = M^2 R^{-1} \bmod n$, berechnet wird und der daraus resultierende Ciphertext C^* zur Authentisierung des RFID-Tags verwendet wird. Dabei handelt es sich bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts, bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts und bei der Montgomery-Basis R um eine ganze Zahl, die größer als der Modulus n ist. Hierbei ist die Montgomery-Basis R in der Regel eine Zweierpotenz.

Auf der Grundlage des vorstehend beschriebenen Grundgedankens der vorliegenden Erfindung wird gemäß einem ersten Aspekt der Erfindung ein Verfahren zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät bereitgestellt, wobei das Verfahren die folgenden Schritte umfasst, die im RFID-Tag durchgeführt werden. Das Verschlüsseln eines Klartextes M, in den ein Identifizierungselement des RFID-Tags oder eines damit versehenen Objekts einfließt, zur Berechnung eines Ciphertextes C^*, indem das Montgomery-Residuum des Quadrats des Klartextes M modulo n hinsichtlich einer Montgomery-Basis R, d.h. $C^* = M^2 R^{-1} \bmod n$, berechnet wird und das Aussenden einer Authentisierungsnachricht an das Lesegerät, wobei die Authentisierungsnachricht auf dem Ciphertext C^* basiert.

Ferner wird auf der Grundlage des vorstehend beschriebenen Grundgedankens der vorliegenden Erfindung gemäß einem zweiten Aspekt der Erfin-

dung ein Verfahren zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät bereitgestellt, wobei das Verfahren die folgenden Schritte umfasst, die im Lesegerät durchgeführt werden. Das Empfangen einer Authentisierungsnachricht vom RFID-Tag, die auf einem verschlüsselten Klartext M basiert, in den ein Identifizierungselement des RFID-Tags oder eines damit versehenen Objekts eingeflossen ist, und das Entschlüsseln des verschlüsselten Klartextes M, wobei der Schritt des Entschlüsselns die Multiplikation des verschlüsselten Klartextes M mit einer Montgomery-Basis R und die anschließende Durchführung der Modulo-Operation mit dem Modulus n umfasst. Vorzugsweise umfasst der Schritt des Entschlüsselns ferner die anschließende Ziehung der Quadratwurzel modulo n analog dem herkömmlichen Rabin-Verfahren.

Des weiteren wird auf der Grundlage des vorstehend beschriebenen Grundgedankens der vorliegenden Erfindung gemäß einem dritten Aspekt der Erfindung ein RFID-Tag zur gesicherten Kommunikation mit einem Lesegerät bereitgestellt. Dabei umfasst das RFID-Tag eine Prozessoreinheit und eine Speichereinheit. In der Speichereinheit ist ein Identifizierungselement hinterlegt. Die Prozessoreinheit ist dazu ausgestaltet, einen Klartext M, in den das Identifizierungselement des RFID-Tags oder eines damit versehenen Objekts einfließt, zur Berechnung eines Ciphertextes C^* zu verschlüsseln, indem das Montgomery-Residuum des Quadrats des Klartextes M modulo n hinsichtlich einer Montgomery-Basis R, d.h. $C^* = M^2 R^{-1} \bmod n$, berechnet wird, und eine Authentisierungsnachricht an das Lesegerät zu senden, wobei die Authentisierungsnachricht auf dem Ciphertext C^* basiert.

Ferner wird auf der Grundlage des vorstehend beschriebenen Grundgedankens der vorliegenden Erfindung gemäß einem vierten Aspekt der Erfindung ein Lesegerät zur gesicherten Kommunikation mit einem RFID-Tag

bereitgestellt. Das Lesegerät umfasst eine Prozessoreinheit, die dazu ausgestaltet ist, eine Authentisierungsnachricht vom RFID-Tag zu empfangen, die auf einem verschlüsselten Klartext M basiert, in den ein Identifizierungselement des RFID-Tags oder eines damit versehenen Objekts eingeflossen ist, und den verschlüsselten Klartext zu entschlüsseln, wobei bei der Entschlüsselung der verschlüsselte Klartext M mit einer Montgomery-Basis R multipliziert und anschließend die Modulo-Operation mit dem Modulus n durchgeführt wird. Vorzugsweise ist die Prozessoreinheit des Lesegeräts zur Entschlüsselung des verschlüsselten Klartextes ferner dazu ausgestaltet, anschließend analog dem herkömmlichen Rabin-Verfahren die Quadratwurzel modulo n zu ziehen.

Schließlich wird auf der Grundlage des vorstehend beschriebenen Grundgedankens der vorliegenden Erfindung gemäß einem fünften Aspekt der Erfindung ein System zur gesicherten Kommunikation mit wenigstens einem RFID-Tag gemäß dem dritten Aspekt der Erfindung und wenigstens einem Lesegerät gemäß dem vierten Aspekt der Erfindung bereitgestellt.

Wie vorstehend erwähnt, handelt es sich dabei bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts, bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts und bei der Montgomery-Basis R um eine ganze Zahl, die größer als der Modulus n ist.

Vorzugsweise enthält die vom RFID-Tag an das Lesegerät übertragene Authentisierungsnachricht den verschlüsselten Klartext M in Form des Ciphertextes C^* mit $C^* = M^2 R^{-1} \bmod n$.

Gemäß bevorzugter Ausführungsformen der Erfindung fließen in den Klartext M ferner eine vom Lesegerät erzeugte erste Zufallszahl *RND1* und eine

vom RFID-Tag erzeugte zweite Zufallszahl *RND2* ein. Dabei wird die erste Zufallszahl *RND1* vorzugsweise als Challenge im Rahmen eines Challenge-Response-Verfahrens an das RFID-Tag übertragen. Bei dieser bevorzugten Ausgestaltung werden die in den Klartext *M* einfließenden Daten, insbesondere das Identifizierungselement des RFID-Tags, die erste Zufallszahl *RND1* und die zweite Zufallszahl *RND2*, vorzugsweise mittels einer Interleaving-Operation verwürfelt, um die vom Lesegerät und vom RFID-Tag stammenden zufälligen Daten zufällig über den Klartext *M* zu verteilen. Durch die enthaltenen zufälligen Bestandteile *RND1* und *RND2* wird erreicht, dass sowohl der Klartext *M* als auch der Ciphertext C^* bei jedem Auslesevorgang, d.h. bei jeder Abfrage, anders ausfallen.

Vorteilhafterweise ist das RFID-Tag derart ausgestaltet, dass das RFID-Tag noch während des Einlesens der Challenge mit der Verschlüsselung beginnen kann. Ferner können die ersten Bits bzw. Bytes des vom RFID-Tag berechneten Ciphertextes C^* bereits an das Lesegerät übertragen werden, während die nachfolgenden Bits bzw. Bytes des Ciphertextes C^* vom RFID-Tag noch berechnet werden. Mit anderen Worten: das RFID-Tag ist vorzugsweise dazu ausgestaltet, den Ciphertext C^* sukzessive Bit für Bit zu berechnen und die bereits berechneten Bits des Ciphertextes C^* als Teil der Authentifizierungsnachricht an das Lesegerät zu senden, wodurch keine Zwischenspeicher (Register) erforderlich sind und das Kommunikationsprotokoll schneller durchgeführt werden kann.

Wahlweise fließt in den Klartext *M* ferner eine digitale Signatur des Identifizierungselements des RFID-Tags ein, die vorzugsweise im Speicher des RFID-Tags hinterlegt ist und vom Lesegerät überprüft werden kann.

Gemäß bevorzugter Ausführungsformen wird zur Einsparung von Rechenzeit der Modulus n wie folgt gewählt: $n = 1 (\mathrm{mod} 2^{bl \cdot nd})$, wobei nd eine ganze Zahl mit $1 \leq nd < d$ ist, bl die Wortbreite der Prozessoreinheit des RFID-Tags in Bits und d die Länge des Modulus n in Wortbreiten der Prozessoreinheit ist.

In der Praxis wird für einen gegebenen Modulus n die Zahl R typischerweise als die nächst größere Zweierpotenz gewählt, d.h. für einen aus k Bits (z.B. 1024 Bits) bestehenden Modulus n wird $R = 2^k$ gewählt. Gemäß bevorzugter Ausführungsformen der Erfindung wird $R = 2^{bl \cdot (d+sd)}$ gesetzt, wobei bl die Wortbreite der Prozessoreinheit des RFID-Tags, d die Länge des Modulus n in Wortbreiten der Prozessoreinheit und sd ein Sicherheitsparameter ist, der so gewählt ist, dass $bl \cdot sd \geq 1$, vorzugsweise $bl \cdot sd \geq 10$ und am meisten bevorzugt $bl \cdot sd \geq 100$ gilt.

Vorzugsweise ist das Lesegerät nur ein Lesegerät einer Vielzahl von Lesegeräten, die über ein Hintergrundsystem miteinander verbunden sind und auf im Hintergrundsystem hinterlegte Daten zugreifen können, die jeweils mit einem jeweiligen RFID-Tag verknüpft sind.

Gemäß einer bevorzugten Ausführungsform handelt es sich bei dem RFID-Tag um ein UHF-Tag nach dem Standard ISO/IEC 18000-63 bzw. dem Standard Class-1 Gen-2 EPC.

Die vorliegende Erfindung weist insbesondere die folgenden Vorteile auf. Bei der erfindungsgemäßen Verschlüsselung wird keine modulare Reduktion, also keine Division benötigt und es werden nicht mehr Daten erzeugt, als der Länge des Modulus n entspricht. Ferner bietet die Erfindung die Möglichkeit, mit der Berechnung des Ciphertextes C^* zu beginnen, bevor das

RFID-Tag alle in die Berechnung eingehenden Daten empfangen hat, und sodann damit zu beginnen, das Ergebnis dieser Berechnung an das Lesegerät zu senden, bevor die Berechnung des Ciphertextes C^* abgeschlossen ist, wodurch Datenübertragung und Berechnung parallel ausgeführt werden können und Transaktionszeit eingespart werden kann. Da es sich bei den erfindungsgemäßen Verfahren um Public-Key-Verfahren handelt, muss lediglich ein öffentlicher Schlüssel auf dem RFID-Tag hinterlegt werden, so dass die Sicherheit des Systems nicht gefährdet ist, wenn ein Angreifer diesen öffentlichen Schlüssel erlangt. Ein weiterer Vorteil der Erfindung besteht darin, dass zur Entschlüsselung des Ciphertextes C^* ein Lesegerät nicht mit einem Hintergrundsystem verbunden sein muss, da der dafür erforderliche private Schlüssel lokal auf dem Lesegerät hinterlegt sein kann. Schließlich besteht ein weiterer Vorteil darin, dass die Erfindung auf herkömmlichen Lesegeräten ohne Hardwaremodifikationen implementiert werden kann.

Wie der Fachmann erkennen wird, lassen sich die die vorstehend beschriebenen und in den Unteransprüchen definierten bevorzugten Ausgestaltungen im Rahmen des ersten Aspekts der Erfindung, im Rahmen des zweiten Aspekts der Erfindung, im Rahmen des dritten Aspekts der Erfindung sowie im Rahmen des vierten Aspekts der Erfindung vorteilhaft implementieren.

Weitere Merkmale, Vorteile und Aufgaben der Erfindung gehen aus der folgenden detaillierten Beschreibung mehrerer Ausführungsbeispiele und Ausführungsalternativen hervor. Es wird auf die Zeichnungen verwiesen, in denen zeigen:

Fig. 1 eine schematische Darstellung eines Systems zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät gemäß einer bevorzugten Ausführungsform der Erfindung,

Fig. 2 eine schematische Detailansicht eines RFID-Tags des Systems von Figur 1,

Fig. 3 eine schematische Darstellung einer bevorzugten Ausführungsform eines erfindungsgemäßen Verfahrens zur gesicherten Kommunikation zwischen einem RFID-Tag und einem Lesegerät des Systems von Figur 1, und

Fig. 4 einen Algorithmus zur Implementierung des erfindungsgemäßen Verfahrens von Figur 3.

Figur 1 zeigt eine schematische Darstellung eines Systems 10 zur Kommunikation zwischen einem RFID-Tag und einem Lesegerät gemäß einer bevorzugten Ausführungsform der Erfindung. Bei dem System 10 könnte es sich beispielsweise um ein elektronisches Ticketing-System handeln, bei dem ein RFID-Tag ein elektronisches Ticket darstellt, das eine Person mit sich trägt.

Das System 10 umfasst beispielhaft zwei RFID-Tags, nämlich das RFID-Tag 20a und das RFID-Tag 20b, die jeweils über die Luftschnittstelle mit einem Lesegerät 30a bzw. einem Lesegerät 30b kommunizieren können, in dessen Kommunikations- bzw. Lesebereich sich das jeweilige RFID-Tag 20a, 20b befindet. Vorzugsweise handelt es sich bei den RFID-Tags 20a, 20b um RFID-Tags gemäß dem Standard ISO/IEC 18000-63 bzw. EPC Class 1 Generation 2, die hier auch als EPC Tags bezeichnet werden.

Die Lesegeräte 30a, 30b sind über ein geeignetes Kommunikationsnetzwerk 40 mit einem Hintergrundsystem bzw. Backendsystem 50 verbunden, in dem vorzugsweise in einer Datenbank mit den RFID-Tags 20a, 20b verknüpfte Daten hinterlegt sind. Neben den Lesegeräten 30a, 30b können in das in Figur 1 dargestellte System 10 noch eine Vielzahl weiterer Lesegeräte integriert

sein, die über das Kommunikationsnetzwerk 40 mit dem Hintergrundsystem 50 in Kommunikation stehen und auf die dort hinterlegten Daten zugreifen können. Der Übersichtlichkeit halber sind in Figur 1 lediglich zwei RFID-Lesegeräte 30a, 30b und zwei RFID-Tags, nämlich die RFID-Tags 20a, 20b, dargestellt. Selbstverständlich ist das in Figur 1 dargestellte System 10 jedoch dazu ausgestaltet, dass neben den RFID-Tags 20a, 20b noch eine Vielzahl weiterer RFID-Tags in diesem System 10 betrieben werden können.

Figur 2 zeigt eine Detailansicht des beispielhaften RFID-Tags 20a des Systems 10 von Figur 1, in der die für die vorliegende bevorzugte Ausführungsform der Erfindung wesentlichen Komponenten des RFID-Tags 20a schematisch dargestellt sind. Das RFID-Tag 20a, dessen Aufbau bevorzugt identisch zum Aufbau des RFID-Tags 20b sein kann, aber nicht sein muss, umfasst eine externe oder interne Antenneneinrichtung 22 zur jeweiligen Kommunikation über die Luftschnittstelle mit den Lesegeräten 30a, 30b des Systems 10 von Figur 1. Die Antenneneinrichtung 22 steht über eine Input-/Output-Schnittstelle 24 in Kommunikation mit einer Prozessoreinheit 25, die auf einen Speicher 26 des RFID-Tags 20a zum Speichern und zum Auslesen von Daten zugreifen kann.

In dem in Figur 2 dargestellten Speicher 26 des RFID-Tags 20a, bei dem es sich beispielsweise um ein ROM und/oder EEPROM (Flash-Speicher) handeln kann, sind die Daten, die für die bevorzugte, nachstehend im Detail beschriebene erfindungsgemäße gesicherte Kommunikation des RFID-Tags 20a mit einem der Lesegeräte 30a, 30b verwendet werden, hinterlegt bzw. können dort hinterlegt werden. Insbesondere ist im Speicher 26 des RFID-Tags 20a wenigstens ein Identifizierungselement hinterlegt, das eine eindeutige Identifizierung des RFID-Tags 20a und/oder des mit dem RFID-Tag 20a versehenen Objektes ermöglicht. Bei dem im Speicher 26 hinterlegten Identifi-

zierungselement kann es sich beispielsweise um ein TID-Element ("Tag Identifier") oder ein UII-Element ("Unique Item Identifier") handeln, vorzugsweise um den dem Fachmann aus dem EPC Standard bekannten Electronic Product Code (EPC). Wie sich dies der Figur 2 entnehmen lässt, sind im Speicher 26 des RFID-Tags 20a ferner ein öffentlicher Schlüssel n sowie vorzugsweise eine digitale Signatur des im Speicher 26 hinterlegten Identifizierungselements, beispielsweise die digitale Signatur des UII-Elements, die in Figur 2 als SIG(UII) gekennzeichnet ist, hinterlegt, deren Zweck nachstehend im Zusammenhang mit Figur 3 detaillierter beschrieben wird.

Vorzugsweise umfasst das RFID-Tag 20a ferner einen Zufallszahlengenerator 28 (RND) zur Erzeugung von Zufallszahlen, die für die gesicherte Kommunikation zwischen dem RFID-Tag 20a und einem der Lesegeräte 30a, 30b verwendet werden, wie dies nachstehend im Zusammenhang mit Figur 3 im Detail beschrieben wird. Obgleich in Figur 2 der Zufallszahlengenerator 28 als separate Einheit dargestellt ist, wird der Fachmann erkennen, dass der Zufallszahlengenerator 28 auch ein Teil der Prozessoreinheit 25 sein oder als ein Softwaremodul der Prozessoreinheit 25 implementiert sein könnte. Ebenso könnte der Speicher 26 als Teil der Prozessoreinheit 25 ausgestaltet sein.

Neben dem Zugriff auf den Speicher 26 des RFID-Tags 20a sowie der internen Kommunikation mit der Input-/Output-Schnittstelle 24 und dem Zufallszahlengenerator 28 beispielsweise über ein Bussystem ist die Prozessoreinheit 25 des RFID-Tags 20a vorzugsweise ferner dazu ausgestaltet, die nachstehend im Zusammenhang mit Figur 3 beschriebenen Schritte auf Seiten des RFID-Tags 20a durchzuführen bzw. zu veranlassen, um eine gesicherte Kommunikation zwischen dem RFID-Tag 20a und einem der Lesegeräte 30a, 30b zu ermöglichen.

Sobald ein Lesegerät, beispielsweise das Lesegerät 30a, erfasst, dass sich ein RFID-Tag, beispielsweise das RFID-Tag 20a, in dessen Kommunikationsbereich befindet, wird das in Figur 3 skizzierte Kommunikationsprotokoll vom Lesegerät 30a angestoßen. Dabei generiert in Schritt S1 von Figur 3 das Lesegerät 30a zunächst eine erste Zufallszahl *RND1* (auch Nonce genannt) und sendet diese erste Zufallszahl *RND1* als Challenge im Rahmen eines Challenge-Response-Verfahrens in Schritt S2 von Figur 3 an das RFID-Tag 20a. Vorzugsweise in Reaktion auf den Empfang der ersten Zufallszahl *RND1* vom Lesegerät 30a erzeugt in Schritt S3 von Figur 3 das RFID-Tag 20a eine zweite Zufallszahl *RND2*. Dabei wird diese zweite Zufallszahl *RND2* vorzugsweise von dem Zufallszahlengenerator 28 des RFID-Tags 20a erzeugt, und zwar unabhängig von der ersten Zufallszahl *RND1*.

Wie dies nachstehend im Detail beschrieben wird, fließen vorzugsweise sowohl die erste vom Lesegerät 30a beigesteuerte Zufallszahl *RND1* als auch die zweite vom RIFD-Tag 20a beigesteuerte Zufallszahl *RND2* in den vom RFID-Tag 20a zu verschlüsselnden und an das Lesegerät 30a zu übertragenden Klartext *M* ein. Da der zu verschlüsselnde Klartext *M* somit ein zufälliges, sich von Auslesevorgang zu Auslesevorgang änderndes Element aufweist, wird bei jedem Auslesevorgang auch ein anderer verschlüsselter Klartext *M*, d.h. ein anderer Ciphertext, vom RFID-Tag 20a an das Lesegerät 30a übertragen. Hierdurch kann vermieden werden, dass ein Angreifer ein RFID-Tag anhand eines vom diesem RFID-Tag ausgesendeten, unveränderlichen Ciphertextes identifizieren kann. Darüber hinaus hat die vom Lesegerät 30a erzeugte erste Zufallszahl *RND1*, wie vorstehend bereits erwähnt, die Funktion einer Challenge im Rahmen eines dem Fachmann bekannten Challenge-Response-Verfahrens zur Authentifizierung des RFID-Tags 20a gegenüber dem Lesegerät 30a.

In Schritt S4 von Figur S3 wird vom RFID-Tag 20a ein zu verschlüsselnder Klartext *M* erzeugt, der es dem Lesegerät 30a ermöglicht, das den verschlüsselten Klartext *M* empfängt und entschlüsselt, das RFID-Tag 20a zu identifizieren. Hierzu fließt insbesondere ein Identifizierungselement in den Klartext *M* ein, das eine eindeutige Identifizierung des RFID-Tags 20a und/oder des mit dem RFID-Tag 20a versehenen Objekts ermöglicht. Bei der in den Figuren dargestellten bevorzugten Ausführungsform handelt es sich bei dem Identifizierungselement um das im Speicher 26 des RFID-Tags 20a hinterlegte UII-Element.

Damit das Lesegerät 30a die Echtheit des UII-Elements des RFID-Tags 20a überprüfen kann, fließt in den Klartext *M* vorzugsweise ferner eine digitale Signatur des UII-Elements ein. Vorzugsweise ist eine digitale Signatur des UII-Elements im Speicher 26 des RFID-Tags 20a hinterlegt, wie dies in Figur 2 mit der Bezeichnung SIG(UII) angedeutet ist, damit diese nicht bei jedem Auslesevorgang vom RFID-Tag 20a neu berechnet werden muss. Wie dies dem Fachmann bekannt ist, lässt sich eine digitale Signatur des UII-Elements des RFID-Tags 20a beispielsweise dadurch erstellen, dass auf das UII-Element im Rahmen eines Public-Key-Verfahrens ein privater Schlüssel angewendet wird. Zur Überprüfung der digitalen Signatur des UII-Elements durch das Lesegerät 30a wird ein zum privaten Schlüssel passender öffentlicher Schlüssel auf die digitale Signatur angewendet.

Vorzugsweise fließen neben dem UII-Element und der digitalen Signatur des UII-Elements ferner, wie bereits vorstehend beschrieben, sowohl die vom Lesegerät 30a bereitgestellte erste Zufallszahl *RND1* als auch die vom RFID-Tag 20a bereitgestellte zweite Zufallszahl *RND2* in den Klartext *M* ein. Dies erfolgt vorzugsweise mittels einer auf der Prozessoreinheit 25 des RFID-Tags 20a implementierten Interleaving-Operation MIX, die dazu ausgestaltet ist,

das UII-Element, die digitale Signatur des UII-Elements, die erste Zufallszahl *RND1* und die zweite Zufallszahl *RND2* miteinander zu vermischen bzw. zu verwürfeln. Dabei kann die Vermischung durch die Interleaving-Operation MIX beispielsweise auf Byte-Ebene erfolgen. Das Ergebnis der Anwendung der Interleaving-Operation MIX auf das UII-Element, die digitale Signatur des UII-Elements, die erste Zufallszahl *RND1* und die zweite Zufallszahl *RND2* ist der zu verschlüsselnde Klartext *M*. Die aus den Zufallszahlen *RND1* und *RND2* stammenden Bits des Klartextes *M* können als Padding-Bits betrachtet werden. Dabei kann es vorteilhaft sein, durch eine geeignete Wahl der Längen der Zufallszahlen *RND1* und *RND2* zu erreichen, dass der Klartext *M* dieselbe Länge wie der Modulus *n* aufweist, beispielsweise 1024 Bits.

Nachdem in Schritt S4 von Figur 3 der unter anderem das UII-Element enthaltende Klartext *M* vom RFID-Tag 20a erstellt worden ist, wird dieser Klartext *M* in Schritt S5 von Figur 3 folgendermaßen vom RFID-Tag 20a verschlüsselt. Wie beim herkömmlichen Rabin-Verfahren wird der Klartext *M* zunächst quadriert. Zur Erzeugung des Ciphertextes wird das Ergebnis dieser Quadratur jedoch anschließend nicht wie beim herkömmlichen Rabin-Verfahren einer Modulo-Operation mit dem Modulus *n* unterzogen, sondern es wird das Montgomery-Residuum des quadrierten Klartextes gebildet. Allgemein wird das Montgomery-Residuum ("Montgomery reduction") einer ganzen Zahl *T* modulo *n* hinsichtlich einer ganzen Zahl *R* definiert als $TR^{-1} \bmod n$, wobei *R* größer als der Modulus *n* ist, *R* und der Modulus *n* teilerfremd sind (d.h. ggT(*R*,*n*)=1) und $0 \leq T < nR$ (siehe Kapitel 14.3.2 von A. J. Menezes, P.C. van Oorschot, S.C. Vanstone, "*Handbook of Applied Cryptography*"). In der Literatur wird die ganze Zahl *R* zuweilen als Montgomery-Basis bezeichnet.

Im Rahmen der vorliegenden Erfindung wird das vom RFID-Tag 20a berechnete Montgomery-Residuum des Quadrats des Klartextes M modulo n hinsichtlich der ganzen Zahl R als der Ciphertext C^* definiert, d.h. $C^* = M^2 R^{-1} \bmod n$, wobei die ganze Zahl R, wie vorstehend bereits erwähnt, größer als der Modulus n gewählt wird. In der Praxis wird für einen gegebenen Modulus n die Zahl R typischerweise als die nächst größere Zweierpotenz gewählt, d.h. für einen aus k Bits (z.B. 1024 Bits) bestehenden Modulus n wird $R = 2^k$ gewählt. Weitere gemäß der vorliegenden Erfindung bevorzugte Wahlmöglichkeiten der Zahl R werden weiter unten beschrieben.

Nachdem in Schritt S5 von Figur 3 der Ciphertext $C^* = M^2 R^{-1} \bmod n$ vom RFID-Tag 20a berechnet worden ist, wird in Schritt S6 von Figur 3 der so berechnete Ciphertext C^* als Response auf die in Schritt S2 von Figur 3 übersendete Challenge an das Lesegerät 30a gesendet. Der Fachmann wird jedoch erkennen, dass prinzipiell statt des Ciphertextes $C^* = M^2 R^{-1} \bmod n$ auch ein vom RFID-Tag 20a nochmals weiterverarbeiteter Ciphertext C^{**} an das Lesegerät 30a übertragen werden könnte, sofern das RFID-Tag 20a und das Lesegerät 30a untereinander vereinbart haben, wie das Lesegerät 30a aus dem vom RFID-Tag 20a weiterverarbeiteten und übermittelten Ciphertext C^{**} auf den Ciphertext $C^* = M^2 R^{-1} \bmod n$ zurückrechnen kann.

In Schritt S7 von Figur 3 wird zunächst der vom RFID-Tag 20 in Schritt S6 übermittelte Ciphertext C^* mit R multipliziert und anschließend die Modulo-Operation mit dem Modulus n durchgeführt, d.h. $C^* R \bmod n$. Setzt man für C^* den im Zusammenhang mit Schritt S5 von Figur 3 beschriebenen Ausdruck ein, so erhält man: $C^* R \bmod n = M^2 R^{-1} R \bmod n = M^2 \bmod n$. Wie der Fachmann erkennt, handelt es sich bei dem letzten Ausdruck $M^2 \bmod n$ um den Ciphertext des bekannten Rabin-Verfahrens, der hier als Ciphertext C bezeichnet wird. Mit anderen Worten: In Schritt S7 von Figur 3 wird der aus

dem bekannten Rabin-Verfahren bekannte Ciphertext $C = M^2 \bmod n$ erhalten, indem der vom RFID-Tag 20 gesendete Ciphertext C^* mit R multipliziert wird und anschließend die Modulo-Operation mit dem Modulus n durchgeführt wird.

Wie im Fall des klassischen Rabin-Verfahrens kann nun in Schritt S8 von Figur 3 durch das Lesegerät 30a der ursprünglich in Schritt S4 vom RFID-Tag 20a erzeugte Klartext M ermittelt werden, indem die Quadratwurzel des in Schritt S7 bestimmten Ciphertextes C modulo n berechnet wird. Wie bereits vorstehend beschrieben, kann hierzu unter Verwendung des dem Lesegerät 30a vorliegenden privaten Schlüssel in Form der Primzahlen p und q der Chinesische Restklassensatz (CRT) ausgenutzt werden, um die vier Quadratwurzeln des Ciphertextes C zu berechnen. Vorzugsweise wird mittels einer geeigneten Markierung dem Lesegerät 30a gegenüber deutlich gemacht, welche der vier Quadratwurzeln des Ciphertextes C der vom RFID-Tag 20a ursprünglich generierte Klartext M ist. Beispielsweise kann die vom Lesegerät 30a übermittelte erste Zufallszahl *RND1* dazu verwendet werden, die richtige Quadratwurzel, d.h. den richtigen Klartext M, auszuwählen.

Wie vorstehend beschrieben, wird der Klartext M in Schritt S4 von Figur 3 generiert, indem die Interleaving-Operation MIX durchgeführt wird. Wie der Fachmann erkennt, muss auf Seiten des Lesegeräts 30a diese Interleaving-Operation wieder rückgängig gemacht bzw. invertiert werden, um das UII-Element des RFID-Tags 20a, die digitale Signatur SIG(UII) des UII-Elements, die erste Zufallszahl *RND1* und die zweite Zufallszahl *RND2* aus dem Klartext M extrahieren zu können. Diese Invertierung der Interleaving-Operation MIX und die Extraktion der im Klartext M enthaltenen Informationen erfolgt vorzugsweise in Schritt S9 von Figur 3. Selbstverständlich muss zwischen dem RFID-Tag 20a und dem Lesegerät 30a vereinbart worden sein,

welche Interleaving-Operation in Schritt S4 von Figur 3 verwendet wird, um in Schritt S9 von Figur 3 die Umkehrfunktion hierzu anwenden zu können.

Nach der erfolgreichen Durchführung von Schritt S9 von Figur 3 liegen dem Lesegerät 30a das UII-Element des RFID-Tags 20a, die digitale Signatur des UII-Elements, die erste Zufallszahl *RND1* und die zweite Zufallszahl *RND2* vor. Anhand dieser vorliegenden Elemente kann das Lesegerät 30a das RFID-Tag 20a identifizieren und authentifizieren. Vorzugsweise wird in Schritt S10 von Figur 3 ferner die Unversehrtheit des UII-Elements des RFID-Tags 20a vom Lesegerät 30a überprüft, indem das Lesegerät 30a die digitale Signatur des UII-Elements überprüft. Es ist denkbar, dass hierzu das Lesegerät 30a auf das Hintergrundsystem 50 zugrifft, um anhand des UII-Elements des RFID-Tags 20a einen öffentlichen Schlüssel zu finden, der zu dem privaten Schlüssel passt, mit dem die digitale Signatur des UII-Elements des RFID-Tags 20a ursprünglich erstellt worden ist.

Nachstehend wird unter Bezugnahme auf Figur 4 eine bevorzugte Implementierung der erfindungsgemäßen Berechnung des Ciphertextes C^*, d.h. der Verschlüsselung des Klartextes *M*, durch das RFID-Tag 20a beschrieben, deren Ablauf sich grob in drei Abschnitte gliedern lässt.

In einem ersten Abschnitt der Verschlüsselung wird der Klartext *M* sukzessive, vom niederwertigsten bis zum höchstwertigsten Byte verarbeitet. Wenn die Interleaving-Operation MIX, dazu ausgestaltet ist, die erste Zufallszahl *RND1* des Lesegeräts 30a gleichmäßig verteilt in den Klartext *M* einzustreuen, kann bereits nach Empfang des ersten Bytes der Zufallszahl *RND1* mit dem ersten Verschlüsselungsabschnitt begonnen und so lange gerechnet werden, wie Bytes des Klartextes *M* zur Verfügung stehen. Nach Empfang des nächsten Bytes der Zufallszahl *RND1* vom Lesegerät 30a wird die Ver-

schlüsselung so lange weiter berechnet, bis der gesamte Klartext M verschlüsselt worden ist.

In einem zweiten Abschnitt der Verschlüsselung erfolgt eine systemweit vereinbarte Anzahl zusätzlicher Montgomery-Schritte, d.h. die Zahl R wird entsprechend größer als die nächste oberhalb des Modulus n zur Verfügung stehende Zweierpotenz gewählt. Der Grund für diese Maßnahme ist, dass sich die Wahrscheinlichkeit verringert, dass das Endergebnis der Verschlüsselung größer ist als der Modulus n (was ein Angreifer natürlich erkennen und zum Anlass für eine Seitenkanalattacke nehmen könnte). Die Wahrscheinlichkeit eines solchen Überlaufs ist beschränkt durch $2^{-bl \cdot sd}$, wobei bl die verwendete Bitlänge der Langzahloperation angibt und sd die Anzahl der zusätzlichen Runden (= Ziffern) im zweiten Abschnitt der Verschlüsselung. Es ist ratsam, diese Zahlen so zu wählen, dass vorzugsweise $bl \cdot sd \geq 10$ und am meisten bevorzugt $bl \cdot sd \geq 100$ gilt, und dafür auf eine explizite Prüfung auf Überlauf zu verzichten. Sollte es trotzdem zufällig zu einem Überlauf kommen, kann das Ergebnis ohne modulare Reduktion an das Lesegerät 30a gesendet werden.

Im dritten Abschnitt der Verschlüsselung werden schließlich sukzessive die verschlüsselten Ausgabedaten erzeugt, die folglich überlappend mit dem Abschluss der Berechnung an das Lesegerät 30a gesendet werden können. Dies ist besonders vorteilhaft, da wegen der Länge des Ciphertextes C^* (bei der üblichen und notwendigen Länge des Modulus n von 1024 Bit ergibt sich ein Ciphertext von 128 Byte) die Daten ohnehin nicht in einem einzigen Übertragungsschritt (Datenblock) gesendet werden können. Handelsübliche UHF-RFID-Lesegeräte (nach ISO/IEC 18000-63) sind nicht dafür eingerichtet größere Datenblöcke zu übertragen, sondern begrenzen die Blockgröße nach dem Stand der Technik auf 2 bis 16 Byte. Durch die abschnittsweise Übertra-

gung der Daten des Ciphertextes C^* (dem sogenannten Chaining) werden die Daten in sequentieller Folge portionsweise übertragen. Die dadurch entstehende Überlappung zwischen Berechnung und Übertragung kann dahingehend sehr vorteilhaft genutzt werden, dass bereits nach dem Empfang der ersten Daten parallel zur Datenübertragung mit der Berechnung begonnen werden kann.

Fig. 4 zeigt einen Algorithmus ("MontgomerySquare") zur Berechnung des Ciphertextes C^*, d.h. zur Verschlüsselung des Klartextes M, durch das RFID-Tag 20a. Für die nachstehende Beschreibung dieses Algorithmus sind die folgenden Definitionen hilfreich. Es wird angenommen, dass die Prozessoreinheit 25 des RFID-Tags 20a eine Wortbreite von bl Bits aufweist. Dabei ist die Prozessoreinheit 25 des RFID-Tags 20a dazu ausgestaltet, zwei bl Bit breite Worte miteinander multiplizieren zu können, wobei das Ergebnis bis zu $2 \cdot bl$ Bit lang sein kann. In nicht beschränkender Art und Weise wird ferner angenommen, dass der Modulus n höchstens eine Länge von d Worten und damit $d \cdot bl$ Bits aufweist. Gemäß einer bevorzugten Ausführungsform der Erfindung wird ein Sicherheitsparameter sd derart gewählt, dass die vorstehend beschriebene Überlaufwahrscheinlichkeit in der Größenordnung $2^{-bl \cdot sd}$ liegt. Wie der Fachmann erkennt, bedingt ein größerer Wert von sd eine längere Rechenzeit. Es wird nicht beschränkend $R = 2^{bl \cdot (d+sd)}$ gesetzt. Wie vorstehend bereits beschrieben, sollte R bzw. der Sicherheitsparameter sd vorzugsweise so gewählt werden, dass vorzugsweise $bl \cdot sd \geq 10$ und am meisten bevorzugt $bl \cdot sd \geq 100$ gilt.

Zu einem Klartext M, bei dem es sich um eine Zahl handelt, mit $0 \leq M < n$ kann der Ciphertext C^* mit $C^* = M^2 \cdot R^{-1} \bmod n$ mittels der zwei folgenden Schritte berechnet werden:

1. Berechne ein a so das gilt: $a = -M^2 / n \bmod R$, $0 \leq a < R$.

2. Setze $C^* = (M^2 + a \cdot n)/R$

Hierbei ist die Division im zweiten Schritt ohne Rest ausführbar. Da $0 \leq M < n$ kann bei einem zufällig gewähltem M angenommen werden, dass der Wert a im Intervall [0, ... , R-1] ebenfalls gleich verteilt ist. Somit ist die Wahrscheinlichkeit für einen Überlauf von C^* (d.h. es gilt $C^* \geq n$) höchstens gleich n/R, und damit höchstens gleich $2^{-bl \cdot sd}$.

Zu einer ganzen Zahl x sei $(x_0, x_1, ..., x_i, ..., x_{v-1})$ die Darstellung von x zur Basis 2^{bl}, d.h. es gilt $x = \sum_{i=0}^{v-1} 2^{bl \cdot i} \cdot x_i$, $0 \leq x_i < 2^{bl}$. Seien $(M_0, ..., M_{d-1})$, $(n_0, ..., n_{d-1})$, $(a_0, ..., a_{d+sd-1})$, und $(C^*_0, ..., C^*_{d-1})$ die Darstellungen von M, n, a und C^* zur Basis 2^{bl}. Ferner sei n_{inv} die durch $n \cdot n_{inv} = -1 \pmod{2^{bl}}$ und $0 \leq n_{inv} < 2^{bl}$ eindeutig bestimmte ganze Zahl. Dann können a und C^* nach dem in Figur 4 dargestellten Algorithmus "MontgomerySquare" berechnet werden, wobei zu beachten ist, dass in dem in Figur 4 dargestellten Algorithmus die Binärziffern $C^*_0, ..., C^*_{d-1}$ von C^* mit c_{i-s-sd} bezeichnet werden.

Hinsichtlich des in Figur 4 dargestellten Algorithmus "MontgomerySquare" wird der Fachmann folgendes erkennen.

Nach i Durchläufen der Hauptschleife gilt $a = -M^2/n \pmod{2^{bl \cdot \min(i, d+sd)}}$ und im Fall $i > d + sd$ gilt außerdem $C^* = (M^2 + a \cdot n)/R \pmod{2^{bl \cdot (i-d-sd)}}$. Beim i-ten Durchlauf der Hauptschleife werden nur die ersten i Eingabewerte $M_0, ..., M_{i-1}$ benötigt, so dass dieser Durchlauf schon nach Vorliegen der ersten i Eingabewerte durchgeführt werden kann. Der i-te Ausgabewert kann schon nach $i+s+sd$ Durchläufen der Hauptschleife ausgegeben werden. Somit ist die oben beschriebene Überlappung von Eingabe, Verarbeitung und Ausgabe erfindungsgemäß ohne weiteres möglich.

Von dem Zwischenwert a werden im i-ten Durchlauf der Hauptschleife höchstens die Stellen $a_i, \ldots, a_{i-d+1}$ benötigt, so dass d Worte zu je bl Bits zur Speicherung des gerade benötigten Teils von a ausreichen.

Der Algorithmus benötigt insgesamt höchstens $(d + 1)(3d/2 + sd)$ Multiplikationen.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird zur Einsparung von Rechenzeit der Modulus n wie folgt gewählt: $n = 1 \pmod{2^{bl \cdot nd}}$, wobei nd eine ganze Zahl mit $1 \leq nd < d$ ist. In diesem Fall gilt $n_{inv} = 2^{bl} - 1$. Die Multiplikation mit $n_{inv} = 2^{bl} - 1$ (modulo 2^{bl}) ist dann eine einfache Negation. Abgesehen von der letzten Stelle n_0 sind die niederwertigen Stellen $n_{nd-1}, \ldots, n_1$ von n dann gleich null, so dass im Vergleich zu dem oben beschriebenen Algorithmus "MontgomerySquare" $nl \cdot (d+sd)$ Multiplikationen eingespart werden können. Wählt man z.B. $nl=d/2$, so liegt die Anzahl der Multiplikationen in der Größenordnung $d(d+sd)$. Dies spart etwa ein Drittel der Multiplikationen im Vergleich zum oben beschriebenen Algorithmus "MontgomerySquare". Primzahlen p, q mit $\log p \approx \log q$, $2^{bl \cdot d-1} < n = p \cdot q < 2^{bl \cdot d}$ und $n = p \cdot q = 1 \pmod{2^{bl \cdot d/2}}$ lassen sich leicht konstruieren. Die genannte Bedingung für n bedeutet, dass die Bits der unteren Hälfte (bis auf das letzte Bit) in der Binärdarstellung von n gleich null sind. Nach dem heute bekannten Stand der Forschung bedeutet dies keine Einschränkung für die Sicherheit des Verfahrens. Der schnellste derzeit bekannte Algorithmus zur Faktorisierung von beliebigen Zahlen n ist das General Number Field Sieve (GNFS). Der einzige bekannte deutlich schnellere Algorithmus, der unter gewissen Umständen eine Zahl $n = p \cdot q$, mit $\log p \approx \log q$ für Primzahlen p, q, faktorisieren kann, ist das Special Number Field Sieve (SNFS). Für ein zufällig ge-

wähltes $n = p \cdot q$, bei dem die untere Hälfte der Bits (bis auf das letzte Bit) gleich null ist, kann man das SNSF aber nicht anwenden.

Wie der Fachmann erkennen wird, müssen die einzelnen Schritte des in Figur 3 dargestellten Kommunikationsprotokolls nicht unbedingt in der dargestellten zeitlichen Abfolge ablaufen. Ersichtlich ist dies nur dort erforderlich, wo die Ergebnisse eines Schrittes die Eingabedaten eines weiteren Schrittes darstellen. Ferner wird der Fachmann erkennen, dass obgleich vorstehend bevorzugte Ausführungsformen der Erfindung unter Bezugnahme auf ein RFID-Tag beschrieben worden sind, bei dem es sich vorzugsweise um ein UHF-Tag nach ISO/IEC 18000-63 bzw. Class-1 Gen-2 EPC handelt, die Erfindung ebenfalls mit anderen Arten von ressourcenbeschränkten portablen Datenträgern vorteilhaft eingesetzt werden kann, die sich über die Luftschnittstelle gegenüber einem Lesegerät authentisieren müssen, wie beispielsweise kontaktlose Chipkarten, Tokens und dergleichen.

Patentansprüche

1. Verfahren zur gesicherten Kommunikation zwischen einem RFID-Tag (20a, 20b) und einem Lesegerät (30a, 30b), wobei das Verfahren die folgenden Schritte umfasst, die im RFID-Tag (20a, 20b) durchgeführt werden:

Verschlüsseln eines Klartextes M, in den ein Identifizierungselement (UII) des RFID-Tags (20a, 20b) oder eines damit versehenen Objekts einfließt, zur Berechnung eines Ciphertextes C^*, indem das Montgomery-Residuum des Quadrats des Klartextes M modulo n hinsichtlich einer Montgomery-Basis R, d.h. $C^* = M^2 R^{-1} \bmod n$, berechnet wird, und

Aussenden einer Authentisierungsnachricht an das Lesegerät (30a, 30b), wobei die Authentisierungsnachricht auf dem Ciphertext C^* basiert,

wobei es sich bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts (30a, 30b), bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts (30a, 30b) und bei der Montgomery-Basis R um eine ganze Zahl handelt, die größer als der Modulus n ist.

2. Verfahren zur gesicherten Kommunikation zwischen einem RFID-Tag (20a, 20b) und einem Lesegerät (30a, 30b), wobei das Verfahren die folgenden Schritte umfasst, die im Lesegerät (30a, 30b) durchgeführt werden:

Empfangen einer Authentisierungsnachricht vom RFID-Tag (20a, 20b), die auf einem verschlüsselten Klartext M basiert, in den ein Identifizierungselement (UII) des RFID-Tags (20a, 20b) oder eines damit versehenen Objekts eingeflossen ist, und

Entschlüsseln des verschlüsselten Klartextes M, wobei der Schritt des Entschlüsselns die Multiplikation des verschlüsselten Klartextes M mit einer

Montgomery-Basis R und die anschließende Durchführung der Modulo-Operation mit dem Modulus n umfasst,

wobei es sich bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts (30a, 30b), bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts (30a, 30b) und bei der Montgomery-Basis R um eine ganze Zahl handelt, die größer als der Modulus n ist.

3. Verfahren nach Anspruch 1 oder 2, wobei die vom RFID-Tag (20a, 20b) an das Lesegerät (30a, 30b) übertragene Authentisierungsnachricht den verschlüsselten Klartext M in Form des Ciphertextes C^* mit $C^* = M^2 R^{-1} \bmod n$ enthält.

4. Verfahren nach Anspruch 1 oder 2, wobei in den Klartext M ferner eine vom Lesegerät (30a, 30b) erzeugte erste Zufallszahl *RND1* und eine vom RFID-Tag (20a, 20b) erzeugte zweite Zufallszahl *RND2* einfließen, wobei die erste Zufallszahl *RND1* vorzugsweise als Challenge im Rahmen eines Challenge-Response-Verfahrens an das RFID-Tag (20a, 20b) übertragen wird.

5. Verfahren nach Anspruch 4, wobei die in den Klartext M einfließenden Daten, insbesondere das Identifizierungselement (UII) des RFID-Tags, die erste Zufallszahl *RND1* und die zweite Zufallszahl *RND2*, mittels einer Interleaving-Operation verwürfelt werden, um die vom Lesegerät (30a, 30b) und vom RFID-Tag (20a, 20b) stammenden zufälligen Daten zufällig über den Klartext M zu verteilen.

6. Verfahren nach Anspruch 4, wobei das RFID-Tag (20a, 20b) derart ausgestaltet ist, dass das RFID-Tag (20a, 20b) noch während des Einlesens der Challenge in Form der ersten Zufallszahl *RND1* mit der Verschlüsselung beginnen kann und die ersten Bytes des berechneten Ciphertextes C^* bereits

an das Lesegerät (30a, 30b) ausgegeben werden können, während die nachfolgenden Bytes des Ciphertextes C^* noch berechnet werden.

7. Verfahren nach Anspruch 1 oder 2, wobei ferner eine digitale Signatur (SIG(UII)) des Identifizierungselements (UII) des RFID-Tags (20a, 20b) in den Klartext M einfließt, die vorzugsweise in der Speichereinheit (26) des RFID-Tags (20a, 20b) hinterlegt ist und vom Lesegerät (30a, 30b) überprüft werden kann.

8. Verfahren nach Anspruch 1 oder 2, wobei zur Einsparung von Rechenzeit der Modulus n wie folgt gewählt wird: $n = 1 (\mathrm{mod}\, 2^{bl \cdot nd})$, wobei nd eine ganze Zahl mit $1 \leq nd < d$ ist, bl die Wortbreite der Prozessoreinheit (25) des RFID-Tags (20a, 20b) und d die Länge des Modulus n in Wortbreiten der Prozessoreinheit (25) ist.

9. Verfahren nach Anspruch 1 oder 2, wobei für einen gegebenen Modulus n die Montgomery-Basis R wie folgt gewählt wird: $R = 2^{bl \cdot (d+sd)}$, wobei bl die Wortbreite der Prozessoreinheit (25) des RFID-Tags (20a, 20b), d die Länge des Modulus n in Wortbreiten der Prozessoreinheit (25) und sd ein Sicherheitsparameter ist, der so gewählt ist, dass $bl \cdot sd \geq 1$, vorzugsweise $bl \cdot sd \geq 10$ und am meisten bevorzugt $bl \cdot sd \geq 100$ gilt.

10. RFID-Tag (20a, 20b) zur gesicherten Kommunikation mit einem Lesegerät (30a, 30b), wobei das RFID-Tag (20a, 20b) eine Prozessoreinheit (25) und eine Speichereinheit (26) umfasst, in der ein Identifizierungselement (UII) hinterlegt ist, und wobei die Prozessoreinheit (25) dazu ausgestaltet ist, einen Klartext M, in den das Identifizierungselement (UII) des RFID-Tags (20a, 20b) oder eines damit versehenen Objekts einfließt, zur Berechnung eines Ciphertextes C^* zu verschlüsseln, indem das Montgomery-Residuum

des Quadrats des Klartextes M modulo n hinsichtlich einer Montgomery-Basis R, d.h. $C^* = M^2 R^{-1} \bmod n$, berechnet wird, und eine Authentisierungsnachricht an das Lesegerät (30a, 30b) zu senden, wobei die Authentisierungsnachricht auf dem Ciphertext C^* basiert und wobei es sich bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts (30a, 30b), bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts (30a, 30b) und bei der Montgomery-Basis R um eine ganze Zahl handelt, die größer als der Modulus n ist.

11. Lesegerät (30a, 30b) zur gesicherten Kommunikation mit einem RFID-Tag (20a, 20b), wobei das Lesegerät (30a, 30b) eine Prozessoreinheit umfasst, die dazu ausgestaltet ist, eine Authentisierungsnachricht vom RFID-Tag (20a, 20b) zu empfangen, die auf einem verschlüsselten Klartext M basiert, in den ein Identifizierungselement (UII) des RFID-Tags (20a, 20b) oder eines damit versehenen Objekts eingeflossen ist, und den verschlüsselten Klartext M zu entschlüsseln, wobei bei der Entschlüsselung der verschlüsselte Klartext M mit einer Montgomery-Basis R multipliziert und anschließend die Modulo-Operation mit dem Modulus n durchgeführt wird, wobei es sich bei dem Modulus $n = p \cdot q$ um den öffentlichen Schlüssel des Lesegeräts (30a, 30b), bei den Primzahlen p, q um den privaten Schlüssel des Lesegeräts (30a, 30b) und bei der Montgomery-Basis R um eine ganze Zahl handelt, die größer als der Modulus n ist.

12. System (10) zur gesicherten Kommunikation mit wenigstens einem RFID-Tag (20a, 20b) gemäß Anspruch 10 und wenigstens einem Lesegerät (30a, 30b) gemäß Anspruch 11.

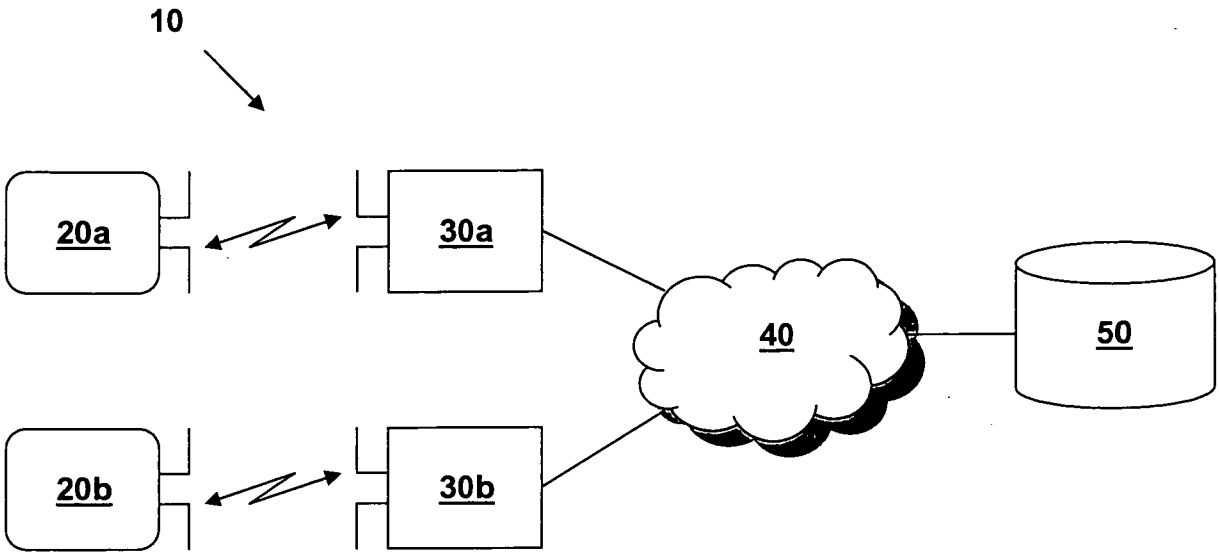


Fig. 1

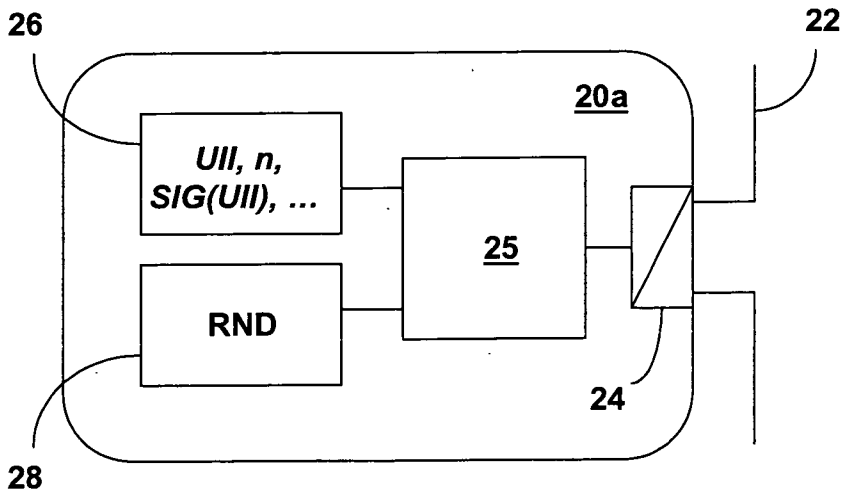


Fig. 2

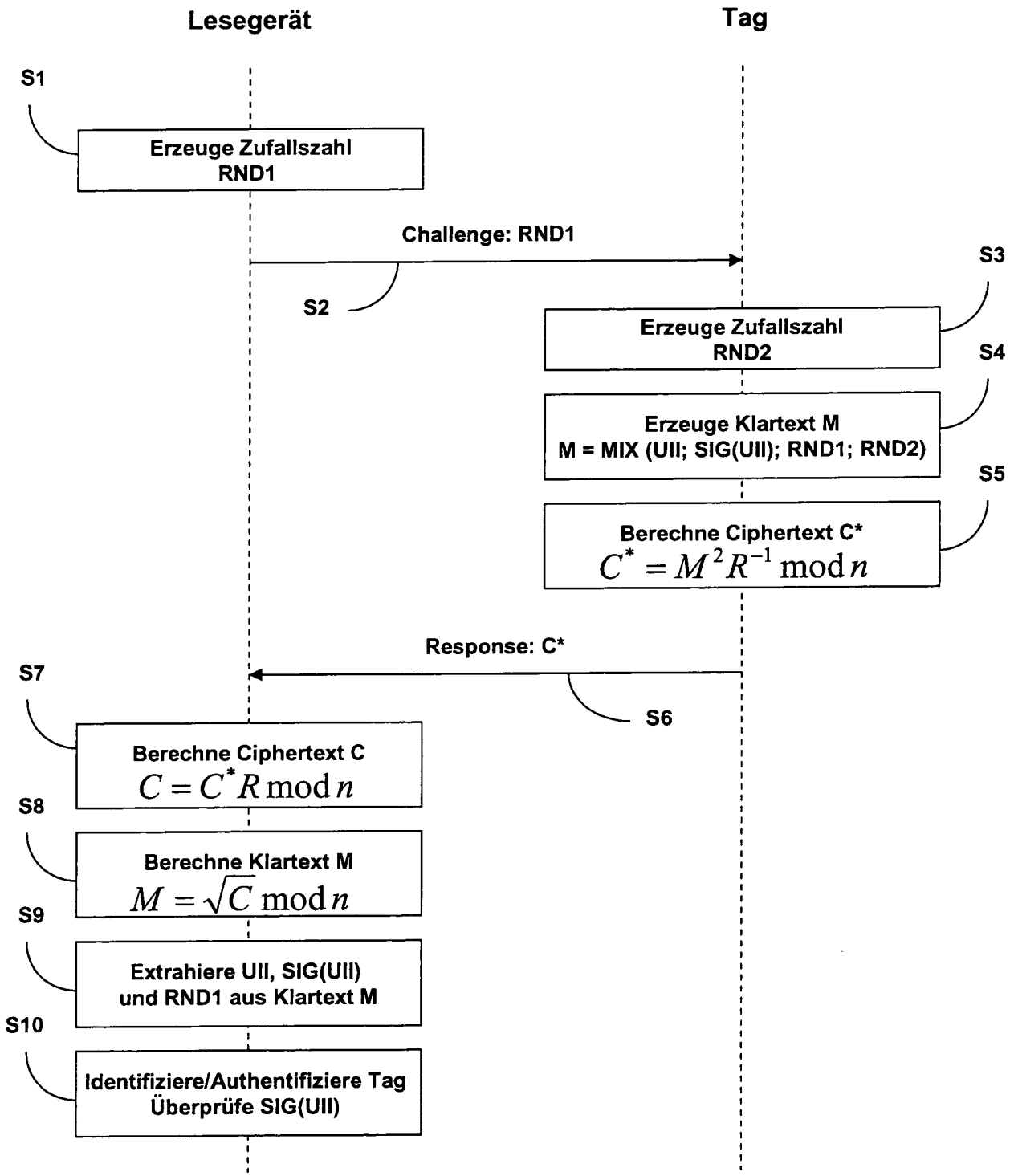

Lesegerät
Tag
S1
Erzeuge Zufallszahl RND1
Challenge: RND1
S2
S3
Erzeuge Zufallszahl RND2
S4
Erzeuge Klartext M
M = MIX (UII; SIG(UII); RND1; RND2)
S5
Berechne Ciphertext C*
$C^* = M^2 R^{-1} \bmod n$
Response: C*
S6
S7
Berechne Ciphertext C
$C = C^* R \bmod n$
S8
Berechne Klartext M
$M = \sqrt{C} \bmod n$
S9
Extrahiere UII, SIG(UII) und RND1 aus Klartext M
S10
Identifiziere/Authentifiziere Tag
Überprüfe SIG(UII)

Fig. 3

```
Algorithmus MontgomerySquare:
    acc = 0
    i = 0
    while (i < 2 * d + sd):
        // Quadrieren von m
        j = max(0, i + 1 - d);  k = i - j
        acc1 = 0
        while k > j:
            acc1 = acc1 + m_j * m_k
            j = j + 1 ;  k = k - 1
        acc = acc + 2 * acc1
        if j == k:
            acc = acc + m_j * m_j
        // Montgomery Reduktion
        if i < d + sd:
            k = min(i, d - 1);  j = i - k
            while k > 0:
                acc =  acc + a_j * n_k
                j = j + 1;  k = k - 1
            a_i = (acc * n_inv) mod 2^bl
            acc = acc + a_i * n_j
        else:
            k = max(0, i - d - sd + 1);  j = i - k
            while k < d:
                acc = acc +  a_j * n_k
                j = j - 1;  k = k + 1
            c_i-d-sd = acc mod 2^bl
        acc = acc / 2^bl
        i = i + 1
    stop
```

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/000421

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/30 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 198 20 605 A1 (GIESECKE & DEVRIENT GMBH [DE]) 11 November 1999 (1999-11-11) the whole document -----	1-12
X	OREN Y ET AL: "A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes", PROCEEDINGS OF THE SECOND ACM CONFERENCE ON WIRELESS NETWORK SECURITY : ZURICH, SWITZERLAND, MARCH 16 - 18, 2009, NEW YORK, NY : ACM, vol. 2009, 16 March 2009 (2009-03-16), pages 59-68, XP001553406, ISBN: 978-1-60558-460-7 cited in the application the whole document ----- -/--	1-12

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 May 2013	14/05/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Di Felice, M

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/000421

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHAE HOON LIM ED - HEUNG YOUL YOUM ET AL: "Practical Broadcast Authentication Using Short-Lived Signatures in WSNs", 25 August 2009 (2009-08-25), INFORMATION SECURITY APPLICATIONS, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 366 - 383, XP019136005, ISBN: 978-3-642-10837-2 the whole document	1-12
A	MONTGOMERY P L: "MODULAR MULTIPLICATION WITHOUT TRIAL DIVISION", MATHEMATICS OF COMPUTATION, AMERICAN MATHEMATICAL SOCIETY, US, vol. 44, no. 170, 1 April 1985 (1985-04-01), pages 519-521, XP000747434, the whole document	1-12
X,P	Walter Hinz ET AL: "Secure UHF Tags with Strong Cryptography", SENSORNETS 2013, 2nd international conference on sensor networks, 21 February 2013 (2013-02-21), pages 1-9, XP055061853, Retrieved from the Internet: URL:http://www.rfid-handbook.de/downloads/SensorNets2013-Paper_V20121120.pdf [retrieved on 2013-05-03] the whole document	1-12
A,P	CHIEN-NING CHEN ET AL: "Standardized Signature Algorithms on Ultra-constrained 4-Bit MCU", 7 November 2012 (2012-11-07), ADVANCES IN INFORMATION AND COMPUTER SECURITY, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 37 - 50, XP047021122, ISBN: 978-3-642-34116-8 the whole document	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/000421

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19820605 A1	11-11-1999	AT 305683 T	15-10-2005
		DE 19820605 A1	11-11-1999
		DE 59912605 D1	03-11-2005
		EP 1080559 A1	07-03-2001
		JP 4708565 B2	22-06-2011
		JP 2002515614 A	28-05-2002
		US 6405923 B1	18-06-2002
		WO 9959287 A1	18-11-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/000421

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L9/30 H04L9/32
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 198 20 605 A1 (GIESECKE & DEVRIENT GMBH [DE]) 11. November 1999 (1999-11-11) das ganze Dokument	1-12
X	OREN Y ET AL: "A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes", PROCEEDINGS OF THE SECOND ACM CONFERENCE ON WIRELESS NETWORK SECURITY : ZURICH, SWITZERLAND, MARCH 16 - 18, 2009, NEW YORK, NY : ACM, Bd. 2009, 16. März 2009 (2009-03-16), Seiten 59-68, XP001553406, ISBN: 978-1-60558-460-7 in der Anmeldung erwähnt das ganze Dokument	1-12

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
6. Mai 2013	14/05/2013

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Di Felice, M

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/000421

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	CHAE HOON LIM ED - HEUNG YOUL YOUM ET AL: "Practical Broadcast Authentication Using Short-Lived Signatures in WSNs", 25. August 2009 (2009-08-25), INFORMATION SECURITY APPLICATIONS, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 366 - 383, XP019136005, ISBN: 978-3-642-10837-2 das ganze Dokument	1-12
A	MONTGOMERY P L: "MODULAR MULTIPLICATION WITHOUT TRIAL DIVISION", MATHEMATICS OF COMPUTATION, AMERICAN MATHEMATICAL SOCIETY, US, Bd. 44, Nr. 170, 1. April 1985 (1985-04-01), Seiten 519-521, XP000747434, das ganze Dokument	1-12
X,P	Walter Hinz ET AL: "Secure UHF Tags with Strong Cryptography", SENSORNETS 2013, 2nd international conference on sensor networks, 21. Februar 2013 (2013-02-21), Seiten 1-9, XP055061853, Gefunden im Internet: URL:http://www.rfid-handbook.de/downloads/SensorNets2013-Paper_V20121120.pdf [gefunden am 2013-05-03] das ganze Dokument	1-12
A,P	CHIEN-NING CHEN ET AL: "Standardized Signature Algorithms on Ultra-constrained 4-Bit MCU", 7. November 2012 (2012-11-07), ADVANCES IN INFORMATION AND COMPUTER SECURITY, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 37 - 50, XP047021122, ISBN: 978-3-642-34116-8 das ganze Dokument	1-12

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/000421

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19820605 A1	11-11-1999	AT 305683 T	15-10-2005
		DE 19820605 A1	11-11-1999
		DE 59912605 D1	03-11-2005
		EP 1080559 A1	07-03-2001
		JP 4708565 B2	22-06-2011
		JP 2002515614 A	28-05-2002
		US 6405923 B1	18-06-2002
		WO 9959287 A1	18-11-1999