(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
21. August 2003 (21.08.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/069462 A2

(51) Internationale Patentklassifikation[7]: G06F 7/00

(21) Internationales Aktenzeichen: PCT/EP03/00669

(22) Internationales Anmeldedatum:
23. Januar 2003 (23.01.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 05 713.3 12. Februar 2002 (12.02.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **FISCHER, Wieland** [DE/DE]; Müllerstr. 11, 80469 München (DE).

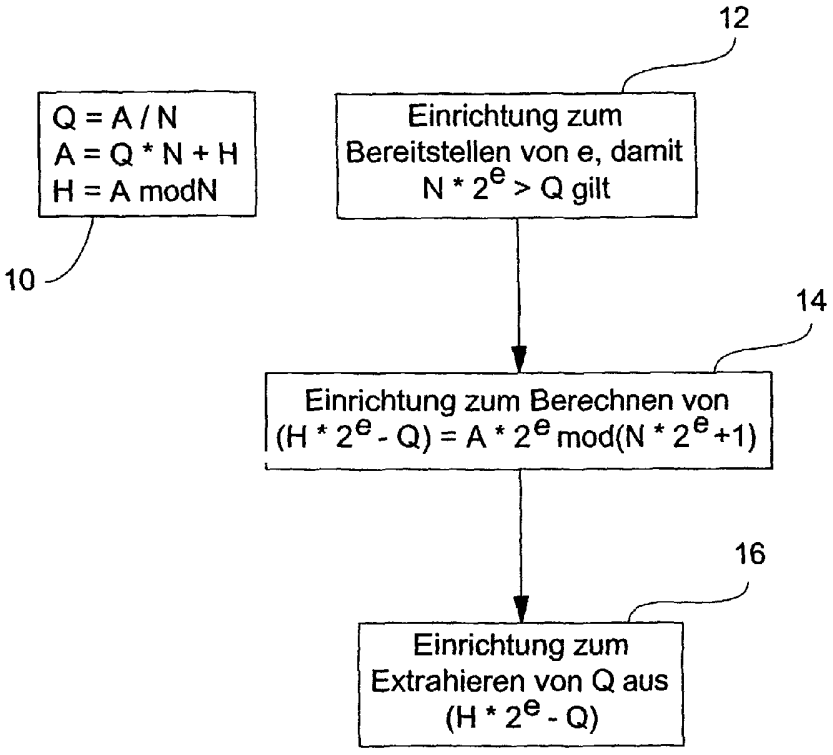
(74) Anwälte: **SCHOPPE, Fritz** usw.; Schoppe, Zimmermann, Stöckeler & Zinkler, Postfach 246, 82043 Pullach bei München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR,

[Fortsetzung auf der nächsten Seite]

(54) Title: SYSTEM AND METHOD FOR CALCULATING A RESULT FROM A DIVISION

(54) Bezeichnung: VORRICHTUNG UND VERFAHREN ZUM BERECHNEN EINES ERGEBNISSES AUS EINER DIVISION



12... DEVICE FOR PROVIDING E GIVEN THAT $N * 2^E > Q$

14... DEVICE FOR CALCULATING $(H * 2^E - Q) = A * 2^E MOD(N * 2^E + 1)$

16... DEVICE FOR EXTRACTING Q FROM $(H * 2^E - Q)$

(57) Abstract: The invention relates to a system for calculating a result or an integer multiple of the result (Q) from a division of a numerator (A) by a denominator (N). The inventive system comprises a device (12) for providing a factor that is selected so that a product of the factor and the denominator is greater than the result. The system also comprises a device (14) for modularly reducing a first product of the numerator and the factor while using a modulus, which is equal to the sum of a second product of the denominator, the factor and an integer in order to obtain an auxiliary quantity that contains the result. A device (16) is used for extracting the result or the integer multiple of the result from the auxiliary quantity. This reduces a division to a modular reduction and to an extraction requiring few calculations whereby increasing speed and certainty, particularly when carrying out long number division problems.

[Fortsetzung auf der nächsten Seite]

WO 03/069462 A2

CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Eine Vorrichtung zum Berechnen eines Ergebnisses oder eines ganzzahligen Vielfachen des Ergebnisses (Q) aus einer Division eines Zählers (A) durch einen Nenner (N) umfaßt eine Einrichtung (12) zum Bereitstellen eines Faktors, der so gewählt ist, daß ein Produkt aus dem Faktor und dem Nenner größer als das Ergebnis ist. Die Vorrichtung umfaßt ferner eine Einrichtung (14) zum modularen Reduzieren eines ersten Produkts aus dem Zähler und dem Faktor unter Verwendung eines Moduls, der gleich einer Summe aus einem zweiten Produkt des Nenners und des Faktors und einer ganzen Zahl ist, um eine Hilfsgröße zu erhalten, die das Ergebnis aufweist. Eine Einrichtung (16) wird verwendet, um das Ergebnis oder das ganzzahlige Vielfache des Ergebnisses aus der Hilfsgröße zu extrahieren. Eine Division wird somit auf eine modulare Reduktion und eine rechenunaufwendige Extraktion zurückgeführt, so daß insbesondere bei Langzahl-Divisionsaufgaben die Schnelligkeit einerseits und die Sicherheit andererseits erhöht sind.

Beschreibung

Vorrichtung und Verfahren zum Berechnen eines Ergebnisses aus einer Division

Die vorliegende Erfindung bezieht sich auf kryptographische Algorithmen und insbesondere auf Divisionsalgorithmen, die für kryptographische Anwendungen geeignet sind.

In kryptographischen Algorithmen wird oftmals die Division zweier langer Zahlen benötigt. Beispielsweise ist im RSA-Algorithmus der Modul N ein Produkt aus zwei Primzahlen p, q, wobei q erhalten wird, wenn N durch p geteilt wird, oder p erhalten wird, wenn N durch q geteilt wird.

Ist eine Divisionsroutine auf einem dafür verwendeten kryptographischen Coprozessor nicht als expliziter Befehl, der aus Mikrobefehlen besteht, die schnell intern abgearbeitet werden, eingebaut, so muß die Division mittels Software geschehen. Konventionelle Divisionsroutinen hierfür sind einerseits langsam und andererseits nicht sicher gegen SPA-Angriffe (SPA = Simple Power Analysis = einfache Leistungsanalyse).

Übliche Divisionsroutinen, wie sie beispielsweise in "Computer Arithmetic, Henessy und Patterson, Morgan Kaufmann Publishers, Inc., 1996, beschrieben sind, wie z. B. die Restoring-Division, die Non-Restoring-Division, etc. basieren darauf, daß Registerverschiebungen vorgenommen werden, und daß dann Subtraktionen bzw. Additionen durchgeführt werden, abhängig davon, ob bestimmte Bits bestimmte Werte haben. Solche Routinen sind für SPA-Angriffe anfällig, da der Strom- bzw. Leistungsverbrauch und darüber hinaus der Zeitverbrauch von den zu verarbeitenden Zahlen abhängt. Ein Angreifer könnte daher anhand des Strom- bzw. Zeit-Profils Rückschlüsse auf die verarbeiteten Zahlen erhalten und somit z. B. einen geheimen Schlüssel eines Public-Key-Kryptoalgorithmus ausspähen.

Um diesem Problem zu begegnen, werden sogenannte Dummy-Operationen eingebaut, durch die eine Homogenisierung des Stromprofils erreicht werden kann. Der Einbau von Dummy-Operationen hat jedoch einen zusätzlichen Performance-Verlust zur Folge, der bis zu 33% betragen kann.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein effizienteres und sichereres Konzept zum Berechnen einer Division zu schaffen.

Diese Aufgabe wird durch eine Vorrichtung zum Berechnen eines Ergebnisses einer Division nach Patentanspruch 1 oder durch ein Verfahren zum Berechnen eines Ergebnisses einer Division nach Patentanspruch 15 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß insbesondere für kryptographische Zwecke von den klassischen Divisionsroutinen weggegangen werden muß, um eine Division auszuführen. Erfindungsgemäß wird eine Division auf eine modulare Reduktion zurückgeführt, indem ein Faktor eingeführt wird, der so gewählt ist, daß ein Produkt aus dem Faktor und dem Nenner für die Division größer als das Ergebnis der Division ist. Die modulare Reduktion wird auf ein erstes Produkt aus dem Zähler und dem Faktor ausgeführt, wobei ein Modul verwendet wird, der gleich einer Summe aus einem zweiten Produkt des Nenners und des Faktors und einer ganzen Zahl ist, um eine Hilfsgröße zu erhalten, die das Ergebnis der Division aufweist. Schließlich kann das Ergebnis ohne großen Rechenaufwand aus der Hilfsgröße extrahiert werden.

Das erfindungsgemäße Konzept ist dahingehend vorteilhaft, daß das Strom- und/oder Zeitprofil unabhängig von den zu verarbeitenden Größen, also von dem Zähler und dem Nenner, sind. Darüber hinaus kann die modulare Reduktion, auf die die zu berechnende Division letztendlich zurückgeführt wird, rechenEffizient ausgeführt werden. Insbesondere bei Kryptoprozesso-

ren ist die modulare Reduktion eine vielfach verwendete Operation, für die typischerweise effiziente Algorithmen hardwaremäßig in einem Kryptocoprozessor implementiert sind. Die modulare Reduktion kann daher schnell und effizient ausgerechnet werden.

Je nach Hardwareimplementation kann die Extraktion des Ergebnisses der Division aus der Hilfsgröße entweder unmittelbar aus einem Langzahlregister abgelesen werden, wenn ein Register ausreichender Länge vorhanden ist.

Alternativ kann zur Extraktion des Ergebnisses eine weitere modulare Reduktion und eine Subtraktion durchgeführt werden, wobei in diesem Fall der Rechenaufwand ebenfalls im Rahmen bleibt, da auch die weitere modulare Reduktion schnell und sicher unter Verwendung von auf Kryptocoprozessoren ohnehin vorhandenen effizienten Reduktionsschaltungen durchgeführt wird.

Das erfindungsgemäße Konzept liefert bei gleichzeitiger Erhöhung der Sicherheit eine wesentliche Beschleunigung der Division. Eine Division langer Zahlen benötigt bei dem bekannten Prozessor ACE (ACE = Advanced Crypto Engine), der von der Infineon Technologies AG aus München, Bundesrepublik Deutschland, verfügbar ist, etwa 27 Takte pro Bit. Die erfindungsgemäße Division benötigt auf demselben Prozessor lediglich sechs Takte pro Bit, was einer Beschleunigung um das 4,5-fache entspricht.

Das erfindungsgemäße Divisionskonzept ist gleichzeitig gegenüber SPA-Attacken sicher, da der Strom- bzw. Zeitverbrauch unabhängig von dem speziellen Bitmuster der verarbeiteten Zahlen, also des Zählers und des Nenners, ist.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild einer erfindungsgemäßen Vorrichtung zum Berechnen einer Division;

Fig. 2 ein Blockschaltbild eines erfindungsgemäßen Verfahrens gemäß einem bevorzugten Ausführungsbeispiel; und

Fig. 3 eine Darstellung der Hilfsgröße in einem binären Langzahlregister zur Erläuterung einer Extraktion des Ergebnisses aus der Hilfsgröße.

Bevor detailliert auf die Figuren eingegangen wird, wird zunächst eine Herleitung des erfindungsgemäßen Divisionskonzepts gegeben, das auf einer modularen Reduktion eines ersten Produkts aus dem Zähler und dem Faktor basiert, wobei der Modul gleich einer Summe aus einem zweiten Produkt aus dem Nenner und dem Faktor und einer ganzen Zahl ist.

Gesucht wird das Ergebnis Q aus einer Division eines Zählers A durch einen Nenner N gemäß folgender Gleichung:

$$Q = A/N \tag{1}$$

Ohne Einschränkung der Allgemeinheit sei angenommen, daß sowohl der Zähler A als auch der Nenner N binäre Zahlen sind, so daß gilt:

$$2^{a-1} \leq A < 2^{a} \tag{2a}$$

$$2^{n-1} \leq N < 2^{n} \tag{2b}$$

Die Gleichungen 2a und 2b geben die Größenordnungen des Zählers A und des Nenners N an.

Gleichung 1 kann folgendermaßen umgeformt werden:

$$A = Q \cdot N + H \tag{3a}$$

Der Wert H aus Gleichung 3 berechnet sich folgendermaßen:

$$H = A - Q \cdot N \tag{3b}$$

wobei der Wert H größer oder gleich 0 und kleiner als N ist.

Aus Gleichung 3a wird ersichtlich, daß das Ergebnis Q der Division, das im nachfolgenden von Interesse ist, das ganzzahlige Ergebnis ist, während die Größe H der Rest ist. Das Ergebnis Q der Division aus A und N stellt somit das Ergebnis der sogenannten DIV-Operation dar, während der Rest H durch die modulare Reduktion des Zählers A mit dem Nenner N als Modul erhalten wird:

$$H = A \bmod N. \tag{4}$$

Es sei darauf hingewiesen, daß jede Gleitkommadivision auf eine ganzzahlige Division zurückgeführt werden kann, nämlich z. B. durch Kommaverschiebung und durch eine Rundung auf die nächste ganze Zahl. Üblicherweise werden Gleitkommadivisionen innerhalb eines Rechenwerks auf ganzzahlige Divisionen zurückgeführt.

Erfindungsgemäß wird nunmehr ein Faktor F eingeführt, der im Falle eines binären Zahlensystems folgendermaßen definiert ist:

$$F = 2^e \tag{5}$$

Die Basis ist, da hier lediglich beispielhaft ein binäres Zahlensystem betrachtet wird, die Zahl 2, während der Faktor F sich ergibt, wenn die Basis 2 mit einem Exponenten e potenziert wird. Erfindungsgemäß muß der Faktor F folgende Bedingung erfüllen:

$$N \cdot F > Q \qquad (6)$$

beziehungsweise, wenn Gleichung 5 in Gleichung 6 eingesetzt wird:

$$N \cdot 2^e > Q \qquad (7)$$

Der Faktor wird also so bestimmt, daß das Produkt aus dem Faktor F und dem Nenner der Division (Gleichung 1) größer als das gesuchte Ergebnis Q der Division ist.

Es sei darauf hingewiesen, daß für diese Betrachtung das genaue Ergebnis Q der Division nicht bekannt sein muß, gerade dieses soll ja berechnet werden. Lediglich die Größenordnung von Q muß bekannt sein, um den Faktor F richtig zu dimensionieren.

So ist es jedoch typischerweise kein Problem, die Größenordnung des Ergebnisses der Division aus dem Zähler und dem Nenner abzuschätzen, zumal Gleichung 6 lediglich eine Größer-als-Bedingung umfaßt, so daß immer ein korrekter Ablauf des Algorithmus sichergestellt ist, wenn der Faktor F sehr groß gewählt wird.

Es wird jedoch bevorzugt, den Faktor eher kleiner zu wählen, da der Faktor die Länge der für die Berechnung der Division benötigten Register bestimmt. Wird der Faktor sehr groß gewählt, werden sehr lange Register benötigt, während kürzere Register ausreichen, wenn der Faktor F kleiner gewählt wird. Die nachfolgende Gleichung 8 gibt für den binären Fall (Gleichung 5) eine bevorzugte Dimensionierung der Größe e an:

$$e \geq a + 2 - 2n \qquad (8)$$

Gleichung 8 enthält lediglich Informationen über den Zähler A (Gleichung 2a) und Informationen über den Nenner N (Gleichung

2b). Wenn e so wie in Gleichung 8 dimensioniert wird, so ist die Bedingung für den Faktor aus Gleichung 6 immer erfüllt.

Wenn Gleichung 3 mit dem Faktor F multipliziert wird, so ergibt sich folgende Gleichung:

$$A \cdot F = Q \cdot N \cdot F + H \cdot F \qquad (9)$$

Wenn darüber hinaus Gleichung 4 ebenfalls mit dem Faktor F auf beiden Seiten multipliziert wird, so ergibt sich folgende Gleichung 10:

$$H \cdot F = A \cdot F \bmod (N \cdot F) \qquad (10)$$

Es gilt ferner:

$$0 \leq H \cdot F < N \cdot F \qquad (11)$$

Gleichung 11 zeigt an, daß das Ergebnis der modularen Reduktion von Gleichung 10 in der Restklasse des Moduls N · F liegen muß, also größer oder gleich 0 und kleiner als N · F ist.

Auf der rechten Seite von Gleichung 9 wird nunmehr das Resultat Q hinzuaddiert und gleichzeitig abgezogen, was folgender Gleichung entspricht:

$$A \cdot F = Q \cdot N \cdot F + Q + H \cdot F - Q \qquad (12)$$

Wenn Gleichung 12 so umgeformt wird, daß das Resultat Q von den ersten beiden Termen auf der rechten Seite von Gleichung 12 ausgeklammert wird, so ergibt sich folgender Ausdruck:

$$A \cdot F = Q\,(N \cdot F + 1) + H \cdot F - Q \qquad (13)$$

Alternativ kann Gleichung 12 auch so umgeformt werden, daß die Summe von HF und Q und nicht die Differenz beider Terme gebildet wird:

$$A \cdot F = Q\ (N \cdot F - 1) + H \cdot F + Q \qquad (13')$$

Eine Umformung von Gleichung 13 bzw. 13' dahingehend, daß die Differenz $H \cdot F - Q$ (bzw. deren Summe) auf der linken Seite der Gleichung steht, führt zu folgendem Ausdruck:

$$H \cdot F - Q = A \cdot F - Q\ (N \cdot F + 1) \qquad (14)$$

Für die "Summenalternative" ergibt sich folgendes:

$$H \cdot F + Q = A \cdot F - Q\ (N \cdot F - 1) \qquad (14')$$

Wenn Gleichung 14 oder 14' nunmehr mit Gleichung 3a und 3b verglichen wird, so zeigt sich, daß Gleichung 14 eine neue Bestimmungsgleichung für eine neue Division ist, wobei die Differenz bzw. Summe auf der linken Seite von Gleichung 14 bzw. 14', also die Hilfsgröße $(H \cdot F - Q)$ bzw. $(H \cdot F + Q)$, in der das gesuchte Resultat Q enthalten ist, dem Rest einer ganzzahligen Division eines Zählers $A \cdot F$ durch einen Nenner $(N \cdot F + 1)$ bzw. $(N \cdot F - 1)$ entspricht.

Der Rest dieser Division, also die Hilfsgröße auf der linken Seite von Gleichung 14 kann durch folgende Gleichung 15 in Analogie zu Gleichung 4 berechnet werden:

$$H \cdot F - Q = A \cdot F \bmod (N \cdot F + 1) \qquad (15)$$

Gleichung 15 stellt somit die modulare Reduktion dar, die als Ergebnis die Hilfsgröße $H \cdot F - Q$ ergibt, aus der, wie es nachfolgend dargestellt ist, auf verschiedene Arten und Weisen ohne erheblichen Aufwand das gesuchte Resultat Q extrahiert werden kann. Gleichung 15 stellt somit die zentrale modulare Reduktion dar, auf die die Division (Gleichung 1) zurückgeführt worden ist. Es sei darauf hingewiesen, daß die Differenz auf der linken Seite der vorstehenden Gleichung auch negativ sein könnte. In diesem Fall wird der Modul hin-

zuaddiert, damit die Gleichung erfüllt ist, zumal das Ergebnis einer modularen Reduktion per Definition nicht negativ sein kann.

Für die "Summenalternative" ergibt sich folgende Gleichung:

$$H \cdot F + Q = A \cdot F \bmod (N \cdot F - 1) \qquad (15')$$

Wie es nachfolgend dargelegt wird, existieren verschiedene Möglichkeiten, um das gesuchte Resultat Q aus der Hilfsgröße $H \cdot F +/- Q$ zu extrahieren.

Hierzu wird zunächst auf Fig. 3 Bezug genommen, um eine Art und Weise zum Extrahieren des Ergebnisses Q der Division des Zählers A durch den Nenner N zu zeigen. Fig. 3 zeigt ein binäres Langzahlregister 300, in das das Ergebnis der modularen Reduktion auf der rechten Seite von Gleichung 15 eingespeichert worden ist. Das Langzahlregister hat eine msb-Seite und eine lsb-Seite (msb = most significant bit = höchstwertiges Bit; lsb = least significant bit = niederstwertiges Bit).

In dem Register 300 befinden sich nunmehr die Zahlen $H \cdot F$ und Q wie folgt. Die Zahl $H \cdot F$ ist eine große Zahl und entspricht hinsichtlich ihres Bitmusters der Zahl H, wie es in Fig. 3 dargestellt ist, da die Zahl $H \cdot F$ aus der Zahl H erhalten wird, wenn die Zahl H um i Stellen in dem Langzahlregister nach links verschoben wird, wobei der Faktor F als 2^e gewählt ist.

Darüber hinaus ist in dem binären Langzahlregister 300 von Fig. 3 eine im Vergleich zur Zahl $H \cdot F$ kleine Zahl "-/+Q" enthalten, d. h. das Negative bzw. das Positive des gesuchten Ergebnisses Q. Ist das Langzahlregister 300 so groß und ist der Faktor F so groß gewählt worden, daß sich die Zahlen H und -Q bzw. +Q im Register 300 nicht überlappen, wobei ein solcher Fall in Fig. 3 dargestellt ist, so kann die gesuchte Zahl -Q aus dem Register 300 direkt ausgelesen werden. Die

Zahl Q ergibt sich nach einer Invertierung von -Q. Hierzu sind die entsprechenden Bits auf der lsb-Seite des Registers zu betrachten (das ergibt -Q). Dann wird - bei der üblichen Verwendung des Zweierkomplements - das darin enthaltene Bitmuster invertiert, wonach noch zu den invertierten Bits eine Eins hinzuaddiert wird, um das gesuchte Resultat Q zu erhalten.

Es ist somit lediglich eine einfache arithmetische Operation in Form des Hinzuaddierens einer Eins zu den invertierten Bits erforderlich. Keine größeren arithmetischen Operationen, wie z. B. eine Subtraktion unter Verwendung des Registerinhalts etc., ist vonnöten. Aufgrund der Größenunterschiede der Zahlen $H \cdot F$ und Q ist es ohne weiteres möglich Q gewissermaßen aus dem Register 300 separat abzulesen, also aus der Hilfsgröße (der linken Seite von Gleichung 15) zu extrahieren.

Es sei darauf hingewiesen, daß der Faktor F nicht unbedingt so groß gewählt werden muß, daß die Zahlen H und -Q in dem in Fig. 3 gezeigten Register keinen Überlappungsbereich haben. Selbst wenn diese Zahlen einen Überlappungsbereich haben, ist es ebenfalls, wie es nachfolgend dargelegt wird, möglich, die Zahl Q aus der Hilfsgröße zu extrahieren. Hierzu wird eine weitere modulare Reduktion ausgeführt, wie sie in Gleichung 16 dargestellt ist:

$$H \cdot F = A \cdot F \bmod (N \cdot F) \qquad (16)$$

Gleichung 16 entspricht Gleichung 4, wobei jedoch nunmehr der Faktor F berücksichtigt ist.

Das gesuchte Resultat Q ergibt sich in diesem Fall dadurch, daß von dem Ergebnis von Gleichung 16 die Gleichung 15 subtrahiert wird:

$$H \cdot F - (H \cdot F - Q) = Q \qquad (17)$$

Es sei auf folgende Fallunterscheidung hingewiesen, wenn die Hilfsgröße, also die Differenz $H \cdot F - Q$ negativ ist. Wenn die Differenz $H \cdot F - Q$ in Gleichung 15 negativ ist, so wird auf der linken Seite von Gleichung 15 der Modul $(N \cdot F + 1)$ hinzuaddiert, da definitionsgemäß das Ergebnis einer modularen Reduktion stets positiv sein soll. Wenn also die Hilfsgröße negativ ist, so daß in Gleichung 15 auf der linken Seite ein Modul hinzuaddiert wird, so wird dies auch bei der Subtraktion der Gleichung 15 von der Gleichung 16 folgendermaßen berücksichtigt:

$$Q = A \cdot F \bmod (N \cdot F) - A \cdot F \bmod (N \cdot F+1) + N \cdot F+1 \qquad (18)$$

Im nachfolgenden wird auf Fig. 1 eingegangen, um ein Blockschaltbild einer bevorzugten Vorrichtung zum Berechnen eines Ergebnisses, oder, wie es später noch ausgeführt wird, eines ganzzahligen Vielfachen des Ergebnisses Q einer Division eines Zählers durch einen Nenner zu berechnen. Die Bestimmungsgleichungen sind der Übersichtlichkeit halber in einem Block 10 in Fig. 1 dargestellt. Die erfindungsgemäße Vorrichtung umfaßt eine Einrichtung 12 zum Bereitstellen eines Faktors und insbesondere einer Zahl e, die als Exponent der Basis 2 den Faktor bildet, damit Gleichung 6 bzw. Gleichung 7 erfüllt ist.

Die erfindungsgemäße Vorrichtung umfaßt ferner eine Einrichtung 14 zum Berechnen der Hilfsgröße, also zum Ausführen der Gleichung 15. Schließlich umfaßt die erfindungsgemäße Vorrichtung eine Einrichtung 16 zum Extrahieren von Q aus der Hilfsgröße auf eine von verschiedenen Arten und Weisen, beispielsweise durch den in Fig. 3 beschriebenen Mechanismus oder durch Berechnen einer weiteren modularen Reduktion (Gleichung 16) und durch Subtrahieren der Ergebnisse der beiden modularen Reduktionen, wie es durch Gleichung 17 veranschaulicht ist.

Im nachfolgenden wird auf Fig. 2 Bezug genommen, um ein bevorzugtes Verfahren darzustellen, das lediglich mit vier Registern auskommt, nämlich mit einem ersten Register für den Zähler A, mit einem zweiten Register für den Nenner N, mit einem dritten Register für die erste Hilfsgröße H1 und mit einem vierten Register H2 für die zweite Hilfsgröße. Optional kann ein fünftes Ergebnisregister verwendet werden, oder das Zählerregister, das Nennerregister oder das dritte Register für die erste Hilfsgröße können als Ergebnisregister eingesetzt werden, wenn es gewünscht ist.

In einem Schritt 20 wird zunächst der Wert e gemäß Gleichung 8 gewählt. Hierauf wird das Zählerregister mit dem ersten Produkt $A \cdot F$ geladen (Schritt 22). Anschließend wird das Nennerregister ebenfalls neu geladen, und zwar mit dem zweiten Produkt (24). In einem Schritt 26 wird dann eine modulare Reduktion gemäß Gleichung 16 berechnet. Dann, nach dem Berechnen im Schritt 26 wird der Nenner um 1 inkrementiert (Schritt 28), um in einem Schritt 30 die zentrale Reduktionsgleichung 15 zu berechnen. In einem Schritt 32 wird dann eine Subtraktion der beiden relevanten Gleichungen 15 und 16 durchgeführt, wie es durch Gleichung 17 dargestellt ist. Nach dem Berechnen der Differenz im Schritt 32 wird in einem Schritt 34 überprüft, ob das Resultat negativ ist. Ist dies der Fall, so wird der Modul hinzuaddiert (Schritt 36), um das Ergebnis Q der Division zu erhalten (Schritt 38).

Wird dagegen im Schritt 34 festgestellt, daß das durch den Schritt 32 erhaltene Resultat größer als 0 ist, so wird dieses Resultat unmittelbar als Resultat der Division ausgegeben (Schritt 38´).

Es sei darauf hingewiesen, daß das in Fig. 2 gezeigte Ausführungsbeispiel der vorliegenden Erfindung insbesondere dann vorteilhaft eingesetzt werden kann, wenn die Zahlen H und Q in dem binären Langzahlregister 300 von Fig. 3 überlappend sind, da dann die anhand von Fig. 3 beschriebene Vorgehens-

weise des Auslesens der untersten Bits des Registers 300 und des anschließenden Invertierens, um das Resultat Q zu erhalten, nicht zu korrekten Ergebnissen führt. Bei dem in Fig. 2 gezeigten Ausführungsbeispiel der vorliegenden Erfindung umfaßt die Einrichtung 16 zum Extrahieren des Resultats Q aus der Differenz $H \cdot 2^e - Q$ die Funktionalität der Schritte 26, 32, 34 und 36.

Wie es nachfolgend dargelegt wird, kann das erfindungsgemäße Konzept ohne erhöhten Aufwand auch dazu verwendet werden, um nicht nur das Ergebnis einer Division zu berechnen, sondern das ganzzahlige Vielfache der Division. Dies kann ohne weiteres dadurch erreicht werden, daß in dem Modul auf der rechten Seite von Gleichung 15 statt der Zahl "1" eine Ganzzahl $x > 1$ eingesetzt wird, wobei gleichzeitig auf der linken Seite von Gleichung 15 das Resultat Q ebenfalls mit der Ganzzahl x multipliziert wird, so daß sich die folgende Gleichung 19 ergibt:

$$H \cdot F - Q \cdot x = A \cdot F \bmod (N \cdot F + x) \qquad (19)$$

Wird eine Zahl x größer als 1 verwendet, so muß dies auch in Gleichung 6, bei der Wahl des Faktors F berücksichtigt werden, und zwar dahingehend, daß der Faktor im Vergleich zu $x = 1$ das x-fache betragen muß.

Bei der Betrachtung von Gleichung 19 zeigt sich, daß das Resultat $Q \cdot x$, das beispielsweise durch Registerauslesen erhalten werden kann, entweder unmittelbar verwendet werden kann, wenn ein nachfolgender Algorithmusschritt nicht das Resultat Q, sondern ein x-faches des Resultats Q benötigt.

Alternativ kann, wenn doch das Resultat Q benötigt wird, wenn jedoch die modulare Reduktion mit dem Modul $(N \cdot F + x)$ aus irgendeinem Grund günstiger ausgerechnet werden kann als für den Fall $x = 1$, dieses erreicht werden, daß Q wieder durch x dividiert wird. Insbesondere in dem Fall, bei dem x ein ganz-

zahliges Vielfaches von 2 ist und ein binäres System vorliegt, kann dies durch Registerverschieben nach rechts um eine entsprechende Anzahl von Stellen erreicht werden.

Wenn Gleichung 19 in Analogie zu Gleichung 16 und 17 ausgewertet wird, so wird ebenfalls das x-fache von Q erhalten.

Eine weitere Alternative zum Extrahieren von Q bzw. einem Vielfachen von Q aus Gleichung 19 besteht darin, zur Auswertung die folgende Gleichung 20 zu verwenden, wobei Gleichung 20 generell Gleichung 19 entspricht, wobei nun jedoch die ganze Zahl y unterschiedlich zu x zu wählen ist. Wenn nunmehr Gleichung 20 von Gleichung 19 subtrahiert wird, ergibt sich folgende Gleichung 21. Auf der linken Seite von Gleichung 21 ergibt sich nun nicht das Resultat Q, sondern ein ganzzahliges Vielfaches des Resultats Q, nämlich die Differenz aus y und x. Q kann aus Gleichung 21 wieder erhalten werden, indem eine Division durch (y - x) durchgeführt wird. Auf diese Division kann verzichtet werden, wenn y und x so gewählt sind, daß deren Differenz gleich 1 ist.

$$H \cdot F - Q \cdot y = A \cdot F \bmod (N \cdot F + y) \qquad (20)$$

$$Q \cdot (y-x) = A \cdot F \bmod (N \cdot F + x) - A \cdot F \bmod (N \cdot F + y) \qquad (21)$$

Es sei darauf hingewiesen, daß die Parameter x und y auch negativ sein können, und zwar in Analogie zu der Vorgehensweise, die in Verbindung mit den Gleichungen (13') bis (15') dargelegt worden ist.

Die vorliegende Erfindung ist somit aufgrund ihrer Flexibilität, Sicherheit und Leistungsfähigkeit insbesondere für kryptographische Algorithmen und für kryptographische Coprozessoren geeignet, auf denen typischerweise eine sichere und effiziente Implementation der modularen Reduktion schaltungsmäßig implementiert ist.

Bezugszeichenliste

10 Bestimmungsblock
12 Einrichtung zum Bereitstellen
14 Einrichtung zum modularen Reduzieren
16 Einrichtung zum Extrahieren
20 Bestimmen der Hilfszahl
22 Berechnen des ersten Produkts
24 Berechnen des zweiten Produkts
26 Berechnen einer ersten Hilfsgröße
28 Inkrementieren des Moduls
30 Berechnen der Hilfsgröße
32 Subtrahieren der Hilfsgröße von der weiteren Hilfsgröße
34 Überprüfen des Vorzeichens des Resultats
36 Hinzuaddieren eines Moduls
38 Ausgeben des Resultats
38´ Ausgeben des Resultats
300 Langzahlregister

Patentansprüche

1. Vorrichtung zum Berechnen eines Ergebnisses (Q) oder eines ganzzahligen Vielfachen des Ergebnisses (Q) einer Division eines Zählers (A) durch einen Nenner (N), mit folgenden Merkmalen:

einer Einrichtung (12) zum Bereitstellen eines Faktors, der so gewählt ist, daß ein Produkt aus dem Faktor und dem Nenner (N) größer als das Ergebnis (Q) ist;

einer Einrichtung (14) zum modularen Reduzieren eines ersten Produkts aus dem Zähler und dem Faktor unter Verwendung eines Moduls, der gleich einer Summe aus einem zweiten Produkt des Nenners und des Faktors und einer ganzen Zahl ist, um eine Hilfsgröße zu erhalten, die das Ergebnis aufweist; und

einer Einrichtung (16) zum Extrahieren des Ergebnisses oder des ganzzahligen Vielfachen des Ergebnisses aus der Hilfsgröße.

2. Vorrichtung nach Anspruch 1, bei der die Einrichtung (12) zum Bereitstellen ausgebildet ist, um den Faktor derart zu bestimmen, daß eine Basis potenziert mit einer Hilfszahl gleich dem Faktor ist.

3. Vorrichtung nach Anspruch 2, bei der die Basis 2 ist, so daß die Multiplikation mit dem Faktor einer Verschiebung um eine Anzahl von Stellen in einem Register entspricht, wobei die Anzahl von Stellen gleich der Hilfszahl ist.

4. Vorrichtung nach einem der vorhergehenden Ansprüche,

bei der eine Zweierkomplementdarstellung für eine Darstellung von negativen Zahlen verwendet wird, und

bei der die Hilfsgröße in einem Register (300) gespeichert ist, und bei der die Einrichtung (16) zum Extrahieren eine Einrichtung zum Auslesen eines unteren Abschnitts (-Q) des Registers (300), in dem das Ergebnis enthalten ist, und eine Einrichtung zum Invertieren eines ausgelesenen Werts und zum Hinzuaddieren einer Eins aufweist, um das Ergebnis (Q) der Division zu erhalten.

5. Vorrichtung nach einem der Patentansprüche 1 bis 3,

bei der die Einrichtung (16) zum Extrahieren folgende Merkmale aufweist:

eine Einrichtung zum Berechnen (26), als weiterer Hilfsgröße, eines Ergebnisses einer modularen Reduktion des Zählers multipliziert mit dem Faktor, wobei der Nenner multipliziert mit dem Faktor als Modul vorgesehen ist; und

einer Einrichtung (32) zum Subtrahieren der Hilfsgröße von der weiteren Hilfsgröße, um das Ergebnis der Division zu erhalten.

6. Vorrichtung nach einem der vorhergehenden Ansprüche, bei der die Division eine Ganzzahl-Division ist.

7. Vorrichtung nach Anspruch 3, bei der die Hilfszahl so ausgewählt ist, daß sie gleich der Anzahl von Stellen des Zählers weniger einem Doppelten einer Anzahl von Stellen des Nenners plus 2 ist.

8. Vorrichtung nach Anspruch 5, bei der die Einrichtung (16) zum Extrahieren angeordnet ist, um festzustellen (34), ob das Ergebnis negativ ist, und um in diesem Fall zu dem Ergebnis den Modul hinzu zu addieren, der in der Einrichtung (14) zum modularen Reduzieren zur Verwendung vorgesehen ist.

9. Vorrichtung nach Patentanspruch 5, die ferner folgende Merkmale aufweist:

ein erstes Register zum Speichern des Zählers (A);

ein zweites Register zum Speichern des Nenners (N);

ein drittes Register zum Speicher der weiteren Hilfsgröße (H2);

ein viertes Register zum Speichern der Hilfsgröße (H1); und

eine Registersteuerungseinheit zum Steuern der Einrichtung (14) zum Berechnen und der Einrichtung (16) zum Extrahieren, um das Resultat (Q) zu erhalten.

10. Vorrichtung nach Patentanspruch 1,

bei der das Ergebnis multipliziert mit einem ganzzahligen Multiplikator berechnet wird,

bei der die Einrichtung (12) zum Bereitstellen angeordnet ist, um einen Faktor bereitzustellen, der so gewählt ist, daß ein Produkt aus dem Faktor und dem Nenner und dem Ergebnis mulitpliziert mit dem ganzzahligen Mulitplikator größer als das Ergebnis der Division ist, und

bei dem die Einrichtung (16) zum modularen Reduzieren ausgebildet ist, um einen Modul zu verwenden, der gleich einer Summe aus einem Produkt des Nenners und des Faktors und aus dem ganzzahligen Multiplikator ist.

11. Vorrichtung nach Patentanspruch 1,

bei der die Einrichtung (14) zum modularen Reduzieren ausgebildet ist, um einen Modul zu verwenden, der gleich einer Summe aus einem Produkt des Nenners und des Faktors und einer

ganzen Zahl ist, wobei die ganze Zahl größer oder gleich 1 ist, und

bei der die Einrichtung (16) zum Extrahieren angeordnet ist, um eine modulare Reduktion unter Verwendung eines Moduls, der gleich einer Summe aus einem Produkt des Nenners und des Faktors und einer weiteren ganzen Zahl ist, wobei die weitere ganze Zahl ungleich der ganzen Zahl ist, so daß durch die Einrichtung (16) zum Extrahieren das Ergebnis der Division erhalten wird, wenn eine Differenz aus der weiteren ganzen Zahl und der ganzen Zahl gleich 1 ist, oder das Ergebnis multipliziert mit einem ganzzahligen Multiplikator erhalten wird, wobei der ganzzahlige Multiplikator gleich der Differenz aus der weiteren ganzen Zahl und der ganzen Zahl ist.

12. Vorrichtung nach einem der vorhergehenden Patentansprüche, die als Kryptocoprozessor einer kryptographischen Vorrichtung ausgebildet ist.

13. Vorrichtung nach einem der Patentansprüche 1 bis 3, bei der die ganze Zahl negativ ist, so daß das Ergebnis ohne Invertierung erhaltbar ist.

14. Vorrichtung nach Patentanspruch 11, 12 oder 13, bei der die weitere Zahl eine negative ganze Zahl ist.

15. Verfahren zum Berechnen eines Ergebnisses (Q) oder eines ganzzahligen Vielfachen des Ergebnisses (Q) einer Division eines Zählers (A) durch einen Nenner (N), mit folgenden Schritten:

Bereitstellen (12) eines Faktors, der so gewählt ist, daß ein Produkt aus dem Faktor und dem Nenner (N) größer als das Ergebnis (Q) ist;

modulares Reduzieren (14) eines ersten Produkts aus dem Zähler und dem Faktor unter Verwendung eines Moduls, der gleich

einer Summe aus einem zweiten Produkt des Nenners und des Faktors und einer ganzen Zahl ist, um eine Hilfsgröße zu erhalten, die das Ergebnis aufweist; und

Extrahieren (16) des Ergebnisses oder des ganzzahligen Vielfachen des Ergebnisses aus der Hilfsgröße.

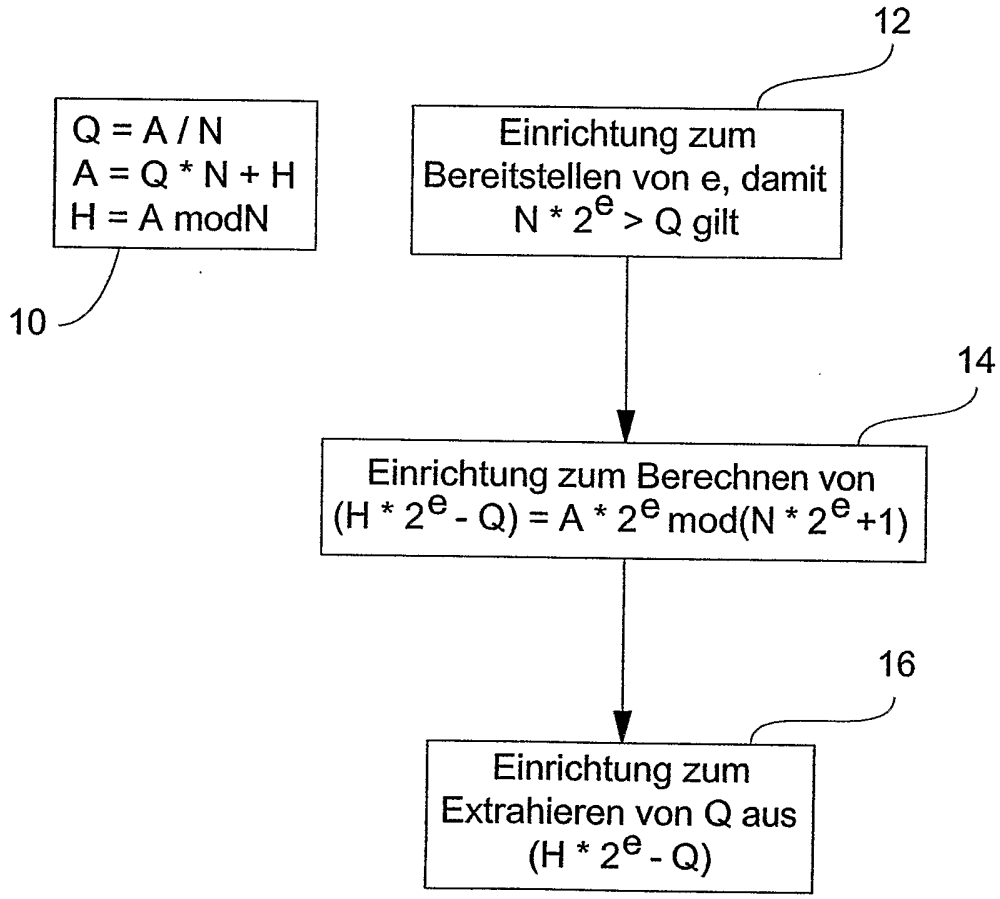

12
Q = A / N
A = Q * N + H
H = A modN
Einrichtung zum Bereitstellen von e, damit N * 2^e > Q gilt
10
14
Einrichtung zum Berechnen von (H * 2^e - Q) = A * 2^e mod(N * 2^e +1)
16
Einrichtung zum Extrahieren von Q aus (H * 2^e - Q)

FIG 1

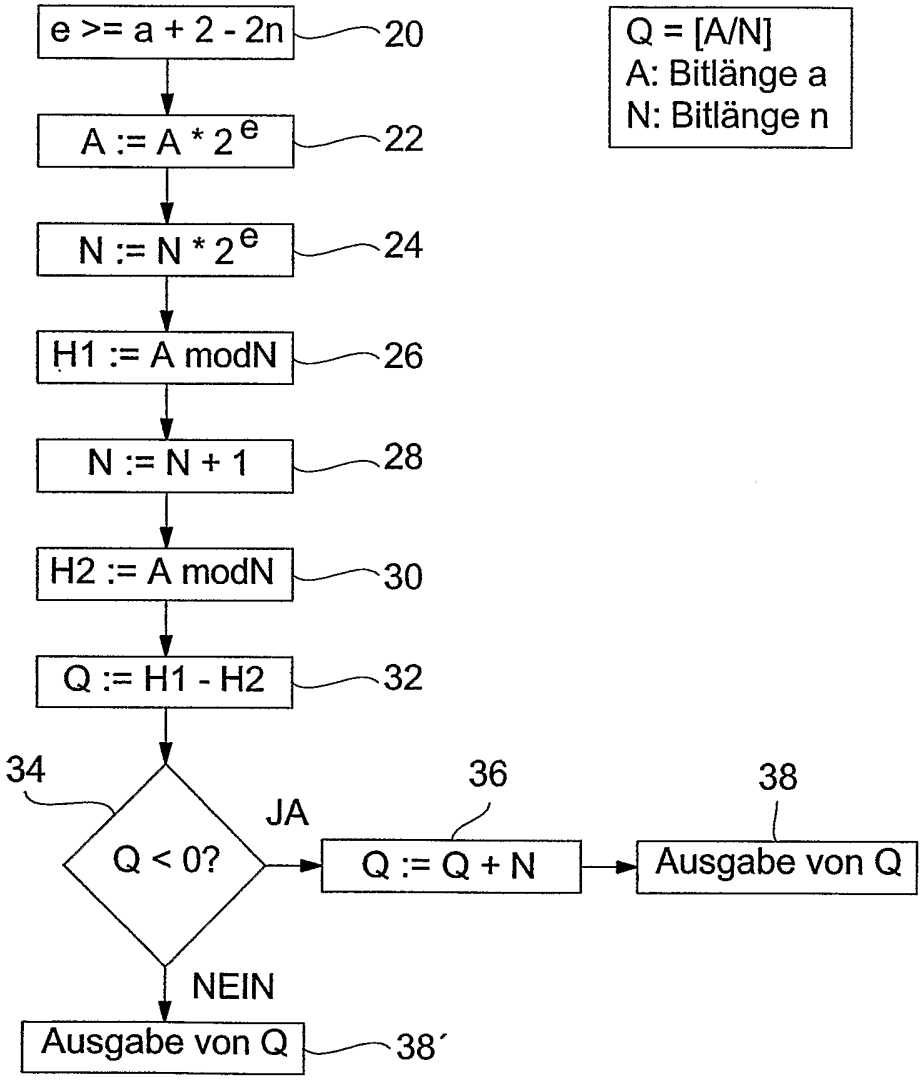

e >= a + 2 - 2n
20
A := A * 2^e
22
N := N * 2^e
24
H1 := A modN
26
N := N + 1
28
H2 := A modN
30
Q := H1 - H2
32
34
Q < 0?
JA
36
Q := Q + N
38
Ausgabe von Q
NEIN
Ausgabe von Q
38´
Q = [A/N]
A: Bitlänge a
N: Bitlänge n

FIG 2

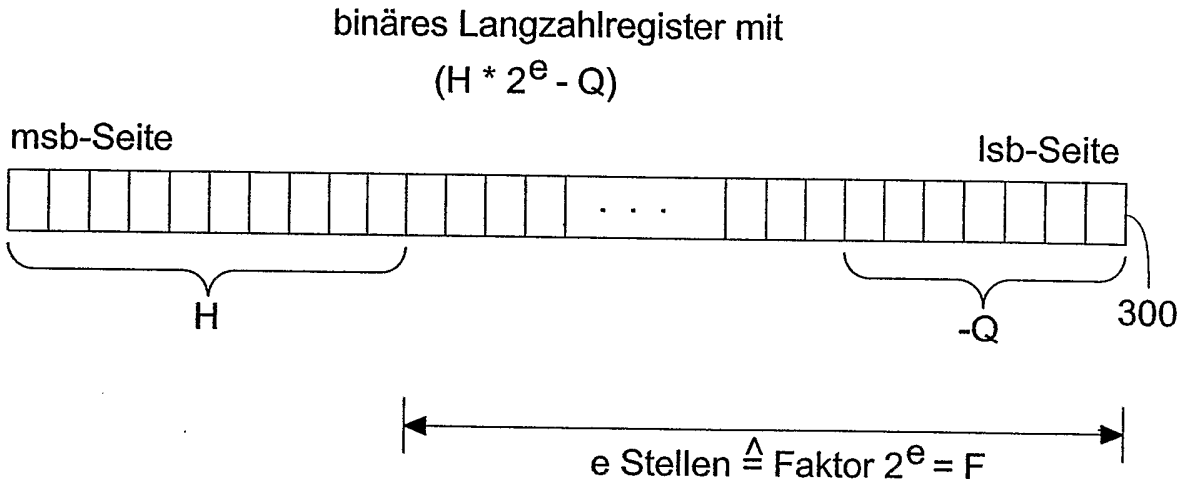

binäres Langzahlregister mit
(H * 2^e - Q)
msb-Seite
lsb-Seite
. . .
H
-Q
300
e Stellen ≙ Faktor 2^e = F

FIG 3