

(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
27. September 2007 (27.09.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/107592 A2

(51) Internationale Patentklassifikation:
Nicht klassifiziert

(21) Internationales Aktenzeichen: PCT/EP2007/052707

(22) Internationales Anmeldedatum:
21. März 2007 (21.03.2007)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2006 013 989.5 22. März 2006 (22.03.2006) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): IHP GMBH - INNOVATIONS FOR HIGH PERFORMANCE MICROELECTRONICS / INSTITUT FÜR INNOVATIVE MIKROELEKTRONIK [DE/DE]; Im Technologiepark 25, 15236 Frankfurt (Oder) (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): LANGENDÖRFER, Peter [DE/DE]; Kiliansberg 3, 15230 Frankfurt (Oder) (DE). PETER, Steffen [DE/DE]; Pfäulmenallee 50, 15234 Frankfurt (Oder) (DE).

(74) Anwalt: EISENFÜHR, SPEISER & PARTNER; Anna-Louisa-Karsch-Strasse 2, 10178 Berlin (DE).

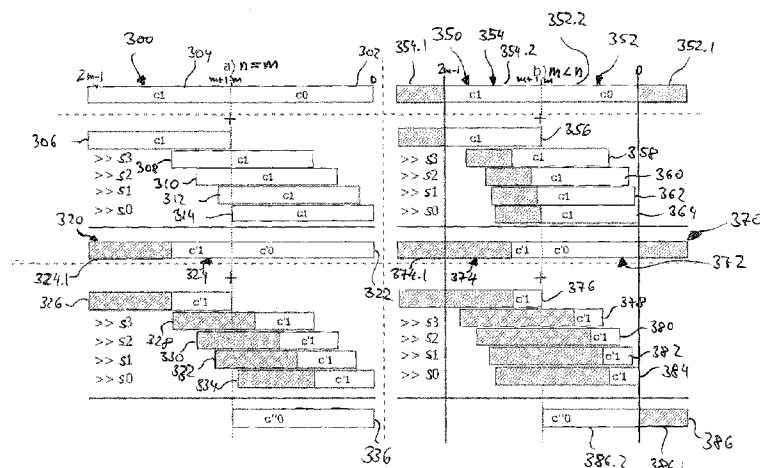
(81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR REDUCING A POLYNOMIAL IN A BINARY FINITE FIELD, IN PARTICULAR FOR A CRYPTOGRAPHIC APPLICATION

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR REDUKTION EINES POLYNOMS IN EINEM BINÄREN FINITEN FELD, INSBESONDERE IM RAHMEN EINER KRYPTOGRAPHISCHEN ANWENDUNG



(57) Abstract: The invention relates to a fast, chip space-saving method for reducing a first data word that corresponds to a polynomial $C(x)$ and has a maximum length $2n-1$, to a second data word with a maximum length m , said second data word corresponding to a polynomial $C''(x)$ that is equivalent to $C(x)$ in a binary finite field $GF(2^m)$, whose elements have a maximum length m , where m is either less than or equal to n . According to said method, the first data word is sub-divided into a binary first sub-data word C_0 and a binary second sub-data word C_1 , C_1 is subjected to an iterative right-shift to form terms of the sum until a respective term of the sum is assigned to each non-disappearing term of a reduction trinomial or pentanomial, which does not equal the term x^m , the terms of the sum formed for the first sub-data word are added together to form a total data word and the method steps are then repeated from the sub-division step to the creation of the total data word, until the total data word that has been determined has a maximum length m , thus forming the desired second data word.

[Fortsetzung auf der nächsten Seite]

WO 2007/107592 A2



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

Erklärung gemäß Regel 4.17:

— *Erfindererklärung (Regel 4.17 Ziffer iv)*

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: Ein schnelles und Chipfläche sparendes Verfahren zur Reduktion eines Polynom $C(x)$ entsprechenden ersten Datenwortes mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C^0(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, beinhaltet ein Partitionieren des ersten Datenwortes in ein binäres erstes Sub-Datenwort $C0$ und ein binäres zweites Sub-Datenwort $C1$, eine wiederholte Rechtsverschiebung von $C1$ zur Bildung von Summandentermen, bis jedem nicht verschwindenden Term eines Reduktionstrinomials oder -pentanomials, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist, ein Addieren der gebildeten Summandenterme zum ersten Sub-Datenwort zur Bildung eines Summandendatenwortes, und eine erneute Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens auf das gebildete Summandendatenwort, bis das ermittelte Summandendatenwort eine Länge von maximal m hat und somit das gesuchte zweite Datenwort bildet.

Verfahren und Vorrichtung zur Reduktion eines Polynoms in einem binären
finiten Feld, insbesondere im Rahmen einer kryptographischen Anwendung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Reduktion eines
einem Polynom $C(x)$ entsprechenden binären ersten Datenworts mit einer Länge
von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das
in einem binären finiten Feld, dessen Elemente eine maximale Länge m haben,
5 einem zu $C(x)$ äquivalenten Polynom $C^0(x)$ entspricht, wobei m entweder kleiner
oder gleich n ist. Weiterhin betrifft die Erfindung ein Kryptographieverfahren und
eine Kryptographievorrichtung.

Kryptographische Verfahren dienen dem Schutz von Daten vor unberechtigtem
10 Zugriff. Kryptographische Verfahren transformieren die zu schützenden Daten,
insbesondere unter Einbeziehung geheimer Schlüssel, in verschlüsselte Daten.
Kryptographische Verfahren dienen auch der Entschlüsselung der verschlüssel-
ten Daten unter Einbeziehung des geheimen Schlüssels zur Wiederherstellung
der zu schützenden Daten.

Asymmetrische Verschlüsselungsverfahren wie RSA und die elliptische Kurvenkryptographie (Elliptic Curve Cryptography, ECC) werden verwendet, um einen sicheren Austausch von Schlüsseln für kryptographische Verfahren zu gewährleisten und um digitale Signaturen zu berechnen.

5

Die elliptische Kurvenkryptographie erfordert eine deutlich kürzere Schlüssellänge als RSA bei gleicher Sicherheitsstufe. Darüber hinaus kann man für die elliptische Kurvenkryptographie binäre endliche (finite) Galois-Felder $GF(2^m)$ nutzen, welche auf Grund ihrer algebraischen Eigenschaften sehr gut für Hardwareimplementierungen geeignet sind. Hierbei gibt m die Länge der Elemente eines jeweiligen Galois-Feldes an.

10

Die wichtigste Operation bei der Anwendung der elliptischen Kurvenkryptographie ist die Multiplikation großer Polynome. Nach einer Polynom-Multiplikation in einem finiten Feld sind die möglichen resultierenden Produkte bekanntlich länger als das größte Element des zu Grunde liegenden endlichen Feldes. Deshalb muss nach einer Polynom-Multiplikation eine so genannte Reduktion ausgeführt werden. In dieser Reduktion wird das lange Polynom des resultierenden Produktes auf einen („äquivalenten“) Wert in den Grenzen des Feldes umgerechnet. Diese Operation ist nach jeder Polynom-Multiplikation notwendig.

15

20

Da die Multiplikation in der elliptischen Kurvenkryptographie eine Hauptoperation darstellt, ist entsprechend nicht nur die Multiplikationsoperation allein kritisch für die Leistungsfähigkeit (Performance) im Sinne von Schnelligkeit einer ECC-Implementierung, sondern auch die Reduktionsoperation.

25

Die Reduktion entspricht der Division mit Rest (Modulo-Operation) in „normalen“ endlichen Feldern. Diese soll anhand eines einfachen Beispiels erläutert werden. Das finite Feld $GF(7)$ besteht aus den Elementen $\{0,1,2,3,4,5,6\}$. Eine Multiplikation von $5 \cdot 4$ ergibt 20, was größer als das größte mögliche Element in dem Feld ist. In dem Fall wird 20 durch 7 dividiert und der Rest dieser Division, nämlich 6, ist dann auch das Ergebnis der Multiplikation von $5 \cdot 4$ innerhalb des finiten Feldes ($GF(7)$).

30

Binäre finite Felder ($GF(2^m)$) enthalten keine Zahlen, sondern Polynome. Ein Element dieser Felder ist $A(x) = a_{m-1} \cdot x^{m-1} + a_{m-2} \cdot x^{m-2} + \dots + a_1 \cdot x + a_0$. Die Koeffizienten a_i sind dabei entweder 0 oder 1. Eine wichtige Eigenschaft der Felder ist, dass bei der Addition und Subtraktion von Koeffizienten die XOR-Operation angewendet wird. Entsprechend ist $1+1 \equiv 1-1 \equiv 1 \text{ XOR } 1 = 0$.

Die maximale Länge eines Elementes des Feldes $GF(2^m)$ ist m . Die Multiplikation zweier Elemente ($A(x) \cdot B(x)$) ergibt ein doppelt so langes Polynom $C(x) = A(x) \cdot B(x) = c_{m-2} \cdot x^{2m-2} + \dots + c_0$. Das Ergebnis hat also eine Länge von $2m-1$.

Man kann nun $C(x)$ zerlegen in $C(x) = C_1(x) \cdot x^m + C_0(x)$. $C_0(x)$ hat dabei die Länge, die der maximalen Länge der Polynome des Feldes entspricht. $C_1(x)$ ist der über die maximale Feldlänge überstehende Teil, der mittels des Reduktionsprozesses in C_0 integriert werden muss.

Diese Reduktion kann man mittels einer kompletten Polynomdivision lösen, was sehr lange dauert. Ein solches Verfahren entspricht genau der oben am Beispiel in $GF(7)$ erläuterten Modulo-Division.

Es sind alternative, schnellere Möglichkeiten bekannt, diese Reduktion auszuführen. Ein oft genutzter Ansatz ist die multiplikative Reduktion. Multipliziert man $C_1(x)$ mit einem Reduktionspolynom $R(x)$ und subtrahiert das entstehende Produkt von $C(x)$, ist das Ergebnis kleiner als das Ausgangspolynom, aber in dem zu Grunde liegendem Feld äquivalent. Es gilt: $C(x) \equiv C(x) - C_1(x) \cdot R(x)$. Wiederholt man diese Operation, kommt man auf immer weitere kleinere, aber im zu Grunde liegenden Feld äquivalente Werte. Wenn $C_1(x)$ die Länge Null erreicht hat, ist die Reduktion abgeschlossen.

Sind die Länge des Feldes und das Reduktionspolynom $R(x)$ bekannt, kann man sehr effizient eine direkte Verdrahtung der Reduktionslogik realisieren. Dies ist zum Beispiel bekannt aus der Veröffentlichung Saqib, N. A., Rodriguez-Henriquez, F., and Diaz-Perez, A., „A parallel architecture for fast computation of

elliptic curve scalar multiplication over $GF(2^m)$ “, 18th International Parallel & Distributed Processing Symposium (IPDPS), Santa Fe, New Mexico, 26-30 Apr 2004.

- 5 Der Nachteil des aus dieser Veröffentlichung bekannten Systems ist jedoch gerade, dass es die Kenntnis der Länge des Feldes und des Reduktionspolynoms $R(x)$ voraussetzt. Es wird daher angestrebt, einen ähnlich effizienten Weg zu finden, der diese Operationen für zur Laufzeit variable Felder mit variablen Reduktionspolynomen in Hardware möglich macht.

10

- Eine aus dem Dokument Eberle, H., Gura, N., and Chang-Shantz, S., “A cryptographic processor for arbitrary elliptic curves over $GF(2^m)$ “, IEEE 14th International Conference on Application-specific Systems, Architectures and Processors (ASAP), June 24-26, 2003, Seiten 444–454 schon bekannte Möglichkeit ist es,
 15 einen kompletten Multiplizierer für den Reduktionsschritt $C(x)-C1(x)*R(x)$ zu nutzen. Eine zusätzliche komplette Multiplikation an dieser Stelle ist für die Schnelligkeit der ECC-Implementierung jedoch sehr negativ.

- Aus der US2003/0208515 A1 (dort Fig. 32) ist es bekannt, bei der multiplikativen
 20 Reduktion zentrierter ausgerichteter Polynome einen Berechnungsschritt $C'(x)=C1(x)*(M-x^m)+x^{n-m}+C0(x)$ durchzuführen, bis der überstehende Teil des resultierenden Polynoms verschwindet. Hierbei kennzeichnet M ein geeignetes irreduzibles Polynom. Das Verfahren beinhaltet, das Reduktionspolynom ohne den Term x^m um $n-m$ Positionen nach links verschoben abzuspeichern und die
 25 Randpositionen links und rechts mit dem Wert Null aufzufüllen. Für eine 233-Bit-Implementierung ($m=233$) mit $M=x^{233}+x^{74}+1$ auf einer 256-Bit-Hardware ($n=256$), ist $(M-x^m)*x^{n-m}=(x^{74}+1)*x^{256-233}=x^{97}+x^{23}$. Dieses für den gesamten Reduktionsprozess wiederverwendbare Polynom wird mit dem überstehenden Teil $C1(x)$ multipliziert und zu $C0(x)$ addiert (XOR), bis $C1(x)$ Null ist. Es sind daher wiederholte
 30 komplette Polynommultiplikationen notwendig. Abschließend wird das so berechnete äquivalente, reduzierte Polynom durch eine Multiplikation mit x^m nach links verschoben.

Eine in der US2003/0208515 A1 beschriebene Variante (Fig. 33) sieht vor, statt des ursprünglichen Polynoms ein teilweise reduziertes Polynom für die Berechnung von Punktmultiplikationsoperationen zu verwenden, um erst danach abschließend die Reduktion entsprechend dem eben beschriebenen Verfahren vorzunehmen. Auf diese Weise können mit einer Implementierung Operationen in Feldern $GF(2^m)$ mit unterschiedlichen Werten m vorgenommen werden.

Nachteil der in diesem Dokument beschriebenen Verfahren ist jedoch, dass wiederholte vollständige Polynom-Multiplikationen zur Reduktion durchgeführt werden müssen. Für die Reduktion wird eine Vielzahl von Taktzyklen benötigt.

Das der vorliegenden Erfindung zugrunde liegende technische Problem ist es daher, ein Verfahren und eine Vorrichtung zur Reduktion eines Polynomproduktes anzugeben, das eine in besonders wenigen Taktzyklen durchführbare Reduktion in Feldern unterschiedlicher Länge und mit unterschiedlichen Reduktionspolynomen ermöglicht.

Die Erfindung spiegelt sich in drei Aspekten wieder, wovon zwei Aspekte Verfahren betreffen und ein dritter Aspekt eine Vorrichtung.

Gemäß einem ersten Aspekt der Erfindung wird ein Verfahren zur Reduktion eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m bereitgestellt. Das zweite Datenwort entspricht in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C^0(x)$, wobei m entweder kleiner oder gleich n ist. Das Verfahren weist die folgenden Schritten auf:

- Bereitstellen eines Reduktionspolynoms $R(x)$, das ein Trinomial oder ein Pentanomial bildet;
- Partitionieren des ersten Datenworts in ein binäres erstes Sub-Datenwort C_0 und ein binäres zweites Sub-Datenwort C_1 , deren entsprechende Poly-

nome $C_0(x)$ und $C_1(x)$ die Gleichung $C(x) = C_1(x) * x^m + C_0(x)$ erfüllen, und Abgreifen des zweiten Sub-Datenwortes zur Bildung eines ersten Summandenterms;

- 5 - Rechtsverschieben des zweiten Sub-Datenworts zur Bildung eines zweiten Summandenterms, und Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme, bis jedem nicht verschwindenden Term des Reduktionspolynoms, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist, indem die Schrittweite einer jeweiligen Rechtsverschiebung gleich der Differenz von m und der Ordnung eines jeweiligen
- 10 nicht verschwindenden Terms des Reduktionspolynoms ist;
- Addieren der gebildeten Summandenterme zum ersten Sub-Datenwort zur Bildung eines Summendatenwortes;
- 15 - wenn das so ermittelte Summendatenwort eine Länge größer als m hat, Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens auf das gebildete Summandendatenwort, bis das so ermittelte Summendatenwort eine Länge von maximal m hat und somit das zweite Datenwort bildet.

20 Das erfindungsgemäße Verfahren zur Reduktion eines ersten Datenwortes ermöglicht in einer Hardwareimplementierung eine besonders schnelle Durchführung in wenigen Taktzyklen. In einem bevorzugten Ausführungsbeispiel, das weiter unten beschrieben wird, gelingt die Reduktion sogar in nur einem Taktzyklus.

25 lus.

Das erfindungsgemäße Verfahren beinhaltet verschiedene Maßnahmen, die zu dieser Beschleunigung der Reduktionsoperation gegenüber bekannten Verfahren führen.

30 Zunächst wird erfindungsgemäß ein Reduktionspolynom $R(x)$ bereitgestellt, das ein Trinomial oder ein Pentanomial bildet. Trinomiale sind Polynome mit drei besetzten Termen. Pentanomiale sind Polynome mit fünf besetzten Termen. Mit

dieser Maßnahme macht sich das erfindungsgemäße Verfahren die Eigenschaften derjenigen binären finiten Felder zunutze, die in der elliptischen Kurvenkryptographie in der Praxis zum Einsatz kommen, weil sie von Standardisierungsgremien wie beispielsweise dem amerikanischen National Institut of Standards and Technology (NIST) empfohlen werden.

Da zusätzlich die zweithöchste besetzte Stelle der empfohlenen Reduktionspolynomen in aller Regel kleiner als $m/2$ ist, kann eine komplette Reduktion nach zwei aufeinanderfolgenden Multiplikationen vollendet werden.

10

Weiterhin werden bei dem erfindungsgemäßen Verfahren Multiplikationsschritte durch flexible Verschiebeoperationen realisiert. Dies führt zu einer wesentlichen Vereinfachung der erforderlichen Multiplikationsschritte und gleichzeitig zu einer flexiblen Hardwareimplementierung, die es erlaubt, Produkte von Datenworten mit unterschiedlicher (in einem jeweiligen Produkt jedoch gleicher) Länge zu reduzieren.

20

Mathematisch kann das erfindungsgemäße Reduktionsverfahren wie folgt beschrieben werden. Ausgehend von einem Polynom der Form

$$C(x) = C1(x) * x^m + C0(x) \quad (1)$$

Wird in einer ersten Iteration der Reduktionsoperation die folgende Differenz berechnet :

25

$$C'(x) = C(x) - C1(x) * R(x) \quad (2)$$

Nachfolgend wird erläutert, wie diese Differenz erfindungsgemäß besonders einfach berechnet wird. Gleichung (2) lässt sich auch darstellen als

30

$$C'(x) = C1(x) * x^m + C0(x) - (C1(x) * x^m + C1(x) * x^m/x^{S3} + C1(x) * x^m/x^{S2} + C1(x) * x^m/x^{S1} + C1(x) * x^m/x^{S0}) \quad (3)$$

Gleichung (3) ist äquivalent mit

$$C'(x) = C_0(x) - (C_1(x) * x^m/x^{s_3} + C_1(x) * x^m/x^{s_2} + C_1(x) * x^m/x^{s_1} + C_1(x) * x^m/x^{s_0}) \quad (4)$$

- 5 Hierbei entsprechen die Divisionen durch die Terme x^{s_3} , x^{s_2} , x^{s_1} , x^{s_0} Rechtsverschiebeoperationen um eine Schrittweite, die der Ordnung der nicht verschwindenden Terme x^{s_3} , x^{s_2} , x^{s_1} und x^{s_0} des Reduktionspolynoms entspricht.

10 In zahlreichen Fällen ist nach dieser erstmaligen Anwendung des Reduktionspolynoms noch keine vollständige Reduktion erzielt. Es erfolgt daher ein nächster Iterationsschritt der auf einer Darstellung des Zwischenergebnisses $C'(x)$ in der Form:

$$C'(x) = C_1'(x) * x^m + C_0'(x) \quad (5)$$

15 basiert. Die maximale Länge des Zwischenergebnisses $C_1'(x)$ ist $m - s_3 - 1$. Die erneute Anwendung des Reduktionspolynoms erfolgt gemäß der Gleichung

$$C''(x) = C'(x) - C_1'(x) * R(x) = C_1''(x) * x^m + C_0''(x) \quad (6)$$

20 Dabei ist, falls $m < 2 * s_3$, die Ordnung des Terms $C_1''(x)$ Null. Die Reduktion benötigt daher in diesem Fall nur zwei Iterationen.

25 Der im erfindungsgemäßen Verfahren enthaltene Schritt des Partitionierens des ersten Datenworts beinhaltet nicht notwendiger Weise eine physikalische Aufspaltung des ersten Datenworts in zwei getrennte Sub-Datenworte oder gar ihre getrennte Abspeicherung in Speichern oder Registern. Wesentlich für das Partitionieren ist allein, dass im weiteren Verlauf des Verfahrens die Sub-Datenworte getrennt verwendet werden. Hierzu kann in einer vorteilhaften Hardware-Implementierung jedoch schon das getrennte Verdrahten der Bitpositionen der
30 Sub-Datenworte in einem Register, welches das vollständige erste Datenwort enthält, mit jeweils nachgeschalteten Operator-Implementierungen genügen.

Unter der Länge eines gebildeten Summandendatenwortes ist die höchstwertige Position zu verstehen, deren Wert ungleich Null ist. Wenn also ein Summanden-Datenwort eine Länge von größer als m hat, bedeutet, dass auf Positionen $> m$ Werte ungleich Null vorhanden sind.

5

Der im erfindungsgemäßen Verfahren enthaltene Schritt des Rechtsverschiebens des zweiten Sub-Datenworts zur Bildung eines zweiten Summandenterms, und die Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme, ist so zu verstehen, dass der zweite Summandenterm im Ergebnis gegenüber dem zweiten Sub-Datenwort (C1) in seiner ursprünglichen Position im ersten Datenwort ($C0 + C1$) nach rechts verschoben verwendet wird. Dies kann nicht nur durch eine tatsächliche Rechtsverschiebung, sondern beispielsweise auch auf dem Wege erreicht werden, dass das zweite Sub-Datenwort zunächst rechtsbündig abgegriffen und dann um eine jeweils entsprechend anzupassende Schrittweite nach links verschoben wird. Offensichtlich ist das Ergebnis jedoch dasselbe.

Gemäß einem zweiten Aspekt der vorliegenden Erfindung wird ein Verfahren zur Reduktion eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m bereitgestellt, das in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C^0(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, mit den Schritten:

- 25 - Bereitstellen eines Reduktionspolynoms $R(x)$, das ein Trinomial oder ein Pentanomial bildet;
- Partitionieren des ersten Datenworts in ein binäres erstes Sub-Datenwort $C0$ und ein binäres zweites Sub-Datenwort $C1$, deren entsprechende Polynome $C0(x)$ und $C1(x)$ die Gleichung $C(x) = C1(x) * x^m + C0(x)$ erfüllen, und Abgreifen des zweiten Sub-Datenwortes zur Bildung eines ersten Summandenterms;

30

- Rechtsverschieben des zweiten Sub-Datenworts zur Bildung eines zweiten Summandenterms, und Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme, bis jedem nicht verschwindenden Term des Reduktionspolynoms, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist, indem die Schrittweite einer jeweiligen Rechtsverschiebung gleich der Differenz von m und der Ordnung eines jeweiligen nicht verschwindenden Terms des Reduktionspolynoms ist;
 - Addieren der gebildeten Summandenterme, mit Ausnahme des ersten Summandenterms, zum ersten Datenwort (, nachfolgend auch als erster Addierschritt bezeichnet);
 - wenn das so ermittelte Summendatenwort eine Länge größer als m hat, Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens auf das gebildete Summandendatenwort, bis das so ermittelte Summendatenwort eine Länge von maximal m hat;
 - Addieren des ersten Summandenterms und, im genannten Falle einer Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens auf das gebildete Summandendatenwort, jedes weiteren zwischenzeitlich ermittelten zweiten Sub-Datenworts zum zuletzt ermittelten Summendatenwort zur Bildung des zweiten Datenworts (, nachfolgend auch als zweiter Addierschritt bezeichnet).
- Das Verfahren des zweiten Aspekts der Erfindung unterscheidet sich von dem des ersten Aspekts der Erfindung darin, dass die jeweiligen ersten Summandenterme, d. h. die jeweiligen zweiten Sub-Datenworte, erst abschließend, nach Durchführung aller erforderlichen Iterationen zur Reduktion zum zuletzt ermittelten Summendatenwort addiert werden, um das vollständig reduzierte zweite Datenwort zu bilden.

Der zusätzliche Vorteil des Verfahrens des zweiten Aspekts der Erfindung liegt darin, dass auf diese Weise noch kompaktere Hardware-Implementierungen

möglich werden. Denn in einer erfindungsgemäßen Reduktionsvorrichtung muss eine darin vorgesehene Schiebereinheit zur Durchführung dieses Verfahrens nur noch maximal drei Rechtsschiebe-Operationen durchführen. Dies spart Chipfläche.

5

Die Verfahrensführung dieses Aspekts der Erfindung beruht auf der Einsicht, dass alle irreduziblen Polynome die Struktur:

$$R(x) = x^m + \dots + 1 \quad (7)$$

10

haben. Die Terme x^m und 1 sind daher Teil jedes Reduktionspolynoms $R(x)$. Da die niedrigste Ordnung des Reduktionspolynoms immer Null ($x^0 = 1$) ist, und s_0 der Differenz von m und Null entspricht, ist s_0 immer äquivalent zu m . Daher wird für diesen Term tatsächlich keine Rechtsverschiebung benötigt und kann die erforderliche Addition im Anschluss an die Iterationen erfolgen.

15

Weitere Vorteile dieses Verfahrens ergeben sich aus der nachfolgenden Beschreibung von Ausführungsbeispielen, die sich jedoch ebenso auf das Verfahren gemäß dem ersten Aspekt der Erfindung beziehen. Die Ausführungsbeispiele sind miteinander kombinierbar, soweit nicht ausdrücklich beschrieben ist, dass es sich um zueinander alternative Ausführungsbeispiele handelt.

20

Gemäß einem bevorzugten Ausführungsbeispiel der erfindungsgemäßen Verfahren, bei dem das erste Datenwort eine Länge von weniger als $2n-1$ hat, erfolgt vor der Rechtsschiebeoperation ein zusätzlicher erster Justierschritt. Der erste Justierschritt beinhaltet ein Linksverschieben des ersten Datenworts um eine Auffüllschrittweite und ein beiderseitiges Anfügen einer der Auffüllschrittweite entsprechenden Anzahl Nullen an das erste Datenwort. Die Linksverschiebung und das Anfügen der Nullen erfolgt derart, dass die Länge des so modifizierten ersten Datenworts $2n-1$ beträgt und dass im modifizierten ersten Datenwort diejenigen Terme des dem ersten Datenwort entsprechenden Polynoms $C(x)$, die eine Ordnung größer als m haben, an denselben Bitpositionen angeordnet sind wie wenn das erste Datenwort schon anfänglich die Länge $2n-1$ gehabt hätte.

25
30

Auf diese Weise ist es möglich, auch kleinere Datenworte in ein und derselben Hardware-Implementierung zu reduzieren. Damit wird die Flexibilität einer Hardware-Implementierung erhöht.

5

Vorzugsweise wird bei dieser Verfahrensführung ein zweiter Justierschritt durchgeführt, der beim Verfahren gemäß dem ersten Aspekt der Erfindung insbesondere nach dem Addieren der gebildeten Summandenterme zum ersten Sub-Datenwort zur Bildung des Summanden-Datenwortes im letzten Iterationsschritt
10 durchgeführt wird. Beim Verfahren gemäß dem zweiten Aspekt der Erfindung wird der zweite Justierschritt insbesondere vordem zweiten Addierschritt durchgeführt.

Bei einer besonders bevorzugten Ausführungsform der erfindungsgemäßen
15 Verfahren wird das irreduzible Polynom allein durch die Potenzen der nicht verschwindenden Terme des Reduktionspolynoms, die nicht der Term x^m sind, repräsentiert. Das bedeutet, dass das Reduktionspolynom nicht in der vollen Länge eines Datenwortes gespeichert wird, sondern nur in der Form (s_1, s_2, s_3) . Die Verfahrensführung wird dadurch weiter vereinfacht und beschleunigt. Der
20 zusätzliche Parameter der bekannten maximalen Länge m von Datenworten des binären finiten Feldes, der zu einer eindeutigen Kenntnis des irreduziblen Polynoms benötigt wird, kann, muss jedoch nicht zusammen mit den Parametern (s_1, s_2, s_3) abgespeichert werden, da er auch anderweitig vorhanden ist.

25 Ein dritter Aspekt der vorliegenden Erfindung betrifft ein asymmetrisches Kryptographieverfahren zur Verwendung in einer elektronischen Kryptographievorrichtung. Das Verfahren umfasst ein Reduzieren eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld
30 $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C'(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, gemäß einem Verfahren nach dem ersten oder zweiten Aspekt der Erfindung,

oder nach einer der im Rahmen dieser Anmeldung beschriebenen Ausführungsformen der Verfahren nach dem ersten oder zweiten Aspekt der Erfindung.

Als Kryptographieverfahren wird hier ein Verfahren zur Verschlüsselung oder
5 Entschlüsselung einer in Form von insbesondere in Form eines Datenworts dargestellten Nachricht verstanden. Als Nachricht wird zum Beispiel auch ein Teilstück eines Stroms von Daten verstanden, das die Form eines Datenworts annimmt.

10 Eine Ausführungsform des Kryptographieverfahrens des dritten Aspekts der Erfindung bildet ein elliptisches Kurvenkryptographieverfahren, umfassend, vor dem Reduzieren das Multiplizieren zweier, Faktor-Polynomen $A(x)$ und $B(x)$ entsprechenden Faktor-Datenworte zu dem einem Polynom $C(x)$ entsprechenden ersten Datenwort mit einer Länge von maximal $2n-1$.

15 Ein weiterer, vierter Aspekt der Erfindung betrifft ein Verfahren zur Berechnung einer digitalen Signatur. Das Verfahren umfasst ein elliptisches Kryptographieverfahren mit einem Reduzierverfahren nach dem ersten oder zweiten Aspekt der Erfindung oder nach einer der im Rahmen dieser Anmeldung beschriebenen
20 Ausführungsformen der Verfahren nach dem ersten oder zweiten Aspekt der Erfindung.

Ein fünfter Aspekt der Erfindung betrifft eine Vorrichtung zur Reduktion eines
25 einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C'(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, mit:

30 - einem Speicher, der eine Repräsentation mindestens eines Reduktionspolynoms $R(x)$ enthält, das ein Trinomial oder ein Pentanomial bildet;

- einer Selektionseinheit, die ausgebildet ist, ein binäres Sub-Datenwort aus dem ersten Datenwort zu abzugreifen, dessen entsprechendes Polynom $C_1(x)$ die Gleichung $C(x) = C_1(x) * x^m + C_0(x)$ erfüllt und das einen ersten Summandenterm bildet;
- 5 - einer Schiebeeinheit, die mit der Selektionseinheit verbunden und ausgebildet ist, das Sub-Datenwort zur Bildung eines zweiten oder weiterer Summandenterme um eine jeweils vorbestimmte Schrittweite nach rechts zu verschieben und die gebildeten Summandenterme auszugeben;
- 10 - einer Addiereinheit, die mit der Schiebeeinheit verbunden und ausgebildet ist, einen jeweiligen Summandenterm sowie die von der Schiebeeinheit ausgegebenen Summanden zum ersten Datenwort zu addieren; und
- 15 - einer Steuereinheit, die ausgebildet ist,
 - die Schrittweite einer jeweiligen, von der Schiebeeinheit auszuführenden Rechtsverschiebung zur Bildung eines Summandenterms als Differenz von m und der Ordnung eines jeweiligen nicht verschwindenden Terms des Reduktionspolynoms zu bestimmen,
 - 20 - die Schiebeeinheit zur wiederholten Durchführung des Rechtsverschiebungsschritts für eine Bildung weiterer Summandenterme mit jeweils neu bestimmter Schrittweite zu instruieren, bis jedem nicht verschwindenden Term eines jeweils vorgegebenen Reduktionspolynoms, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist,
 - 25 - die Berechnungseinheit, die Schiebeeinheit und die Addiereinheit erforderlichenfalls erneut zu aktivieren, bis ein ermitteltes Summandatenwort eine Länge von maximal m hat und somit das zweite Datenwort bildet.
 - 30

Die erfindungsgemäße Reduktionsvorrichtung, die gleichbedeutend auch als Reduzierungsvorrichtung bezeichnet wird, ermöglicht eine schnelle Reduktion von Datenwörtern. Sie bietet die Voraussetzung für eine hohe Flexibilität, die in bevorzugten Ausführungsbeispielen die Reduktion von Datenwörtern unterschiedlicher Länge ermöglicht.

Gegenüber bekannten Vorrichtungen gelingt dies mit einer besonders einfachen Struktur, die ohne jegliche dezidierte Multiplikationseinheit auskommt. Durch entsprechende Steuerung der flexiblen Schiebeeinheit, die ein selektiertes Sub-Datenwort um eine jeweils vorbestimmte Schrittweite nach rechts verschiebt, kann in Zusammenarbeit mit einer Addiereinheit eine multiplikative Reduktion durch nur wenige einfache Schiebe- und Addieroperationen ausgeführt werden. Die Tatsache, dass die Steuereinheit ausgebildet ist, die Berechnungseinheit, die Schiebeeinheit und die Addiereinheit erforderlichenfalls erneut zu aktivieren, bis ein ermitteltes Summendatenwort eine Länge von maximal m hat und somit das zweite Datenwort bildet, ist nicht notwendigerweise mit einem Prüfschritt verbunden, in dem die Länge eines teilreduzierten Datenwortes ermittelt wird. In einer bevorzugten Implementierung findet vielmehr keine Kontrolle auf die Länge statt. Dabei macht man sich zunutze, dass ein geeignet ausgewähltes Reduktionspolynom gewährleistet, dass die Reduktion nach 2 Iterationen komplett ist.

Nachfolgend werden Ausführungsbeispiele der erfindungsgemäßen Vorrichtung beschrieben. Die Ausführungsbeispiele können miteinander kombiniert werden, soweit sie nicht ausdrücklich als alternative Ausführungsbeispiele beschrieben sind.

Bei einem bevorzugten Ausführungsbeispiel der Reduzierungsvorrichtung ist die Steuereinheit ausgebildet, die Addiereinheit im Falle einer Wiederholung der Verfahrensschritte ab dem Schritt des Ermitteln eines binären Sub-Datenworts, zu instruieren, die jeweils gebildeten Summandenterme mit Ausnahme des ersten Summandenterms zum jeweiligen ersten Datenwort zu addieren, und nach einer Feststellung, dass ein ermitteltes Summendatenwort eine Länge hat, die nicht größer als m ist, zur Bildung des zweiten Datenworts jeden zwischenzeitlich

ermittelten ersten Summandenterm zum ermittelten Summendatenwort zu addieren.

5 Dieses Ausführungsbeispiel realisiert das Verfahren des zweiten Aspekts der Erfindung.

Ein weiteres bevorzugtes Ausführungsbeispiel enthält eine erste und eine zweite Justiereinheit. Die erste Justiereinheit ist ausgebildet, ein eingehendes erstes Datenwort mit einer Länge von weniger als $2n-1$ vor der Rechtsschiebeoperation
10 um eine Auffüllschrittweite nach links zu verschieben und beiderseits des ersten Datenwortes eine der Auffüllschrittweite entsprechende Anzahl Nullen an das erste Datenwort anzufügen, derart, dass die Länge des so modifizierten ersten Datenworts $2n-1$ beträgt und dass im modifizierten ersten Datenwort diejenigen
15 Terme des dem ersten Datenwort entsprechenden Polynoms $C(x)$, die eine Ordnung größer als m haben, an denselben Bitpositionen angeordnet sind wie wenn das erste Datenwort schon anfänglich die Länge $2n-1$ gehabt hätte.

Die zweite Justiereinheit ist ausgebildet, das ermittelte Summendatenwort der Länge von maximal m um die Auffüllschrittweite nach rechts zu verschieben und
20 die anfänglich angefügten Nullen zu entfernen.

Zur Beschleunigung der Reduktion enthält die Schiebeeinheit vorzugsweise eine Anzahl parallel geschalteter Rechtsschieber, denen das Sub-Datenwort zugeführt ist.

25 Alternativ enthält die Schiebeeinheit genau einen Rechtsschieber, und die Steuereinheit ist ausgebildet, die Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme durch zusätzliches Rechtsschieben des zuletzt vom Rechtsschieber ausgegebenen Summandenterms um eine jeweilige
30 Differenzschrittweite durchzuführen, wobei die jeweilige Differenzschrittweite die Differenz zwischen den Rechtsverschiebungen aufeinander folgender Summandenterme jeweils gegenüber dem ersten Summandenterm ist.

Einen sechsten Aspekt der Erfindung bildet eine Kryptographievorrichtung, insbesondere eine elektronische Kryptographievorrichtung, die eine Reduktionsvorrichtung nach dem fünften Aspekt der Erfindung oder ein im Rahmen dieser Anmeldung offenbartes Ausführungsbeispiel dieser Reduktionsvorrichtung enthält.

Die Kryptographievorrichtung ist in einer Ausführungsform zur Verschlüsselung oder Entschlüsselung von Daten nach einem Verfahren der elliptischen Kurvenkryptographie ausgebildet ist. Das beinhaltet selbstverständlich, dass die Kryptographievorrichtung entweder nur zur Verschlüsselung oder nur zur Entschlüsselung oder sowohl zur Verschlüsselung als auch zur Entschlüsselung von Daten ausgebildet ist.

In einer weiteren Ausführungsform enthält die elektronische Kryptographievorrichtung eine Multipliziereinheit, die ausgebildet ist zum Multiplizieren zweier, Faktor-Polynomen $A(x)$ und $B(x)$ entsprechenden Faktor-Datenworte zu einem dem Polynom $C(x)$ entsprechenden ersten Datenwort mit einer Länge von maximal $2n-1$. Die Multipliziereinheit kann in mit der Reduktionsvorrichtung in ein und demselben Chip integriert sein. Sie kann aber auch auf einem separaten Chip vorgesehen sein.

Nachfolgend werden die Erfindung und verschiedene Ausführungsbeispiele anhand der beiliegenden Figuren näher erläutert. Es zeigen

Fig. 1 ein Diagramm zur Erläuterung einer einfachen Polynomreduktion;

Fig. 2a) und 2b) zwei alternative Ausführungsformen des erfindungsgemäßen Verfahrens;

Fig. 3 ein weiteres alternatives Ausführungsbeispiel des erfindungsgemäßen Verfahrens;

Fig. 4 ein Blockdiagramm eines Ausführungsbeispiels eines flexiblen Reduzierers;

Fig. 5 ein Blockdiagramm zur Erläuterung einer alternativen Struktur einer Reduziereinheit für den flexiblen Reduzierer der Figur 4.

Figur 1 zeigt ein Diagramm zur Erläuterung einer einfachen Polynomreduktion. Das Grundproblem der Polynomreduktion in finiten binären Feldern besteht darin, dass eine Polynommultiplikation ein erstes Datenwort erzeugt, das eine größere Länge hat als die maximale Länge m des Feldes. Anstelle von der Feldlänge spricht man auch vom Feldgrad. Um das Polynomprodukt in das binäre finite Feld einzupassen, muss es reduziert werden. Der Reduktionsprozess entspricht der Bestimmung eines zum anfänglichen Datenwort äquivalenten Datenwort im binären finiten Feld $GF(2^m)$. Die Operation entspricht der bekannten Modulo-Operation in Primfeldern.

Ein naheliegender Reduktionsansatz besteht demnach darin, dass anfängliche erste Datenwort durch das irreduzible Polynom zu dividieren. Der Rest dieser Division ist das reduzierte Datenwort, das hier auch als zweites Datenwort bezeichnet wird.

Eine alternative Methode zur Reduktion bildet die multiplikative Reduktion. Bei diesem Verfahren wird der überhängende Teil des Datenwortes, der hier auch als zweites Sub-Datenwort bezeichnet wird, mit dem Reduktionspolynom multipliziert und vom anfänglichen ersten Datenwort subtrahiert. Die Subtraktion entspricht bekanntlich wie die Addition einer XOR-Verknüpfung.

Im in Figur 1 dargestellten Beispiel beträgt die maximale Feldlänge des verwendeten binären finiten Feldes $m = 3$. Nach einem ersten Iterationsschritt entsteht ein Summanden-Datenwort $C'(x)$, das sich wiederum als $C1'(x) * x^m + C0'(x)$ darstellen lässt. Das den überhängenden Teil bildende zweite Sub-Datenwort $C1'$ konnte also gegenüber dem anfänglichen ersten Datenwort verkleinert werden. Eine weitere Reduktion ist jedoch noch erforderlich, die durch Multiplikation

des zweiten Sub-Datenworts $C1'(x)$ mit dem Reduktionspolynom R bewerkstelligt wird. Wie im linken Teil des Diagramms der Figur 1 ersichtlich ist, ist nach diesen zwei Reduktionsschritten das anfängliche erste Datenwort 110111 durch zweifache Multiplikation des jeweils überhängenden zweiten Sub-Datenwortes mit dem irreduziblen Polynom 1011 auf das äquivalente Datenwort 110 im Feld $GF(2^3)$ reduziert worden.

Es wird betont, dass das Beispiel der Figur 1 nur zur Veranschaulichung des Prinzips dient. Das verwendete Zahlenbeispiel ist zur Erläuterung gewählt und insofern für den Anwendungsfall uncharakteristisch als die Länge des ersten Datenwortes hier 6 ist. Das entspricht 2^*m , während nach einer Multiplikation ist die Länge des zu reduzierenden Datenworts nicht länger als 2^*m-1 ist.

Die Figuren 2a) und 2b) zeigen zwei alternative Ausführungsformen des erfindungsgemäßen Verfahrens. Die in den Figuren 2a) und 2b) dargestellte Lösung basiert auf den Eigenschaften der finiten binären Felder, die beispielsweise von der NIST für die elliptische Kurvenkryptographie empfohlen sind. Da alle zusätzlich empfohlenen Reduktionspolynome entweder Trinomiale oder Pentanomiale sind, kann man eine Multiplikation durch 3 oder 5 aufsummierte Schiebeoperationen ersetzen. Da zusätzlich die zweithöchste besetzte Stelle in den Reduktionspolynomen in der Regel kleiner als $m/2$ ist, ist die komplette Reduktion nach zwei aufeinanderfolgenden Multiplikationen vollendet. Der entsprechende Reduktionsprozess wird anhand zweier Fälle in den Figuren 2a) und 2b) verdeutlicht.

Figur 2a) zeigt das erfindungsgemäße Verfahren für den Fall, dass die Länge des in Hardware zulässigen Feldes genau der Länge des Feldes entspricht ($m = n$), auf dem eine vorangegangene Polynommultiplikation durchgeführt wurde. Ein erstes, nicht reduziertes Datenwort 300 der Länge $2n-1$ ist in zwei Sub-Datenworte 302 und 304 partitionierbar. Ein erstes Sub-Datenwort $C0$ reicht von niedrigsten Bitposition bis zur Länge m des binären finiten Felds $GF(2^m)$. Ein zweites Sub-Datenwort $C1$ 304 entspricht dem überhängenden Teil des ersten Datenworts 300 und hat die Länge $2n-m-1$.

Die erwähnte Partitionierung des ersten Datenworts 300 in die zwei Sub-Datenwörter 302 und 304 benötigt keinen tatsächlichen Zerlegungsschritt. Es genügt, die Bits der entsprechenden Sub-Datenwörter für die nachfolgenden Rechnungsschritte von ihren jeweiligen Positionen separat abzugreifen.

5

Das zweite Sub-Datenwort 304 wird anschließend in verschiedenen Kopien um unterschiedliche Schrittweiten nach rechts verschoben. Dies ist in Figur 2a) durch die fünf Kopien 306 bis 314 des zweiten Sub-Datenwortes 304 schematisch symbolisiert. Jede Kopie ist um eine für sie aufgrund des verwendeten Reduktionspolynoms vorbestimmte Schrittweite nach rechts verschoben. Die Anzahl der tatsächlich verschobenen Summandenterme 308 bis 314 entspricht der Anzahl der nicht verschwindenden Terme vorbekannten Reduktionspolynoms $R(x)$, die nicht den Term x^m bilden. Die Kopie 306 muss dagegen nicht verschoben werden. Die Schrittweite einer jeweiligen Rechtsverschiebung ist gleich der Differenz von m und der Ordnung eines jeweiligen nicht verschwindenden Terms des Reduktionspolynoms.

10

15

Die Ordnung eines als Beispiel angenommen Terms x^{74} eines Reduktionspolynoms $R(x)$ ist 74. Im Feld $GF(2^{233})$ wird für diesen Term ein Summandenterm aus dem zweiten Sub-Datenwort 304 erzeugt, der um 159 Positionen nach rechts verschoben ist. Die in Figur 2 angezeigten Parameter s_0 bis s_3 repräsentieren die jeweilige Schrittweite einer jeweiligen Rechtsverschiebung.

20

Durch anschließendes Addieren der gebildeten Summandenterme 306 bis 314 zum ersten Sub-Datenwort 302 (C_0) entsteht ein Zwischenergebnis $C'(x) = C'_0(x) + C'_1(x)$, das als Block 320 dargestellt ist und zwei entsprechende Sub-Datenwörter 322 und 324 enthält. Ein schraffiert gekennzeichnete Bereich 324.1 enthält aufgrund der bis hier durchgeführten Verfahrensschritte lediglich Nullen.

25

Da jedoch das so gebildete Summendatenwort 320 noch nicht vollständig reduziert ist, werden die Schritte des Abgreifens des zweiten Sub-Datenwortes 324 und die Rechtsverschiebung des zweiten Sub-Datenwortes 324 entsprechend den Parametern s_0 bis s_3 des irreduziblen Polynoms R , wie oben erläutert,

30

erneut durchgeführt. Entsprechende rechtsverschobene Kopien 326 bis 334 des zweiten Sub-Datenwortes 324 sind in Figur 2a) dargestellt.

Es versteht sich, dass anstelle der parallelen Verschiebung von Kopien auch
5 serielle Verschiebeschritte an ein und demselben Sub-Datenwort vorgenommen werden können. Schneller ist jedoch die parallele Erzeugung der rechtsverschobenen Kopien mit verschiedenen, parallel geschalteten Rechtsschiebern.

Da der Term mit der zweihöchsten gesetzten Ordnung im Reduktionspolynom
10 weniger als die Hälfte des maximalen Grades m beträgt, sind lediglich zwei aufeinanderfolgende Iterationsschritte für eine vollständige Reduktion erforderlich.

Das nach erneut durchgeführter Addition der Summandenterme 326 bis 334 zum
15 ersten Sub-Datenwort 322 entstehende Summendatenwort 336 hat daher lediglich die maximale Länge m . Es bildet das gesuchte reduzierte, zweite Datenwort.

Figur 2b) zeigt ein dem Verfahren der Figur 2a) entsprechendes Verfahren für
den Fall, dass die maximale Feldlänge der eingehenden Datenworte kleiner ist
20 als die zulässige Datenwortbreite n des erfindungsgemäßen Reduzierers.

Zusätzlich zu den in Figur 1 dargestellten Verfahrensschritten, wird anfänglich ein erster Justierschritt durchgeführt, mit dem erreicht wird, dass die Länge des so modifizierten ersten Datenwortes gleich der hardwaremäßig unterstützten
25 Länge $2n-1$ beträgt und dass im so modifizierten ersten Datenwort 350 diejenigen Terme des dem ersten Datenwort entsprechenden Polynom $C(x)$, die eine Ordnung größer als m haben, an denselben Bitpositionen angeordnet sind, wie wenn das erste Datenwort 350 schon anfänglich die Länge $2n-1$ gehabt hätte. Im Ergebnis entspricht die so durchgeführte Linksverschiebung im ersten Justierschritt eine Verschiebung um $(n-m)$, wobei n die größte hardwaremäßig unter-
30 stützte Länge eines Datenwortes bedeutet. Am Eingang des Reduzierers ist die unterstützte Wortbreite dementsprechend $2n-1$.

Die Schrittweite dieser Linksverschiebung im ersten Justierschritt wird auf Auffüllschrittweite bezeichnet, weil die auf diese Weise entstehenden Bitpositionen in den Feldern 352.1 und 354.1 am Rande der Sub-Datenwörter 352 und 354 mit Nullen aufgefüllt werden.

5

Mit diesem so modifizierten ersten Datenwort 350 wird anschließend das Reduzierverfahren wie in Figur 2a) beschrieben. Dabei werden in einem ersten Iterationsschritt Summandenterme 356 bis 364 gebildet und zum ersten Sub-Datenwort 352 addiert. Das auf diese Weise erhaltene Summen-Datenwort 370
10 enthält in seinem überhängenden zweiten Sub-Datenwort 374 einen Block 374.1, der vollständig aus Nullen besteht. Die verbleibenden nicht verschwindenden Bitpositionen des überhängenden zweiten Sub-Datenwortes 374 werden in einem zweiten Iterationsschritt durch Bildung von Summandentermen 376 bis 384 und Addition zum ersten Sub-Datenwort 372 beseitigt, wodurch ein Summen-Datenwort 386 entsteht. Dieses wird in einem abschließenden zweiten Justierschritt um die gleiche Anzahl Bitpositionen, also um die Auffüllschrittweite nach
15 rechts verschoben, um den rechtsseitigen Block 386.1, der anfänglich durch Anfügung von Nullen entstanden war, zu beseitigen. Der verbleibende Block 386.2 entspricht dem gesuchten zweiten Datenwort, das zum ersten Datenwort
20 äquivalent ist.

Figur 3 zeigt einen alternativen Verfahrensfluss für den Fall $m < n$, der auch der Verfahrensführung der Figur 2b) zugrunde lag. Die Darstellung in Figur 3 ist in vier Hauptverfahrensblöcke S400, S410, S420 und S430 unterteilt.

25

Der Verfahrensblock S400 umfasst einen ersten Justierschritt S402, bei dem ein eingehendes Datenwort 450, dessen Länge $2m-1$ kleiner als die hardwaremäßig unterstützte Länge $2n-1$ ist, um eine Auffüllschrittweite sf nach links verschoben wird. Das so modifizierte Datenwort 450' enthält ein erstes Sub-Datenwort 452
30 und ein zweites Sub-Datenwort 454. Diese sind in Figur 4 wie gehabt auch mit C0 und C1 gekennzeichnet. Diese Bezeichnung umfasst auch die links- und rechtsseitig vorhandenen Blöcke 452.1 und 454.1, die mit Nullen gefüllt sind.

Das zweite Datenwort 454 wird anschließend in drei parallel durchgeführten Rechtsschiebeschritten um die Schrittweiten S1, S2 und S3 nach rechts verschoben erfolgt in entsprechenden Schritten S412, S414 und S416. Anschließend werden die so gebildeten Summandenterme in einem Addierschritt S418
5 zum ersten Sub-Datenwort 452 addiert.

Zu beachten ist, dass im Verfahren der Fig. 2 die Summandenterme zu C addiert (300) wurden. In der Verfahrensführung der Fig. 2 werden sie nur noch zu C0 addiert (452). Dadurch entfällt (unter Rückgriff auf die verwendeten Bezugszeichen) im vorliegenden Ausführungsbeispiel die Operation (304)+(306), die stets
10 in Null resultiert. In der vorliegenden Verfahrensführung werden daher insgesamt nur vier Terme zum ersten Sub-Datenwort hinzu addiert.

Nach der so erfolgten Teilreduktion wird das am Ausgang des Addierschritts 418
15 bereitstehende Summendatenwort 470 im nächsten Iterationsschritt S420 einer entsprechenden Schrittfolge S422 bis S428 unterzogen, wie im Zusammenhang mit Figur 2b) ausführlich wurde.

Das am Ausgang des Addierschritts S428 bereitstehende Summen-Datenwort
20 486 wird in einem anschließenden zweiten Justierschritt S432 um die Auffüllschrittweite sf nach rechts verschoben, wodurch ein entsprechend modifiziertes Summen-Datenwort 488 gebildet wird. Zu diesem werden anschließend in einem weiteren Addierschritt S434 die zweiten Sub-Datenwörter 454 und 474 addiert, wodurch am Ausgang des Addierschritts 434 das gesuchte reduzierte zweite
25 Datenwort 490 vorliegt.

Der Vorteil dieser Verfahrensführung liegt darin, dass in jedem Iterationsschritt ein Rechtsschiebeschritt eingespart wird. Dies bedeutet, dass in einer entsprechenden Hardwareimplementierung ein Rechtsschieber weniger benötigt wird,
30 was einerseits zu einer zusätzlichen Verfahrensbeschleunigung und andererseits zu einer Flächenersparnis führt.

Fig. 4 zeigt ein Blockdiagramm eines Reduzierers, der zur Implementierung der Verfahrensführung entsprechend den Figuren 2a) und 2b) ausgebildet ist. Der Reduzierer 500 ist einem Multiplizierer M nachgeschaltet, an dessen Ausgang Datenworte mit der Länge $2m-1$ anliegen. Ein solches Datenwort, dass das Produkt einer im Multiplizierer M durchgeführten Multiplikation bildet, wird einer ersten Justiereinheit 502 zugeführt, die eine Linksverschiebung entsprechend dem Schritt S402 aus Figur 3 ausführt. Hierbei wird die erste Justiereinheit 502 von einer Steuereinheit 504 angesteuert, die den Parameter m , also die Feldgrößen der Datenworte vorgibt. Anhand dieses Parameters ermittelt die erste Justiereinheit eine Auffüllschrittweite, wie zuvor beschrieben. Die Justiereinheit füllt nach einer mit der Auffüllschrittweite durchgeführten Linksverschiebung des eingangs anliegenden ersten Datenwortes am linken und rechten Rand mit Nullen auf, so dass am Ausgang der ersten Justiereinheit 502 ein Datenwort der vom Reduzierer 500 unterstützten Wortlänge $2n-1$ vorliegt. In dem so modifizierten ersten Datenwort liegen diejenigen Terme des dem ursprünglichen ersten Datenwort entsprechendem Polynoms $C(x)$, die eine Ordnung größer als m haben an denselben Bitpositionen, wie wenn schon das ursprüngliche Datenwort die Länge $2n-1$ gehabt hätte.

Der ersten Justiereinheit 502 ist eine Reduziereinheit 506 nachgeschaltet, deren Betrieb ebenfalls von der Steuereinheit 504 kontrolliert wird. Diese liefert der Reduziereinheit insbesondere die für die anhand der Figuren 2a) und 2b) und Figur 3 ausführlich beschriebenen Rechtsverschiebungen erforderlichen Parameter $S0$ bis $S3$. Die nähere Struktur der Reduziereinheit wird anhand der nachfolgenden Figuren 6 und 7 in alternativen Ausführungsbeispielen beschrieben.

Der Reduziereinheit 506 ist eine zweite Justiereinheit 508 nachgeschaltet. Diese sorgt für eine Rücktransformation des am Ausgang des Reduzierers anliegenden Summen-Datenwortes durch eine Rechtsverschiebung und Entfernung der eingangs in der ersten Justiereinheit eingefügten Nullen. Am Ausgang der zweiten Justiereinheit 508 liegt dann das gesuchte reduzierte zweite Datenwort an.

Figur 5 zeigt eine alternative Implementierung der Reduziereinheit, bei der mit lediglich einem Rechtsschieber 702 gearbeitet wird, der seriell unterschiedlich weit verschobene Kopien des zweiten Sub-Datenwortes erzeugt, die zum jeweiligen ersten Sub-Datenwort hinzu addiert werden.

5

Die Reduziereinheit 706 der Figur 5 benötigt dementsprechend viele Zyklen für einen Reduzierschritt, wobei vorausgesetzt wird, dass die Rechtsverschiebungen in der Ordnung $S3 \leq S2 \leq S1 \leq S0$ durchgeführt werden, so dass sukzessive nach rechts geschoben wird.

10

Patentansprüche

1. Verfahren zur Reduktion eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C^0(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, mit den Schritten:
- 10 - Bereitstellen eines Reduktionspolynoms $R(x)$, das ein Trinomial oder ein Pentanomial bildet;
 - Partitionieren des ersten Datenworts in ein binäres erstes Sub-Datenwort C_0 und ein binäres zweites Sub-Datenwort C_1 , deren entsprechende Polynome $C_0(x)$ und $C_1(x)$ die Gleichung $C(x) = C_1(x) * x^m + C_0(x)$ erfüllen, und Abgreifen des zweiten Sub-Datenwortes zur Bildung eines ersten Summandenterms;
 - 20 - Rechtsverschieben des zweiten Sub-Datenworts zur Bildung eines zweiten Summandenterms, und Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme, bis jedem nicht verschwindenden Term des Reduktionspolynoms, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist, indem die Schrittweite einer jeweiligen Rechtsverschiebung gleich der Differenz von m und der Ordnung eines jeweiligen nicht verschwindenden Terms des Reduktionspolynoms ist;
 - 25 - Addieren der gebildeten Summandenterme zum ersten Sub-Datenwort zur Bildung eines Summendatenwortes;
 - 30 - wenn das so ermittelte Summendatenwort eine Länge größer als m hat, Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens

auf das gebildete Summandendatenwort, bis das so ermittelte Summandendatenwort eine Länge von maximal m hat und somit das zweite Datenwort bildet.

- 5 2. Verfahren zur Reduktion eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C'(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, mit den Schritten:

- 10 - Bereitstellen eines Reduktionspolynoms $R(x)$, das ein Trinomial oder ein Pentanomial bildet;
- 15 - Partitionieren des ersten Datenworts in ein binäres erstes Sub-Datenwort C_0 und ein binäres zweites Sub-Datenwort C_1 , deren entsprechende Polynome $C_0(x)$ und $C_1(x)$ die Gleichung $C(x) = C_1(x) * x^m + C_0(x)$ erfüllen, und Abgreifen des zweiten Sub-Datenwortes zur Bildung eines ersten Summandenterms;
- 20 - Rechtsverschieben des zweiten Sub-Datenworts zur Bildung eines zweiten Summandenterms, und Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme, bis jedem nicht verschwindenden Term des Reduktionspolynoms, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist, indem die Schrittweite einer jeweiligen Rechtsverschiebung gleich der Differenz von m und der Ordnung eines jeweiligen nicht verschwindenden Terms des Reduktionspolynoms ist;
- 25 - Addieren der gebildeten Summandenterme, mit Ausnahme des ersten Summandenterms, zum ersten Datenwort;
- 30

- wenn das so ermittelte Summendatenwort eine Länge größer als m hat, Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens auf das gebildete Summandendatenwort, bis das so ermittelte Summendatenwort eine Länge von maximal m hat;
- 5
- Addieren des ersten Summandenterms und, im genannten Falle einer Anwendung der Verfahrensschritte ab dem Schritt des Partitionierens auf das gebildete Summandendatenwort, jedes weiteren zwischenzeitlich ermittelten zweiten Sub-Datenworts zum zuletzt ermittelten Summendatenwort zur Bildung des zweiten Datenworts.
- 10
3. Verfahren nach Anspruch 1 oder 2, bei dem das erste Datenwort eine Länge von weniger als $2n-1$ hat, mit einem vor der Rechtsschiebeoperation durchgeführten zusätzlichen ersten Justierschritt, der ein Linksverschieben
- 15 des ersten Datenworts um eine Auffüllschrittweite und ein beiderseitiges Anfügen einer der Auffüllschrittweite entsprechenden Anzahl Nullen an das erste Datenwort beinhaltet, derart, dass die Länge des so modifizierten ersten Datenworts $2n-1$ beträgt und dass im modifizierten ersten Datenwort diejenigen Terme des dem ersten Datenwort entsprechenden Polynoms
- 20 $C(x)$, die eine Ordnung größer als m haben, an denselben Bitpositionen angeordnet sind wie wenn das erste Datenwort schon anfänglich die Länge $2n-1$ gehabt hätte.
4. Verfahren nach Anspruch 3, mit einem zweiten Justierschritt, der ein Entfernen der anfänglich angefügten Nullen aus dem ermittelten Summendatenwort und ein Rechtsverschieben des Summendatenworts um die Auffüllschrittweite beinhaltet.
- 25
5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem das irreduzible Polynom allein durch die Potenzen der nicht verschwindenden Terme des Reduktionspolynoms, die nicht der Term x^m sind, repräsentiert wird.
- 30

6. Verfahren nach Anspruch 5, bei dem das irreduzible Polynom zusätzlich durch die bekannte maximale Länge m von Datenworten des binären finiten Feldes repräsentiert wird.
- 5 7. Asymmetrisches Kryptographieverfahren zur Verwendung in einer elektronischen Kryptographievorrichtung, umfassend
 - Reduzieren eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld $GF(2^m)$,
10 dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C^{-1}(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, gemäß einem Verfahren eines der Ansprüche 1 bis 6.
- 15 8. Asymmetrisches Kryptographieverfahren nach Anspruch 7, das ein Verfahren der elliptischen Kurvenkryptographie bildet, umfassend vor dem Reduzieren:
 - Multiplizieren zweier, Faktor-Polynomen $A(x)$ und $B(x)$ entsprechenden Faktor-Datenworte zu dem einem Polynom $C(x)$ entsprechenden ersten Datenwort mit einer Länge von maximal $2n-1$.
- 20 9. Verfahren zur Berechnung einer digitalen Signatur, umfassend ein asymmetrisches Kryptographieverfahren nach Anspruch 8.
- 25 10. Vorrichtung zur Reduktion eines einem Polynom $C(x)$ entsprechenden ersten Datenworts mit einer Länge von maximal $2n-1$ auf ein zweites Datenwort mit einer Länge von maximal m , das in einem binären finiten Feld $GF(2^m)$, dessen Elemente eine maximale Länge m haben, einem zu $C(x)$ äquivalenten Polynom $C^{-1}(x)$ entspricht, wobei m entweder kleiner oder gleich n ist, mit:
30
 - einem Speicher, der eine Repräsentation mindestens eines Reduktionspolynoms $R(x)$ enthält, das ein Trinomial oder ein Pentanomial bildet;

- einer Selektionseinheit, die ausgebildet ist, ein binäres Sub-Datenwort aus dem ersten Datenwort zu abzugreifen, dessen entsprechendes Polynom $C1(x)$ die Gleichung $C(x) = C1(x) * x^m + C0(x)$ erfüllt und das einen ersten Summandenterm bildet;
5
- einer Schiebeeinheit, die mit der Selektionseinheit verbunden und ausgebildet ist, das Sub-Datenwort zur Bildung eines zweiten oder weiterer Summandenterme um eine jeweils vorbestimmte Schrittweite nach rechts zu verschieben und die gebildeten Summandenterme auszugeben;
10
- einem Addiereinheit, die mit der Schiebeeinheit verbunden und ausgebildet ist, einen jeweiligen Summandenterm sowie die von der Schiebeeinheit ausgegebenen Summanden zum ersten Datenwort zu addieren;
15 und
- einer Steuereinheit, die ausgebildet ist,
20 die Schrittweite einer jeweiligen, von der Schiebeeinheit auszuführenden Rechtsverschiebung zur Bildung eines Summandenterms als Differenz von m und der Ordnung eines jeweiligen nicht verschwindenden Terms des Reduktionspolynoms zu bestimmen,
- 25 die Schiebeeinheit zur wiederholten Durchführung des Rechtsverschiebungsschritts für eine Bildung weiterer Summandenterme mit jeweils neu bestimmter Schrittweite zu instruieren, bis jedem nicht verschwindenden Term eines jeweils vorgegebenen Reduktionspolynoms, der nicht der Term x^m ist, je ein Summandenterm zugeordnet ist,
30
- und die Berechnungseinheit, die Schiebeeinheit und die Addiereinheit erforderlichenfalls erneut zu aktivieren, bis ein ermitteltes Summendatenwort eine Länge von maximal m hat und somit das zweite Datenwort bildet.

11. Vorrichtung nach Anspruch 10, bei der die Steuereinheit ausgebildet ist, die Addiereinheit im Falle einer Wiederholung der Verfahrensschritte ab dem Schritt des Ermitteln eines binären Sub-Datenworts, zu instruieren, die jeweils gebildeten Summandenterme mit Ausnahme des ersten Summandenterms zum jeweiligen ersten Datenwort zu addieren,

und nach einer Feststellung, dass ein ermitteltes Summendatenwort eine Länge hat, die nicht größer als m ist, zur Bildung des zweiten Datenworts jeden zwischenzeitlich ermittelten ersten Summandenterm zum ermittelten Summendatenwort zu addieren.

12. Vorrichtung nach Anspruch 10 oder 11, mit einer ersten und einer zweiten Justiereinheit,

wobei die erste Justiereinheit ausgebildet ist, ein eingehendes erstes Datenwort mit einer Länge von weniger als $2n-1$ vor der Rechtsschiebeoperation um eine Auffüllschrittweite nach links zu verschieben und beiderseits des ersten Datenwortes eine der Auffüllschrittweite entsprechende Anzahl Nullen an das erste Datenwort anzufügen, derart, dass die Länge des so modifizierten ersten Datenworts $2n-1$ beträgt und dass im modifizierten ersten Datenwort diejenigen Terme des dem ersten Datenwort entsprechenden Polynoms $C(x)$, die eine Ordnung größer als m haben, an denselben Bitpositionen angeordnet sind wie wenn das erste Datenwort schon anfänglich die Länge $2n-1$ gehabt hätte, und

wobei die zweite Justiereinheit ausgebildet ist, das ermittelte Summendatenwort der Länge von maximal m um die Auffüllschrittweite nach rechts zu verschieben und die anfänglich angefügten Nullen zu entfernen.

13. Vorrichtung nach einem der Ansprüche 10 bis 12, bei der die Schiebeeinheit eine Anzahl parallel geschalteter Rechtsschieber enthält, denen das Sub-Datenwort zugeführt ist.

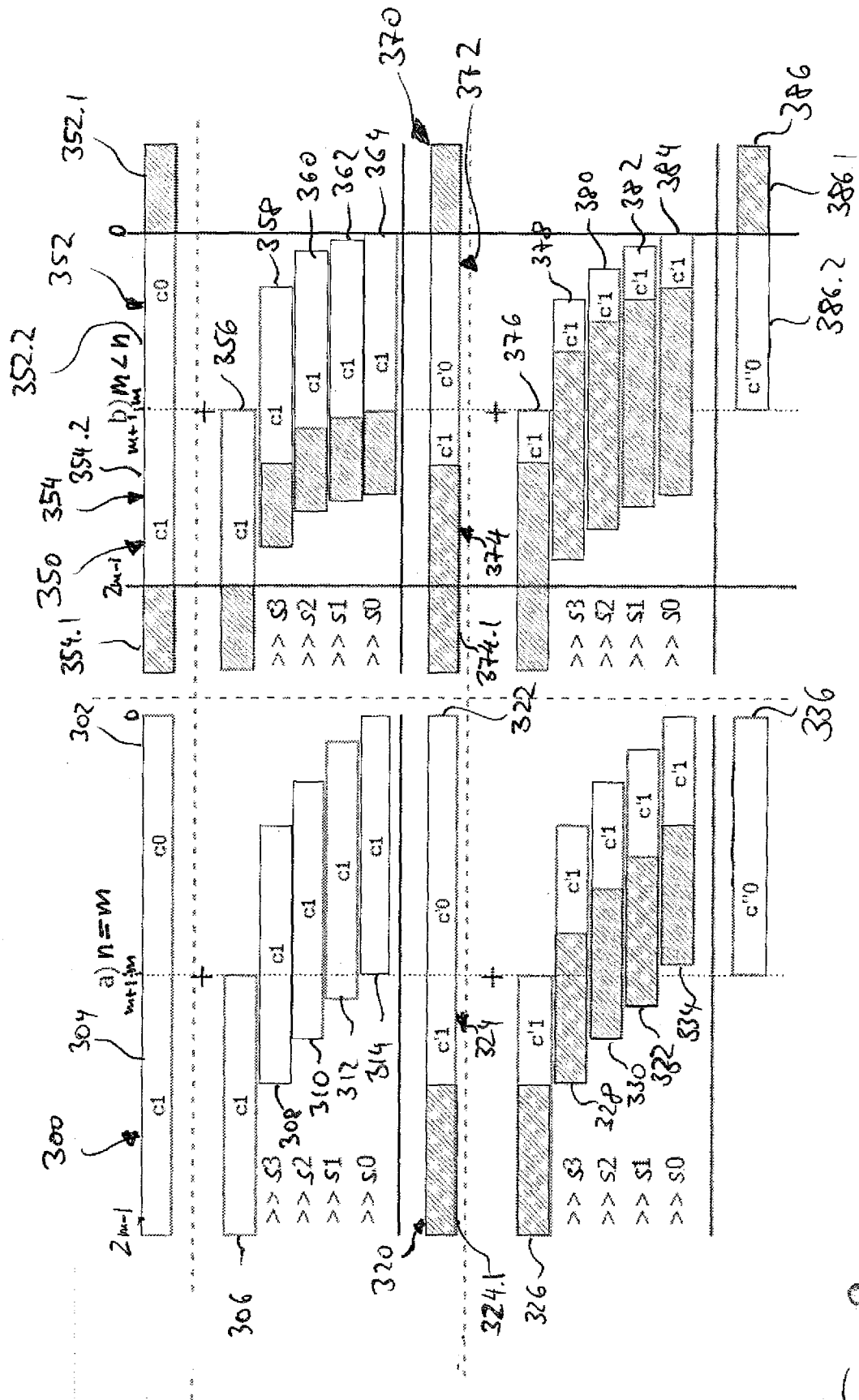
14. Vorrichtung nach einem der Ansprüche 10 bis 12, bei der die Schiebereinheit genau einen Rechtsschieber enthält, und bei der die Steuereinheit ausgebildet ist, die Wiederholung des Rechtsverschiebungsschrittes zur Bildung weiterer Summandenterme durch zusätzliches Rechtsschieben des zuletzt vom Rechtsschieber ausgegebenen Summandenterms um eine jeweilige Differenzschrittweite durchzuführen, wobei die jeweilige Differenzschrittweite die Differenz zwischen den Rechtsverschiebungen aufeinander folgender Summandenterme jeweils gegenüber dem ersten Summandenterm ist.
15. Elektronische Kryptographievorrichtung, enthaltend eine Reduktionsvorrichtung nach einem der Ansprüche 10 bis 14.
16. Elektronische Kryptographievorrichtung nach Anspruch 15, die zur Verschlüsselung oder Entschlüsselung von Daten nach einem Verfahren der elliptischen Kurvenkryptographie ausgebildet ist.
17. Elektronische Kryptographievorrichtung nach Anspruch 16, mit einer Multipliziervorrichtung, die ausgebildet ist zum Multiplizieren zweier, Faktor-Polynomen $A(x)$ und $B(x)$ entsprechenden Faktor-Datenworte zu einem dem Polynom $C(x)$ entsprechenden ersten Datenwort mit einer Länge von maximal $2n-1$.

1	1	0	1	1	1	:	1	0	1	1
1	1	1	0	1	0					
		1	1	0	1					
		1	0	1	1					
			1	1	0					

	C1	C0
$\oplus$	$C1 \cdot R$	
=	C1'	C0'
$\oplus$	$C1' \cdot R$	
=	C0''	

Fig. 1

- STAND DER TECHNIK -



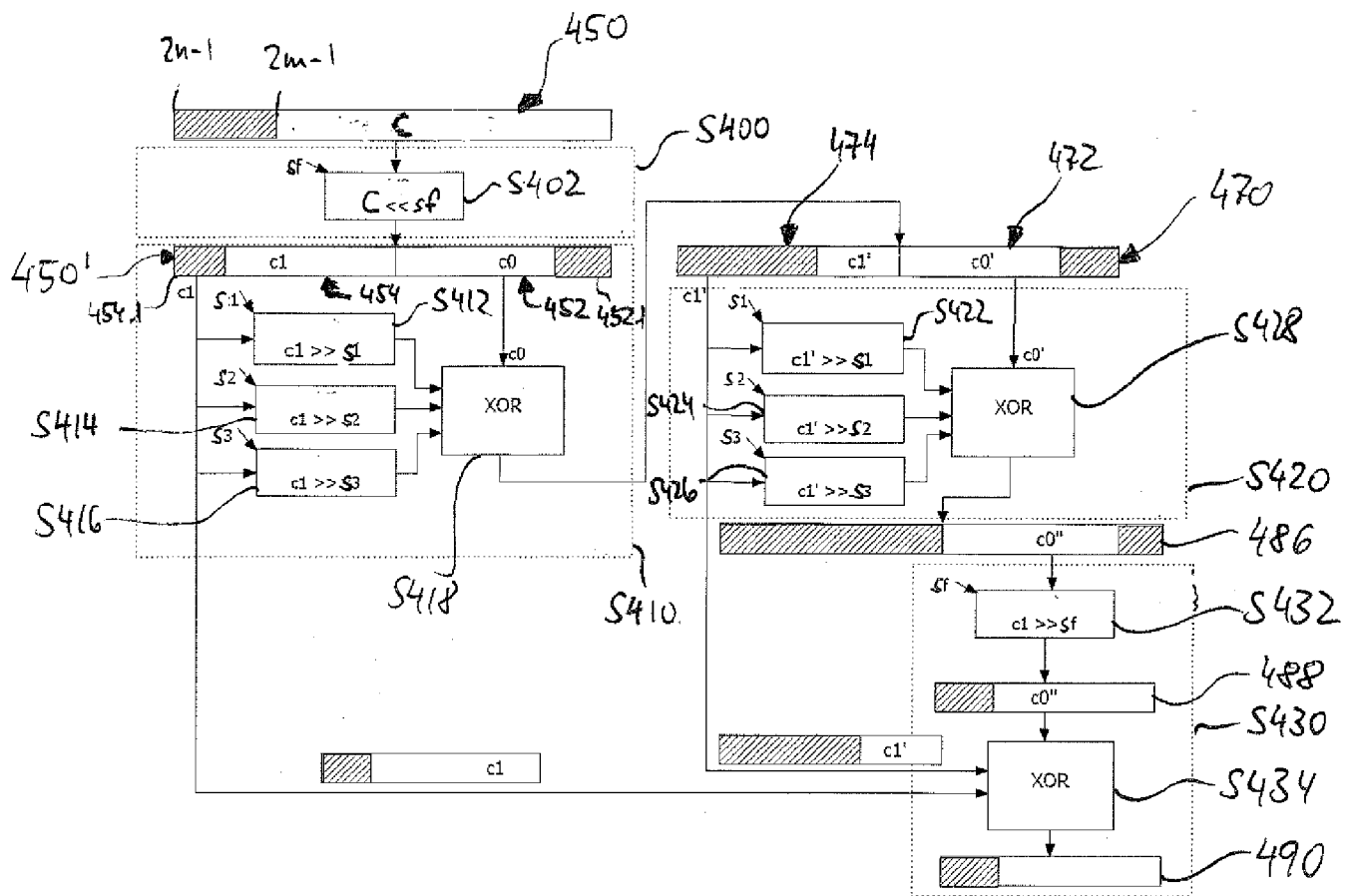


Fig. 3

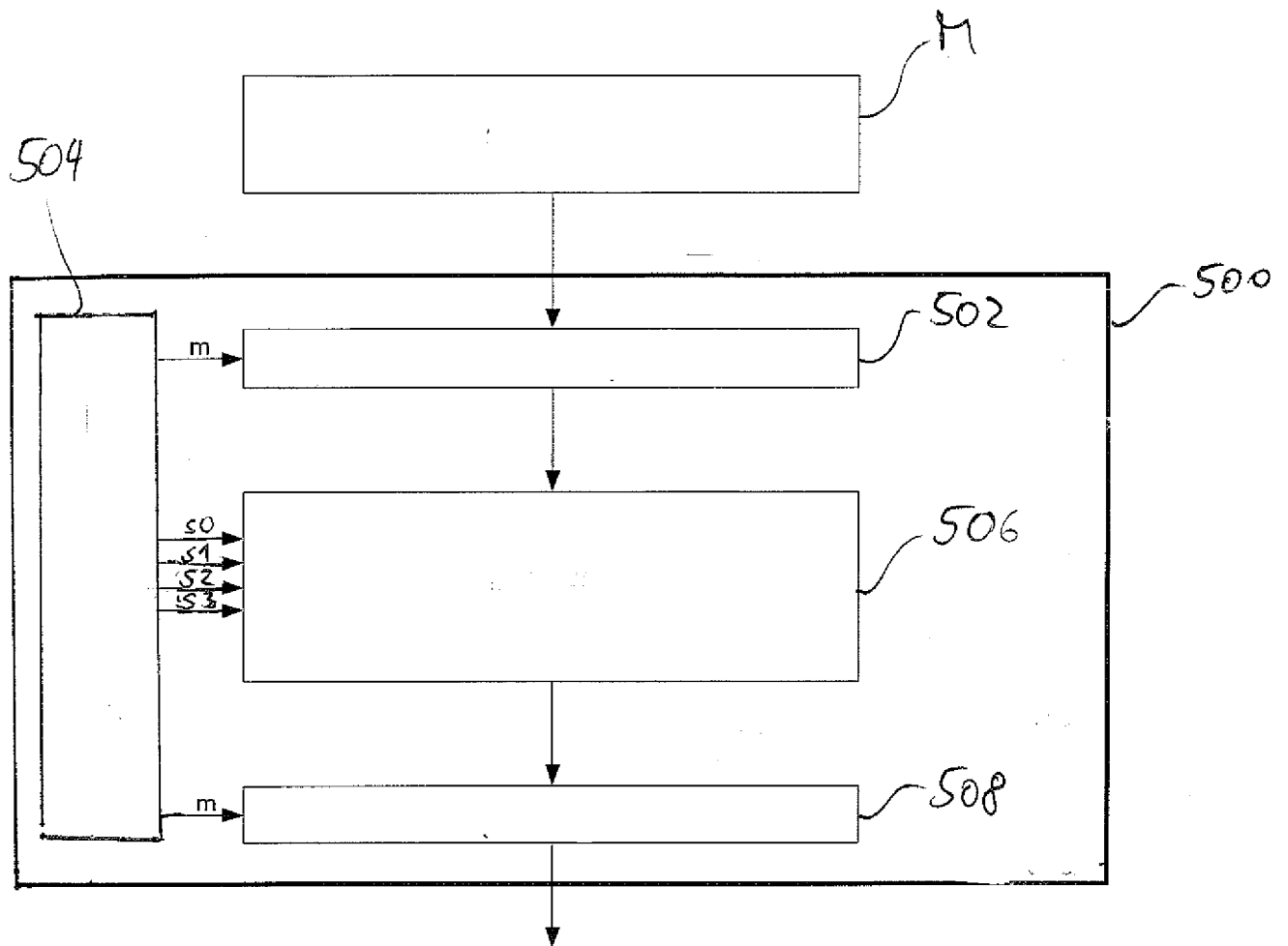


Fig. 4

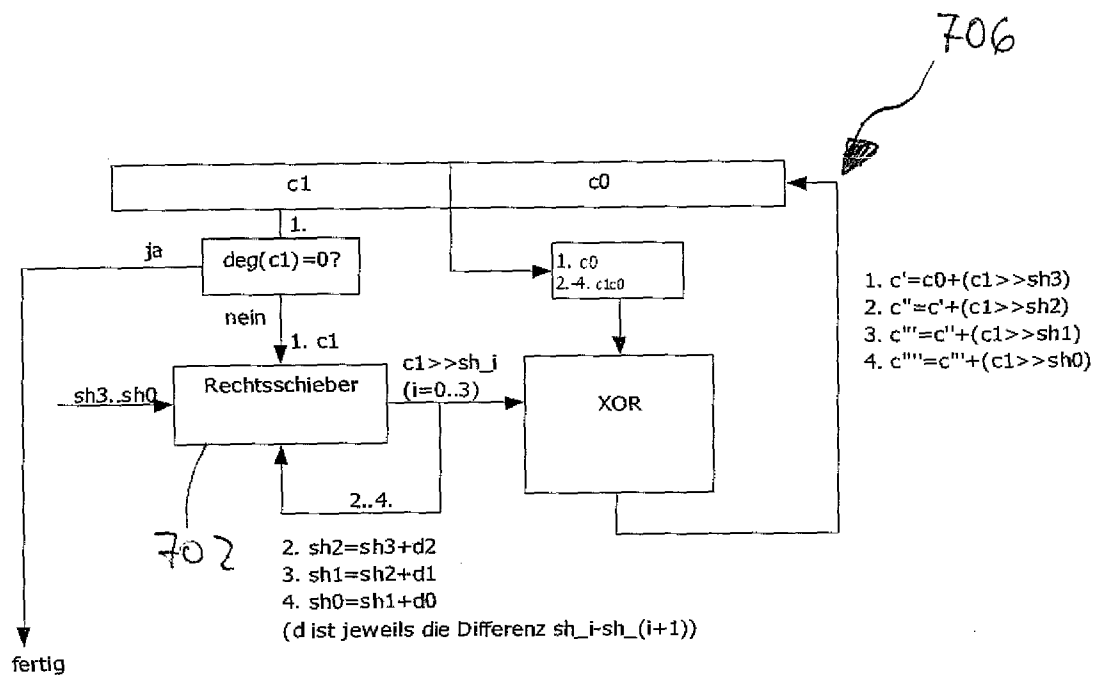


Fig. 5