Deutsches
Patent- und Markenamt

Bibliografie-Mitteilung
für AKZ 10 2017 010 931.1

Stand: 03.01.2018

IPC-Hauptklasse	G06F 17/10
Anmeldetag	25.11.2017
Bezeichnung	Verfahren zur Beschleunigung von Berechnungen in endlichen Körpern
Anmelder-Nr. 19369085	Huber, Klaus, Dr. , 10627 Berlin, DE
Zeichen des Anmelders / Vertreters	KH2017/1
Zustellanschrift-Nr. 142190764	Herrn Dr. Klaus Huber Sesenheimer Str. 21 10627 Berlin
Erfinder	Erfinder gleich Anmelder

1514987873821760105 7

Die Veröffentlichung der Anmeldung erfolgt voraussichtlich am 29.05.2019.
Sie unterbleibt, wenn die Anmeldung vor Abschluss der technischen Vorbereitung für die Veröffentlichung (10 Wochen vor dem vorgesehenen Veröffentlichungstag) zurückgenommen wird oder als zurückgenommen gilt (§ 32 Abs. 4 Patentgesetz).

Bitte beachten Sie die wichtigen Hinweise auf der letzten Seite

Beschreibung

Verfahren zur Beschleunigung von Berechnungen in endlichen Körpern

Die Erfindung betrifft ein Verfahren und eine Anordnung zum verbesserten Rechnen in endlichen Körpern.

Endliche Körper werden bei zahlreichen Anwendungen in der Technik benötigt. Insbesondere bei der Codierung zur Fehlerkorrektur und in der Kryptographie. Die Grundlagen findet man in einschlägigen Lehrbüchern wie etwa
Berlekamp E., 'Algebraic Coding Theory', Aegean Park Press, reprint 1984
oder
Blake I. et al, 'Elliptic Curves in Cryptography', Cambridge University Press, 2000.

Aufgabe der Erfindung ist es, durch geschickte Wahl von Parametern mit denen endliche Körper realisiert werden, Berechnungen wie etwa die Funktionen des Wurzelziehens und der Quadrierung zu vereinfachen. Da diese Funktionen essentiell für die Berechnung von zahlreichen weiteren häufig benötigten Funktionen sind, ergibt sich eine verbesserte Effizienz.

Die Erfindung bezieht sich hauptsächlich auf Körper der Charakteristik zwei, einem in der Praxis besonders häufig auftretenden Fall. Solche Körper werden oft mit $GF(2^m)$ bezeichnet. GF steht dabei für Galoisfeld und 2^m gibt an wieviele Elemente $q = 2^m$ der Körper hat.

Endliche Körper werden mit Hilfe von irreduziblen oder primitiven Polynomen konstruiert. Ein Element des Körpers $GF(2^m)$

wird dabei als binäres Polynom vom Grad $m-1$ beschrieben. Die Operationen Addition und Multiplikation werden dann modulo 2 und modulo des irreduziblen Polynoms $p(x)$ durchgeführt. Ein irreduzibles Polynom lässt sich nicht als Produkt von Polynomen kleineren Grades darstellen. Bei Anwendungen werden meistens spezielle irreduzible Polynome benutzt, die Wurzeln besitzen, mit denen sich sämtliche von Null verschiedenen Elemente des Körpers erzeugen lassen. Diese Polynome nennt man primitive Polynome. Wenn α Wurzel des primitiven Polynoms $p(x)$ ist, d.h. $p(\alpha) = 0$, dann erzeugen die Potenzen $\alpha^i, i = 0, 1, 2, \ldots$ alle Elemente von $GF(2^m)$, die von Null verschieden sind.

Um die Berechnungen modulo des gewählten irreduziblen (oder primitiven) Polynoms möglichst einfach durchführen zu können, werden in der Praxis meist Polynome $p(x)$ gewählt, die eine möglichst einfache Gestalt haben. Man wählt z.B. sogenannte irreduzible oder primitive Trinome $p(x) = x^n + x^k + 1$ oder Polynome der Gestalt $p(x) = x^n + r(x)$, wobei $r(x)$ einen möglichst kleinen Grad hat. Da es nicht für alle Werte von m geeignete Trinome gibt, wählt man oft auch Pentanome aus, d.h. Polynome der Gestalt $p(x) = x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$. Geeignete Polynome kann man leicht für alle benötigten Werte von n mit Hilfe von Computerprogrammen bestimmen.

Das Verfahren um das Wurzelziehen (und auch die Quadrierung) im Körper $GF(2^m)$ zu verbessern besteht darin, unter den primitiven Polynomen mit einfacher Gestalt diejenigen zu benutzen, die das Wurzelziehen und Quadrieren vereinfachen.

Zum Wurzelziehen wird ein Verfahren benutzt, das in den beiden Artikeln
K.Huber, Note on Decoding Binary Goppa Codes", Electronics Letters, 18th January 1996, Vol. 32 No.2, pp. 102-103 und

K.Huber, Taking pth Roots Modulo Polynomials over Finite Fields, Designs, Codes and Cryptography, 28, 303-311, 2003
beschrieben ist.

Ein Element des Körpers, gegeben durch das binäre Polynom $b(x)$, kann leicht in der Form $b(x) = b_0(x)^2 + x \cdot b_1(x)^2$ dargestellt werden. Mit dem Polynom $w(x)$ für das gilt $w(x)^2 \equiv x \bmod p(x)$ kann dann die Wurzel ausgedrückt werden durch

$$\sqrt{b(x)} \equiv b_0(x) + w(x) \cdot b_1(x) \bmod p(x).$$

Somit besteht die wesentliche Operation des Wurzelziehens in einer Multiplikation von $w(x)$ mit $b_1(x)$. Wenn das Hamminggewicht von $w(x)$ klein ist, entspricht dies ein paar wenigen Shift-Operationen.

Das kleinstmögliche Hamminggewicht von $w(x)$ ist gleich zwei. In Tabelle I sind primitive Polynome $p(x)$ angegeben, die zu Polynomen $w(x)$ mit Hamminggewicht zwei führen.

Eine weitere Verbesserung ergibt sich, wenn der Grad von $w(x)$ so klein ist, dass die Multiplikation von $w(x)$ mit $b_1(x)$ zu einem Polynom führt dessen Grad kleiner als der Grad von $p(x)$ ist. In diesem Fall kann auf die Moduloreduktion verzichtet werden und wir erhalten

$$\sqrt{b(x)} = b_0(x) + w(x) \cdot b_1(x).$$

Ausserdem kann in diesem Fall die Gleichung dazu benutzt werden um effizient im Körper zu quadrieren, da bei bekannter rechter Seite die Polynome b_0 und b_1 leicht bestimmt werden können. In Tabelle II sind primitive Polynome $p(x)$ angegeben, die zu derartigen Polynomen $w(x)$ führen (die Gradbedingung lautet $\operatorname{Grad} w(x) \leq (m+1)/2$, d.h. $m/2$ bei geradem m und $(m+1)/2$

bei ungeradem m). Es sind jeweils Polynome gelistet, die die Gradbedingung erfüllen und dabei zum kleinstmöglichen Hamminggewicht für $w(x)$ führen (es wurde eine vollständige Suche durchgeführt). Der einzige Fall, bei dem es kein Polynom gibt, bei dem auf die Moduloreduktion verzichtet werden kann, ist bei $m = 8$ zur Realisierung des Körpers $GF(2^8)$. Hier benutzt man am besten das primitive Polynom $p(x) = x^8 + x^7 + x^2 + x + 1$, das zu $w(x) = x^5 + x^4 + x^2$ führt. Für alle anderen m insbesondere auch für sehr grosse Werte findet man problemlos geeignete Polynome, die die Gradbedingung erfüllen.

In Tabelle III sind weitere Polynome vom Grad 32 bis 64 gelistet, die die Gradbedingung erfüllen und geringes Gewicht für $w(x)$ und $p(x)$ liefern. In Tabelle IV sind Polynome $p(x)$ für noch grössere Körper $GF(2^m)$ gelistet. Körper dieser Grösse werden derzeit mit anderen primitiven Polynomen (die zu $w(x)$ mit grösserem Gewicht führen) für kryptographische Zwecke genutzt. Polynome wie die in den Tabellen III und IV findet man leicht mit gängigen Irreduzibilitäts- bzw. Primitivitätstests, wobei man die Suche von vornherein auf bestimmte Polynome $p(x)$ beschränken kann. So findet man z.B. $w(x)$ mit Gewicht zwei bei Polynomen $p(x)$ der Gestalt $p(x) = x^m+x^k+1$ mit m und k ungerade ($\Rightarrow w(x) = x^{\frac{m+1}{2}} + x^{\frac{m+1}{2}}$) oder $p(x) = x^m + x + 1$ mit m gerade ($\Rightarrow w(x) = x^{\frac{m}{2}} + 1$). $w(x)$ mit Gewicht drei findet man beispielsweise bei Polynomen der Gestalt $p(x) = x^m+x^{m-1}+1$ mit m gerade ($\Rightarrow w(x) = x^{\frac{m+1}{2}}+x^{\frac{m-1}{2}}$) oder $p(x) = x^m+x^k+1$ mit m gerade und k ungerade, $k \geq 3$ ($\Rightarrow w(x) = x^{m-\frac{m-1}{2}}+x^{\frac{m}{2}-\frac{k-1}{2}}+x^{\frac{k-1}{2}}$). $w(x)$ mit Gewicht vier findet man etwa mit $p(x) = x^m+x^{k_1}+x^{k_2}+x+1$ mit m, k_1, k_2 gerade ($\Rightarrow w(x) = x^{\frac{m}{2}}+x^{\frac{k_1}{2}}+x^{\frac{k_2}{2}}+1$) oder $p(x) = x^m+x^{k_1}+x^{k_2}+x^{k_3}+1$ mit m, k_1, k_2, k_3 alle ungerade ($\Rightarrow w(x) = x^{\frac{m+1}{2}} + x^{\frac{k_1+1}{2}}+x^{\frac{k_2+1}{2}} + x^{\frac{k_3+1}{2}}$).

Tabelle I: Primitive Polynome p(x), die zu $w(x)$ mit Hamminggewicht zwei führen		
m	$p(x)$	$w(x)$
2	x^2+x+1	$x+1$
3	x^3+x+1	x^2+x
4	x^4+x+1	x^2+1
5	x^5+x^3+1	x^3+x^2
6	x^6+x+1	x^3+1
7	x^7+x+1	x^4+x
8	$x^8+x^7+x^5+x^3+1$	x^7+x
9	x^9+x^5+1	x^5+x^3
10	$x^{10}+x^8+x^7+x^4+x^2+x+1$	x^7+x^5
11	$x^{11}+x^9+1$	x^6+x^5
12	$x^{12}+x^8+x^7+x^5+x^4+x+1$	$x^{10}+x^7$
13	$x^{13}+x^{10}+x^8+x^7+x^4+x^3+x^2+x+1$	x^9+1
14	$x^{14}+x^{11}+x^9+x^8+x^7+x^4+x^2+x+1$	x^9+x^8
15	$x^{15}+x+1$	x^8+x
16	$x^{16}+x^{14}+x^{13}+x^{10}+x^9+x^8+x^7+x^5+x^4+x^3+x^2+x+1$	$x^{14}+x^{13}$
17	$x^{17}+x^3+1$	x^9+x^2
18	$x^{18}+x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^8+x^7+x^4+x^3+1$	$x^{16}+x^6$
19	$x^{19}+x^{18}+x^{15}+x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^3+1$	$x^{12}+x^{11}$
20	$x^{20}+x^{15}+x^{14}+x^{13}+x^{12}+x^9+x^7+x^6+x^4+x^3+x^2+x+1$	$x^{18}+x^{15}$
21	$x^{21}+x^{19}+1$	$x^{11}+x^{10}$
22	$x^{22}+x+1$	$x^{11}+1$
23	$x^{23}+x^5+1$	$x^{12}+x^3$
24	$x^{24}+x^{20}+x^{19}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^6+x^3+x+1$	$x^{21}+x^4$
25	$x^{25}+x^3+1$	$x^{13}+x^2$
26	$x^{26}+x^{24}+x^{23}+x^{22}+x^{19}+x^{17}+\ldots+x^{14}+x^{11}+x^9+x^8+x^7+x^4+x^2+x+1$	$x^{19}+x^9$
27	$(x^{29}+x+1)/(x^2+x+1)$	$x^{15}+x$
28	$x^{28}+x^{26}+x^{25}+x^{21}+x^{17}+x^{16}+x^{12}+x^{11}+x^9+x^6+x^5+x+1$	$x^{21}+x^9$
29	$x^{29}+x^{27}+1$	$x^{15}+x^{14}$
30	$x^{30}+x^{27}+x^{25}+x^{17}+x^{15}+x^{11}+x^{10}+x^9+x^5+x^4+x^3+x+1$	$x^{21}+x^{15}$
31	$x^{31}+x^3+1$	$x^{16}+x^2$
32	$x^{32}+x^{30}\ldots x^{27}+x^{24}+x^{23}+x^{21}+x^{18}+x^{17}+x^{14}+x^{12}+x^{10}+x^7+x^6+x^4\ldots x^2+1$	$x^{21}+x$
Das Polynom $p(x)$ bei m=27 lautet in binärer Darstellung: $110110110\ldots1101$		

Tabelle II: Primitive Polynome p(x) mit Grad $w(x) = \lfloor \frac{m+1}{2} \rfloor$		
m	$p(x)$	$w(x)$
2	x^2+x+1	$x+1$
3	x^3+x+1	x^2+x
4	x^4+x+1	x^2+1
5	x^5+x^3+1	x^3+x^2
6	x^6+x+1	x^3+1
7	x^7+x+1	x^4+x
8	-	-
9	x^9+x^5+1	x^5+x^3
10	$x^{10}+x^8+x^6+x+1$	$x^5+x^4+x^3+1$
11	$x^{11}+x^9+1$	x^6+x^5
12	$x^{12}+x^8+x^2+x+1$	x^6+x^4+x+1
13	$x^{13}+x^{12}+\ldots+x^2+1$	x^7+x+1
14	$x^{14}+x^6+x^4+x+1$	$x^7+x^3+x^2+1$
15	$x^{15}+x+1$	x^8+x
16	$x^{16}+x^6+x^4+x+1$	$x^8+x^3+x^2+1$
17	$x^{17}+x^3+1$	x^9+x^2
18	$x^{18}+x^8+x^2+x+1$	x^9+x^4+x+1
19	$x^{19}+x^{18}+\ldots+x^{14}+1$	$x^{10}+x^7+1$
20	$x^{20}+x^6+x^4+x+1$	$x^{10}+x^3+x^2+1$
21	$x^{21}+x^{19}+1$	$x^{11}+x^{10}$
22	$x^{22}+x+1$	$x^{11}+1$
23	$x^{23}+x^5+1$	$x^{12}+x^3$
24	$x^{24}+x^{10}+x^6+x+1$	$x^{12}+x^5+x^3+1$
25	$x^{25}+x^3+1$	$x^{13}+x^2$
26	$x^{26}+x^6+x^2+x+1$	$x^{13}+x^3+x+1$
27	$x^{27}+x^9+x^5+x^3+1$	$x^{14}+x^5+x^3+x^2$
28	$x^{28}+x^6+x^4+x+1$	$x^{14}+x^3+x^2+1$
29	$x^{29}+x^{27}+1$	$x^{15}+x^{14}$
30	$x^{30}+x^6+x^4+x+1$	$x^{15}+x^3+x^2+1$
31	$x^{31}+x^3+1$	$x^{16}+x^2$

Tabelle III: Primitive Polynome p(x) mit Grad $w(x) = \lfloor \frac{m+1}{2} \rfloor$		
m	$p(x)$	$w(x)$
32	$x^{32} + x^{14} + x^6 + x + 1$	$x^{16} + x^7 + x^3 + 1$
33	$x^{33} + x^{13} + 1$	$x^{17} + x^7$
34	$x^{34} + x^{30} + x^2 + x + 1$	$x^{17} + x^{15} + x + 1$
35	$x^{35} + x^{33} + 1$	$x^{18} + x^{17}$
36	$x^{36} + x^{14} + x^2 + x + 1$	$x^{18} + x^7 + x + 1$
37	$x^{37} + x^{15} + x^7 + x + 1$	$x^{19} + x^8 + x^4 + x$
38	$x^{38} + x^8 + x^6 + x + 1$	$x^{19} + x^4 + x^3 + 1$
39	$x^{39} + x^{25} + 1$	$x^{20} + x^{13}$
40	$x^{40} + x^{18} + x^{14} + x + 1$	$x^{20} + x^9 + x^7 + 1$
41	$x^{41} + x^3 + 1$	$x^{21} + x^2$
42	$x^{42} + x^{16} + x^{12} + x + 1$	$x^{21} + x^8 + x^6 + 1$
43	$x^{43} + x^{17} + x^9 + x^5 + 1$	$x^{21} + x^9 + x^5 + x^3$
44	$x^{44} + x^{14} + x^{10} + x + 1$	$x^{22} + x^7 + x^5 + 1$
45	$x^{45} + x^{19} + x^7 + x^5 + 1$	$x^{23} + x^{10} + x^4 + x^3$
46	$x^{46} + x^{10} + x^6 + x + 1$	$x^{23} + x^5 + x^3 + 1$
47	$x^{47} + x^5 + 1$	$x^{24} + x^3$
48	$x^{48} + x^{20} + x^{18} + x^{14} + x^4 + x + 1$	$x^{24} + x^{10} + x^9 + x^7 + x^2 + 1$
49	$x^{49} + x^9 + 1$	$x^{25} + x^5$
50	$x^{50} + x^{16} + x^2 + x + 1$	$x^{25} + x^8 + x + 1$
51	$x^{51} + x^{17} + x^5 + x + 1$	$x^{25} + x^9 + x^3 + x$
52	$x^{52} + x^{14} + x^6 + x + 1$	$x^{26} + x^7 + x^3 + 1$
53	$x^{52} + x^{19} + x^{17} + x^{15} + 1$	$x^{27} + x^{10} + x^9 + x^8$
54	$x^{52} + x^{10} + x^8 + x + 1$	$x^{27} + x^5 + x^4 + 1$
55	$x^{55} + x^{31} + 1$	$x^{28} + x^{16}$
56	$x^{56} + x^{22} + x^{14} + x + 1$	$x^{28} + x^{11} + x^7 + 1$
57	$x^{57} + x^7 + 1$	$x^{29} + x^4$
58	$x^{58} + x^{24} + x^{20} + x + 1$	$x^{29} + x^{12} + x^{10} + 1$
59	$x^{59} + x^{25} + x^{17} + x + 1$	$x^{30} + x^{13} + x^9 + x$
60	$x^{60} + x + 1$	$x^{30} + 1$
61	$x^{61} + x^{23} + x^{15} + x^5 + 1$	$x^{30} + x^{12} + x^8 + x^3$
62	$x^{62} + x^{14} + x^{10} + x + 1$	$x^{30} + x^7 + x^5 + 1$
63	$x^{63} + x + 1$	$x^{32} + x$
64	$x^{64} + x^{34} + x^{28} + x + 1$	$x^{32} + x^{17} + x^{14} + 1$

Tabelle IV: Primitive Polynome p(x) für kryptographische Anwendungen		
m	$p(x)$	$w(x)$
163	$x^{163} + x^{57} + x^{49} + x^{29} + 1$	$x^{82} + x^{29} + x^{25} + x^{15}$
233	$x^{233} + x^{159} + 1$	$x^{117} + x^{80}$
239	$x^{239} + x^{81} + 1$	$x^{120} + x^{41}$
283	$x^{283} + x^{141} + x^3 + x + 1$	$x^{142} + x^{71} + x^2 + x$
571	$x^{571} + x^{201} + x^{185} + x^{11} + 1$	$x^{286} + x^{101} + x^{93} + x^6$

Patentansprüche

1. Verfahren und Anordnung zur verbesserten Implementierung von endlichen Körpern in Hard- oder Software, dadurch gekennzeichnet, dass durch Auswahl von bestimmten irreduziblen oder primitiven Polynomen $p(x)$ die Polynome $w(x)$, die quadriert modulo $p(x)$ das Monom x ergeben, ein möglichst kleines Gewicht und einen möglichst kleinen Grad haben.

2. Verfahren nach vorigem Anspruch, dadurch gekennzeichnet, dass bei Körpern der Charakteristik ungleich zwei entsprechende Polynome benutzt werden.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur verbesserten Darstellung von endlichen Körpern, die es ermöglicht, schneller in diesen Körpern Berechnungen durchzuführen durch Bestimmung und Benutzung von geeigneten irreduziblen/primitiven Polynomen, die zu Polynomen $w(x)$ mit geringem Gewicht und möglichst kleinem Grad führen für die gilt $w^2(x) \equiv x \bmod p(x)$. Hierdurch ist es möglich eine ganze Reihe von Berechnungen in endlichen Körpern zu beschleunigen.