BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Verkündet am
11. Juli 2012
…

5 Ni 34/10 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

betreffend das europäische Patent 0 482 154
(DE 591 00 171)

hat der 5. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 11. Juli 2012 durch den Vorsitzenden Richter Gutermuth, die Richterin Martens sowie die Richter Dipl.-Ing. Gottstein, Dipl.-Ing. Kleinschmidt und Dipl.-Geophys. Dr. Wollny

für Recht erkannt:

I. Das europäische Patent 0 482 154 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland teilweise für nichtig erklärt, soweit es über folgende Fassung hinausgeht.

1. Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Digitalblockes einer ersten Länge (N) in einen zugeordneten, zweiten binären Digitalblock gleicher Länge (N) unter Verwendung von wenigstens einem frei wählbaren, binären Steuerblock,

mit wenigstens einem ersten Eingang (25-26; 50, 51; 125-128) zum Eingeben von wenigstens zwei ersten Teilblöcken (X_1-X_4; e_1, e_2; e_5-e_8) einer zweiten Länge (m), die zusammen den ersten Digitalblock (X; W_n) bilden, und

wenigstens einem zweiten Eingang (29, 30, 32, 33, 49, 52, 129, 130, 133) zum Eingeben von wenigstens zwei Steuerblöcken (Z_1-Z_{52}) der zweiten Länge (m), gekennzeichnet

- durch eine primäre Verschlüsselungslogik (40), die jeweils vier logische Operationen zweier unterschiedlicher Sorten (⊞, ⊙) durchführt,
- wobei durch jede Operation jeweils zwei Eingangsblöcke (E_1, E_2) der zweiten Länge (m) in einen Ausgangsblock (A) dieser Länge (m) umgewandelt werden,
- wobei nacheinander durch die erste Operation (41) der eine erste Teilblock mit dem einen Steuerblock (Z_5) nach einer zweiten Sorte (⊙) operiert wird,
- durch die zweite Operation (42) der andere erste Teilblock (e_2) mit dem Ausgangsblock der ersten Operation (41) nach einer ersten Sorte (⊞) operiert wird,
- durch die dritte Operation (43) der Ausgangsblock der zweiten Operation (42) mit dem anderen Steuerblock (Z_6) nach der zweiten Sorte (⊙) operiert wird, und
- durch die vierte Operation (44) der Ausgangsblock der ersten Operation (41) und der Ausgangsblock der dritten Operation (43) nach der ersten Sorte (⊞) operiert wird, wobei

wenigstens ein Ausgang (47, 48) zum Ausgeben von zwei zweiten Teilblöcken (a_1, a_2) vorgesehen ist,

- wobei der eine zweite Teilblock (a_1) der Ausgangsblock der vierten Operation (44) und der andere zweite Teilblock (a_2) der Ausgangsblock der dritten Operation (43)

ist und der eine zweite Teilblock (a_1) und der andere zweite Teilblock (a_2) zusammen den zweiten Digitalblock (W_n, Y) bilden.

2. Vorrichtung nach Anspruch 1,
bei der wenigstens ein erster Eingang (125-128) zum Eingeben von vier ersten Teilblöcken (e_5-e_8) vorgesehen ist,
eine erweiterte Verschlüsselungslogik (140) vorgesehen ist, die eine primäre Verschlüsselungslogik (40) nach Anspruch 1 umfasst und sechs logische Operationen einer dritten Sorte ($\oplus$) durchführt,
- wobei
- durch die erste und zweite Operation (115, 116) der dritten Sorte ($\oplus$) der erste (e_5) mit dem dritten (e_7) und der zweite (e_6) mit dem vierten ersten Teilblock (e_8) operiert werden,
- durch die primäre Verschlüsselungslogik (40) die Ausgangsblöcke der ersten und der zweiten Operation operiert werden,
- durch die dritte (117) und vierte Operation (119) der dritten Sorte ($\oplus$) ein erster Ausgangsblock (a_2) der primären Verschlüsselungslogik (40) mit dem ersten (e_5) bzw. mit dem dritten ersten Teilblock (e_7) operiert wird, und
- durch die fünfte (118) und sechste Operation (120) der dritten Sorte ($\oplus$) ein zweiter Ausgangsblock (a_1) der primären Verschlüsselungslogik (40) mit dem zweiten (e_6) bzw. dem vierten ersten Teilblock (e_8) operiert wird, und
- dass wenigstens ein Ausgang (35-38) zum Ausgeben von vier Teilblöcken (a_5 – a_8) vorgesehen ist,
- wobei der erste (a_5), der zweite (a_6), der dritte (a_7) und der vierte zweite Teilblock (a_8) zugeordnet der Ausgangsblock der dritten, der fünften, der vierten bzw. der sechsten Operation ist.

3. Vorrichtung nach Anspruch 1 und 2,
dadurch gekennzeichnet,
- dass wenigstens ein erster Eingang (25-28) zum Eingeben von vier ersten Teilblöcken (X_1-X_4; W_{n1}-W_{n4}) vorgesehen ist,

- dass wenigstens ein zweiter Eingang (29, 30, 32, 33, 49, 52) zum Eingeben von sechs Steuerblöcken (Z_1-Z_6) vorgesehen ist,
- dass eine Verschlüsselungsstufe (61.1v, 61.2v) vorgesehen ist, die jeweils vierzehn logische Operationen dreier unterschiedlicher Sorten ($\boxplus$, $\odot$, $\oplus$) durchführt,
  - wobei durch die ersten vier Operationen (111, 112, 113, 114) parallel der erste erste (X_1, W_{n1}) und der zweite erste Teilblock (X_2, W_{n2}) zugeordnet mit dem ersten (Z_1) und dem zweiten Steuerblock (Z_2) nach der zweiten Sorte ($\odot$) und der dritte erste (X_3, W_{n3}) und der vierte erste Teilblock (X_4, W_{n4}) zugeordnet mit dem dritten (Z_3) und dem vierten Steuerblock (Z_4) nach der ersten Sorte ($\boxplus$) operiert werden,
  - wobei die weiteren zehn Operationen diejenigen der erweiterten Verschlüsselungslogik (140) von Anspruch 2 sind, und
  - wobei die Ausgangsblöcke (135, 136, 137, 138) der ersten vier Operationen (111, 112, 113, 114) die Eingangsblöcke (125, 126, 127, 128) der erweiterten Verschlüsselungslogik (140) sind, und
- dass wenigstens ein Ausgang (35-38) zum Ausgeben von vier zweiten Teilblöcken (W_{11}-W_{14}; $W_{(n+l)1}$-$W_{(n+l)4}$) vorgesehen ist, die kreuzweise vertauscht den Ausgangsblöcken (a_3, a_6, a_7, a_8) der erweiterten Verschlüsselungslogik (140) entsprechen.

4. Vorrichtung nach Anspruch 1 und 2,
wobei
- wenigstens ein erster Eingang (25-28) zum Eingeben von vier ersten Teilblöcken (X_1-X_4; W_{n1}-W_{n4}) vorgesehen ist,
- dass wenigstens ein zweiter Eingang (29, 30, 32, 33, 49, 52) zum Eingeben von sechs Steuerblöcken (Z_1-Z_6) vorgesehen ist,
- dass eine Verschlüsselungsstufe (61.1v, 61.2v) vorgesehen ist, die jeweils vierzehn logische Operationen (111v, 112v, 113v, 114v) dreier unterschiedlicher Sorten ($\boxplus$, $\odot$, $\oplus$) durchführt,

- wobei durch die ersten vier Operationen parallel der erste erste (X_1, W_{n1}) und der vierte erste Teilblock (X_4, W_{n4}) zugeordnet mit dem ersten (Z_1) und dem dritten Steuerblock (Z_4) nach der zweiten Sorte ($\odot$) und der zweite erste (X_2, W_{n2}) und der dritte erste Teilblock (X_3, W_{n3}) zugeordnet mit dem zweiten (Z_2) und dem dritten Steuerblock (Z_3) nach der ersten Sorte ($\boxplus$) operiert werden,
- wobei die weiteren zehn Operationen diejenigen der erweiterten Verschlüsselungslogik (140) von Anspruch 2 sind, und
- wobei die Ausgangsblöcke (135, 136, 137, 138) der ersten vier Operationen (111v, 112v, 113v, 114v) die Eingangsblöcke (125, 126, 127, 128) der erweiterten Verschlüsselungslogik (140) sind, und
- dass wenigstens ein Ausgang (35-38) zum Ausgeben von vier zweiten Teilblöcken (W_{11}-W_{14}; $W_{(n+l)1}$-$W_{(n+l)4}$) vorgesehen ist,

wobei der erste (35) und der vierte Ausgang (38) direkt und der zweite (36) und der dritte Ausgang (37) kreuzweise vertauscht den Ausgangsblöcken (a_5, a_6, a_7, a_8) der erweiterten Verschlüsselungslogik (140) entsprechen.

5. Vorrichtung nach Anspruch 1 und 3,
dadurch gekennzeichnet,
- dass wenigstens ein erster Eingang (25-28) zum Eingeben von vier ersten Teilblöcken (X_1-X_4) vorgesehen ist,
- dass wenigstens ein zweiter Eingang (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) zum Eingeben einer zweiten Mehrzahl (T) von Steuerblöcken (Z_1-Z_{52}) vorgesehen ist,
- dass eine Verschlüsselungseinheit (60) vorgesehen ist, die eine erste Mehrzahl (S) von gleichen Verschlüsselungsstufen (61.1, 61.2) nach Anspruch 3 umfasst, die so aufeinanderfolgen, dass die Ausgänge der jeweils vorausgehenden Stufe die Eingange der jeweils nachfolgenden Stufe bilden,
- dass die Verschlüsselungseinheit (60) eine abweichende, letzte Verschlüsselungsstufe (69) umfasst, die parallel vier Operationen zweier unterschiedlicher Sorten ($\boxplus$, $\odot$) durchführt, und

- dass wenigstens ein Ausgang (75-78) zum Ausgeben von vier zweiten Teilblöcken (Y_1-Y_4) vorgesehen ist, die den Ausgangsblöcken der abweichenden, letzten Verschlüsselungsstufe (69) entsprechen,
- wobei die zweite Mehrzahl (T) gleich dem sechsfachen der ersten Mehrzahl (S) plus vier ist,
- wobei der erste (W_{n1}) und der zweite Ausgangsblock (W_{n2}) der vorausgehenden, letzten der gleichen Verschlüsselungsstufen (61.1, 61.2) zugeordnet mit dem (T-3)ten und dem (T-2)ten Steuerblock (Z_{49}, Z_{50}) nach der zweiten Sorte (⊙) und der dritte (W_{n3}) und der vierte Ausgangsblock (W_{n4}) der vorausgehenden Stufe mit dem (T-1)ten und dem T-ten Steuerblock (Z_{51}, Z_{52}) nach der ersten Sorte (⊞) operiert werden.

6. Vorrichtung nach Anspruch 1 und 4,
dadurch gekennzeichnet,
- dass wenigstens ein erster Eingang (25-28) zum Eingeben von vier ersten Teilblöcken (X_1-X_4) vorgesehen ist,
- dass wenigstens ein zweiter Eingang (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) zum Eingeben einer zweiten Mehrzahl (T) von Steuerblöcken (Z_1-Z_{52}) vorgesehen ist,
- dass eine Verschlüsselungseinheit (60v) vorgesehen ist, die eine erste Mehrzahl (S) von gleichen Verschlüsselungsstufen (61.lv, 61.2v) nach Anspruch 4 umfasst, die so aufeinanderfolgen, dass die Ausgänge der jeweils vorausgehenden Stufe die Eingänge der jeweils nachfolgenden Stufe bilden,
- dass die Verschlüsselungseinheit (60v) eine abweichende, letzte Verschlüsselungsstufe (69v) umfasst, die parallel vier Operationen zweier unterschiedlicher Sorten (⊞, ⊙) durchführt,
- dass wenigstens ein Ausgang (75-78) zum Ausgeben von vier zweiten Teilblöcken (Y_1-Y_4) vorgesehen ist, die den Ausgangsblöcken der abweichenden, letzten Verschlüsselungsstufe (69v) entsprechen,
- wobei die zweite Mehrzahl (T) gleich dem sechsfachen der ersten Mehrzahl (S) plus vier ist,

- wobei der erste (W_{n1}) und der zweite Ausgangsblock (W_{n2}) der vorausgehenden, letzten der gleichen Verschlüsselungsstufen (61.lv, 61.2v) zugeordnet mit dem (T-3)ten und dem (T-2)ten Steuerblock (Z_{49}, Z_{50}) nach der zweiten Sorte ($\odot$) und der dritte (W_{n3}) und der vierte Ausgangsblock (W_{n4}) der vorausgehenden Stufe mit dem (T-1)ten und dem T-ten Steuerblock (Z_{51}, Z_{52}) nach der ersten Sorte ($\boxplus$) operiert werden, und
- wobei der zweite und der dritte Eingang der abweichenden, letzten Verschlüsselungsstufe (69v) miteinander vertauscht sind.

7. Vorrichtung nach Anspruch 5 oder 6,
dadurch gekennzeichnet,
dass die zweite Mehrzahl (T) gleich zweiundfünfzig und die erste Mehrzahl (S) gleich acht ist.

8. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
- dass die Operation einer ersten Sorte ($\boxplus$, Addition modulo 2^m) so geartet ist,
- dass jeder Eingangsblock (E_1 E_2) der Operation als ganze Zahl in Binärdarstellung und als Element der Menge $\{0, 1, 2, 3 \ldots, (2^m-1)\}$ betrachtet wird, und
- dass der zugeordnete Ausgangsblock (A) die Binärdarstellung der Summe modulo 2^m der Eingangsblöcke (E_1, E_2) ist,
- dass die Operation einer zweiten Sorte ($\odot$, Multiplikation modulo (2^m+1)) so geartet ist,
- dass, sofern alle Bits eines Blockes (E_1, E_2, A) Null sind, dieser Block als die ganze Zahl 2^m in Binärdarstellung betrachtet wird,
- dass ansonsten jeder Eingangsblock (E_1, E_2,) als ganze Zahl in Binärdarstellung und als Element der Menge $\{1, 2, 3, \ldots (2^m-1)\}$ betrachtet wird, und
- dass der jeweilige Ausgangsblock (A) in Binärdarstellung das Produkt modulo (2^m+1) der Eingangsblöcke (E_1, E_2) ist, und
- dass die Operation einer dritten Sorte ($\oplus$, Bit-für-Bit-Exklusiv-ODER) so geartet ist,

- dass jeder Block (E_1, E_2, A) der Operation als Bitfolge betrachtet wird, durch die jedem Bit eine feste Position zugeordnet wird,
- und dass in der durch diese Folge gegebenen Reihenfolge jedes Bit des Ausgangsblocks (A) das Exklusiv-ODER der zwei Bits der jeweils entsprechenden Position der beiden Eingangsblöcke (E_1, E_2) ist.

9. Vorrichtung nach Anspruch 8,
dadurch gekennzeichnet,
dass die zweite Länge (m) entweder vier, acht oder sechzehn ist.

10. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass zur Ausführung jeder einzelnen logischen Operation eine individuell zugeordnete Operationseinheit (41-44, 111-120) vorgesehen ist, die zwei Eingänge zum Eingeben der jeweiligen Eingangsblöcke (E_1, E_2) und einen Ausgang zur Ausgabe des jeweils zugeordneten Ausgangsblockes (A) aufweist.

11. Vorrichtung nach Anspruch 1,
dadurch gekennzeichnet,
dass zur Ausführung der logischen Operationen Operationseinheiten vorgesehen sind, die wenigstens einen gemeinsamen Prozessor umfassen, der die an seinen Eingängen anliegenden Eingangsblöcke entsprechend einem vorgegebenen Programm miteinander verknüpft.

12. Verwendung zweier Vorrichtungen nach Anspruch 5 zum Verschlüsseln eines digitalen Klartextes (X) und zum Entschlüsseln des zugeordneten Chiffriertextes (Y), wobei der Klartext (X) laufend von einer Nachrichtenquelle (11) und der Chiffriertext (Y) von einer Übertragungsleitung (13) abgegeben und blockweise durch eine jeweilige Eingangseinheit (21) den Eingängen (25-28) einer Verschlüsselungseinheit (60) bzw. einer mit dieser identischen Entschlüsselungseinheit als Klartextteilblöcke (X_1-X_4) bzw. Chiffriertextteilblöcke (Y_1-Y_4) einer zweiten Länge (m) zugeführt wird,

wobei zum Verschlüsseln und zum Entschlüsseln ein gemeinsamer, geheimer Schlüsselblock (Z) dient, und

wobei die entstehenden Chiffriertextteilblöcke (Y_1-Y_4) bzw. die Klartextteilblöcke (X_1-X_4) der gleichen zweiten Länge (m) an eine jeweilige Ausgangseinheit (79) abgegeben und von dieser als Chiffriertext (Y) bzw. Klartext (X) laufend ausgegeben wird,

dadurch gekennzeichnet,

- dass aus dem Schlüsselblock (Z) als Steuerblöcke eine zweite Mehrzahl (T) Schlüsselteilblöcke (Z_1-Z_T) bzw. Entschlüsselungsteilblöcke (U_1-U_T) der zweiten Länge (m) gebildet und den Eingängen (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) der Verschlüsselungseinheit (60) bzw. der Entschlüsselungseinheit zugeführt werden, die eine erste Mehrzahl (S) von gleichen, aufeinanderfolgenden Stufen (60.1, 60.2) aufweisen,

derart dass für jede Stufe i der Entschlüsselungseinheit

- ein erster und zweiter Entschlüsselungsteilblock jeder Stufe i (i = 1, 2 . . . (S+l)) gleich sind dem Modulo-(2^m+l)-Multiplikation-Inversen eines jeweils ersten bzw. zweiten Schlüsselteilblockes in der (S-i+2)-ten Stufe der Verschlüsselungseinheit (60),
- ein dritter und vierter Entschlüsselungsteilblock in der i-ten Stufe (i = 1, 2 .... (S+1)) gleich sind dem Negativwert der Modulo-2^m-Addition eines dritten bzw. vierten Schlüsselteilblockes in der (S-i+2)-ten Stufe der Verschlüsselungseinheit (60), und
- ein fünfter und sechster Entschlüsselungsteilblock in der i-ten Stufe (i = 1, 2 ... S) gleich sind dem fünften bzw. sechsten Schlüsselteilblock in der (S-i+l)-ten Stufe der Verschlüsselungseinheit (60).

13. Verwendung zweier Vorrichtungen nach Anspruch 6 zum Verschlüsseln eines digitalen Klartextes (X) und zum Entschlüsseln des zugeordneten Chiffriertextes (Y),

wobei der Klartext (X) laufend von einer Nachrichtenquelle (11) und der Chiffriertext (Y) von einer Übertragungsleitung (13) abgegeben und blockweise durch eine jeweilige Eingangseinheit (21) den Eingängen (25-28) einer Verschlüsselungseinheit (60v) bzw. einer mit dieser identischen Entschlüsselungseinheit als Klartextteilblöcke (X_1-X_4) bzw. Chiffriertextteilblöcke (Y_1-Y_4) einer zweiten Länge (m) zugeführt wird,

wobei zum Verschlüsseln und zum Entschlüsseln ein gemeinsamer, geheimer Schlüsselblock (Z) dient, und

wobei die entstehenden Chiffriertextteilblöcke (Y_1-Y_4) bzw. die Klartextteilblocke (X_1-X_4) der gleichen zweiten Länge (m) an eine jeweilige Ausgangseinheit (79) abgegeben und von dieser als Chiffriertext (Y) bzw. Klartext (X) laufend ausgegeben wird,

dadurch gekennzeichnet,

- dass aus dem Schlüsselblock (Z) als Steuerblöcke eine zweite Mehrzahl (T) Schlüsselteilblöcke (Z_1-Z_T) bzw. Entschlüsselungsteilblöcke (U_1-U_T) der zweiten Länge (m) gebildet und den Eingängen (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) der Verschlüsselungseinheit (60) bzw. der Entschlüsselungseinheit zugeführt werden, die eine erste Mehrzahl (S) von gleichen, aufeinanderfolgenden Stufen (60.lv, 60.2v) aufweisen,

derart dass für jede Stufe i der Entschlüsselungseinheit

- ein erster und vierter Entschlüsselungsteilblock jeder Stufe i (i = 1, 2 . . . . . (S+l)) gleich sind dem Modulo-(2^m+l)-Multiplikation-Inversen eines jeweils ersten bzw. vierten Schlüsselteilblockes in der (S-i+2)-ten Stufe der Verschlüsselungseinheit (60v),
- ein zweiter und dritter Entschlüsselungsteilblock in der i-ten Stufe (i = 2, 3 .... S) gleich sind dem Negativwert der Modulo-2^m-Addition eines dritten bzw. zweiten Schlüsselteilblockes in der (S-i+2)-ten Stufe der Verschlüsselungseinheit (60v),
- ein zweiter und dritter Entschlüsselungsteilblock in der ersten und (S+l)-ten Stufe gleich sind dem Negativwert der Modulo-2^m-Addition eines zweiten und dritten Schlüsselteilblockes in der (S+l)-ten bzw. der ersten Stufe der Verschlüsselungseinheit (60v), und
- ein fünfter und sechster Entschlüsselungsteilblock in der i-ten Stufe (i = 1, 2 ... S) gleich sind dem fünften bzw. sechsten Schlüsselteilblock in der (S-i+l)-ten Stufe der Verschlüsselungseinheit (60v).

14. Verwendung nach Anspruch 12 oder 13,

dadurch gekennzeichnet,

dass die Schlüsselteilblöcke (Z_1-Z_T) dadurch gewonnen werden,

- dass in einem ersten Schritt der Schlüsselblock (Z) in acht erste Schlüsselteilblöcke (Z_1-Z_8) der zweiten Länge (m) unterteilt wird,
- dass in einem zweiten Schritt die Bits des Schlüsselblockes (Z) zyklisch um eine vorgegebene Bitzahl verschoben werden und der hierbei gebildete neue Block in acht weitere Schlüsselteilblöcke (Z_9-Z_{16}) unterteilt wird, und
- dass der zweite Schritt solange wiederholt wird, bis alle Schlüsselteilblöcke (Z_1-Z_T) gebildet sind.

15. Verwendung nach Anspruch 12 oder 13,
dadurch gekennzeichnet,
dass die zweite Mehrzahl (T) zweiundfünfzig ist,
dass die erste Mehrzahl (S) acht ist, und
dass die zweite Länge (m) sechzehn ist.

II. Im Übrigen wird die Klage abgewiesen.

III. Die Klägerin trägt 1/3, die Beklagte 2/3 der Kosten des Rechtsstreits.

IV. Das Urteil ist gegen Sicherheitsleistung in Höhe von 120 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

Die Beklagte war eingetragene Inhaberin des am 16. Mai 1991 angemeldeten und zwischenzeitlich durch Zeitablauf erloschenen europäischen Patents 0 482 154, das auch mit Wirkung für die Bundesrepublik Deutschland erteilt wurde und in der maßgeblichen Verfahrenssprache die Bezeichnung „Vorrichtung für das Umwandeln eines Digitalblockes und Verwendung derselben“ trägt. Das Streitpatent nimmt die Priorität der schweizerischen Patentanmeldung CH 1690/90 vom

18. Mai 1990 in Anspruch und wird beim Deutschen Patent- und Markenamt unter der Nummer DE 591 00 171 geführt. Es umfasst 17 Patentansprüche, die alle mit der Nichtigkeitsklage angegriffen sind.

Der Vorrichtungsanspruch 1 lautet in der erteilten Fassung wie folgt:

1. Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Digitalblockes einer ersten Länge (N) in einen zugeordneten, zweiten binären Digitalblock gleicher Länge (N) unter Verwendung von wenigstens einem frei wählbaren, binären Steuerblock,
gekennzeichnet

- durch wenigstens einen ersten Eingang (25-26; 50, 51; 125-128) zum Eingeben von wenigsten zwei ersten Teilblöcken (X_1-X_4; e_1, e_2; e_5-e_8) einer zweiten Länge (m), die zusammen den ersten Digitalblock (X; W_n) bilden,
- durch wenigstens einen zweiten Eingang (29, 30, 32, 33, 99, 52, 129, 130, 133) zum Eingeben von wenigsten zwei Steuerblöcken (Z_1-Z_{52}) der zweiten Länge (m),
- durch eine Logik (90, 60, 61.1, 61.2, 140), die jeweils nacheinander wenigstens vier logische Operationen wenigstens zweier unterschiedlicher Sorten ($\boxplus$, $\odot$, $\oplus$) durchführt,
  - wobei wenigstens die überwiegende Zahl aller Paare unmittelbar aufeinanderfolgender Operationen aus zwei Operationen unterschiedlicher Sorten ($\boxplus$,

⊙, ⊕) besteht,

- wobei durch jede Operation jeweils zwei Eingangsblöcke (E_1, E_2) der zweiten Länge (m) in einen Ausgangsblock (A) dieser Länge (m) umgewandelt werden,
- wobei als Eingangsblöcke (E_1, E_2) erste Teilblöcke (X_1-X_4; e_1, e_2; e_5-e_8), Steuerblöcke (Z_1-Z_{52}) und/oder Ausgangsblöcke (A) einer jeweils vorhergehenden Operation dienen, und

- durch wenigstens einen Ausgang (75-78; 47, 48; 35-38) zum Ausgeben von wenigstens zwei, den ersten Teilblöcken (X_1-X_4 ; e_1, e_2; e_5-e_8) zugeordneten, zweiten Teilblöcken (W_{n1}-W_{n4}, Y_1-Y_4; a_1, a_2; a_5-a_8) der zweiten Länge (m), die zusammen den zweiten Digitalblock (W_n, Y) bilden.

Wegen der auf Patentanspruch 1 zurückbezogenen Unteransprüche 2 bis 13 sowie der nebengeordneten Patentansprüche 14 und 15 und der auf diese zurückbezogenen Unteransprüche 16 und 17 wird auf die Streitpatentschrift EP 0 482 154 B1 Bezug genommen.

Mit ihrer Nichtigkeitsklage macht die Klägerin geltend, den unter Schutz gestellten Gegenständen des Streitpatents fehle die Patentfähigkeit. Wegen der Zulässigkeit der Klage nach Erlöschen des Schutzrechts beruft sich die Klägerin auf ihr fortdauerndes Rechtsschutzbedürfnis gegen eine drohende Inanspruchnahme durch die Beklagte. Zwar habe diese den gegen sie gestellten Antrag auf Erlass einer einstweiligen Verfügung wegen Verletzung des Streitpatents vor dem Landgericht Düsseldorf zurückgenommen, nicht jedoch auf die Geltendmachung von Rechten gegenüber der Klägerin oder deren Abnehmer aus dem abgelaufenen Streitpatent für die Vergangenheit verzichtet.

Die Klägerin stützt ihr Vorbringen auf folgende Dokumente:

N1 EP 0 221 538 A2
N2 DE 25 58 206 A1
N3 DE 32 28 018 C2
N4 DE 22 31 849 A
N5 DE 39 24 226 A1
N6 DE 38 32 946 A1
N7 DE 38 27 172 A1
N8 DE 35 01 178 A1
N9 DE 35 24 472 C2
N10 DE 36 31 992 C2
N11 DE 34 27 286 A1
N12 DE 33 23 268 A1
N13 DE 28 55 787 A1
N14 DE 28 49 718 C2
N15 DE 28 45 828 A1
N16 DE 27 50 329 A1
N17 EP 0 482 154 B1 (Streitpatent)
N18 Merkmalsgliederung des Anspruchs 1 Streitpatent
N19 Antrag auf Erlass einer einstweiligen Verfügung vom 9. Juni 2010
N20 US 5 214 703 mit Merkmalsgegenüberstellung
N21 Figur: Inhaltsgleiche Veränderung
N22 Figur: Patentgemäßer Aufbau - Allgemein
N23 Figur: Patentgemäßer Aufbau - Konkretisiert
N24 Figur: Patentgemäßer Aufbau - umgezeichnet
N25 Figur: Funktion der Figur 7 gemäß EP 0 221 538 A2
N26 Gegenüberstellung Patentanspruch 1 des Streitpatents / Druckschrift N2
N27 Gegenüberstellung Patentanspruch 1 des Streitpatents / Druckschrift N3
N28 Wikipedia: Verschlüsselung
N29 Gegenüberstellung Patentanspruch 1 des Streitpatents / Druckschrift N4
N30 Wikipedia: Division mit Rest.

Die Klägerin beantragt,

> das europäische Patent 0 482 154 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig zu erklären.

Die Beklagte beantragt,

> das Streitpatent im Umfange des Hilfsantrags I vom 15. Februar 2012 aufrecht zu erhalten und die weitergehende Klage abzuweisen.

Hilfsweise verteidigt sie das Streitpatent mit der Fassung des Hilfsantrages II vom 15. Februar 2012.

Patentanspruch 1 in der nunmehr verteidigten Fassung, eingereicht mit Schriftsatz vom 15. Februar 2012 als Hilfsantrag I, lautet wie folgt:

1. Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Digitalblockes einer ersten Länge (N) in einen zugeordneten, zweiten binären Digitalblock gleicher Länge (N) unter Verwendung von wenigstens einem frei wählbaren, binären Steuerblock,
mit wenigstens einem ersten Eingang (25-26; 50, 51; 125-128) zum Eingeben von wenigstens zwei ersten Teilblöcken (X_1-X_4; e_1, e_2; e_5-e_8) einer zweiten Länge (m), die zusammen den ersten Digitalblock (X; W_n) bilden, und

wenigstens einem zweiten Eingang (29, 30, 32, 33, 49, 52, 129, 130, 133) zum Eingeben von wenigstens zwei Steuerblöcken (Z_1-Z_{52}) der zweiten Länge (m), gekennzeichnet

- durch eine primäre Verschlüsselungslogik (40), die jeweils vier logische Operationen zweier unterschiedlicher Sorten (⊞, ⊙) durchführt,
- wobei durch jede Operation jeweils zwei Eingangsblöcke (E_1, E_2) der zweiten Länge (m) in einen Ausgangsblock (A) dieser Länge (m) umgewandelt werden,
- wobei nacheinander durch die erste Operation (41) der eine erste Teilblock mit dem einen Steuerblock (Z_5) nach einer zweiten Sorte (⊙) operiert wird,
- durch die zweite Operation (42) der andere erste Teilblock (e_2) mit dem Ausgangsblock der ersten Operation (41) nach einer ersten Sorte (⊞) operiert wird,
- durch die dritte Operation (43) der Ausgangsblock der zweiten Operation (42) mit dem anderen Steuerblock (Z_6) nach der zweiten Sorte (⊙) operiert wird, und
- durch die vierte Operation (44) der Ausgangsblock der ersten Operation (41) und der Ausgangsblock der dritten Operation (43) nach der ersten Sorte (⊞) operiert wird, wobei

wenigstens ein Ausgang (47, 48) zum Ausgeben von zwei zweiten Teilblöcken (a_1, a_2) vorgesehen ist,

- wobei der eine zweite Teilblock (a_1) der Ausgangsblock der vierten Operation (44) und der andere zweite Teilblock (a_2) der Ausgangsblock der dritten Operation (43)

ist und der eine zweite Teilblock (a_1) und der andere zweite Teilblock (a_2) zusammen den zweiten Digitalblock (W_n, Y) bilden.

Wegen der Patentansprüche 2 bis 15 wird auf die Anlage zum Schriftsatz der Beklagten vom 15. Februar 2012 Bezug genommen.

Die Beklagte tritt den Ausführungen der Klägerin in allen Punkten entgegen und hält den Gegenstand des Streitpatents in den beschränkt verteidigten Fassungen für patentfähig.

Zur Ergänzung des Tatbestands wird im Übrigen auf die gewechselten Schriftsätze samt Anlagen sowie auf den Hinweis des Senats vom 23. April 2012 Bezug genommen.

Entscheidungsgründe

I.

1. Die Nichtigkeitsklage bleibt auch nach Erlöschen des Streitpatents infolge des Ablaufs der Schutzdauer zulässig, denn die Klägerin stützt ihr fortdauerndes Rechtsschutzinteresse an der Vernichtung des Streitpatents für die Vergangenheit zu Recht auf die Gefahr, von der Beklagten trotz Rücknahme des Antrags auf Erlass einer einstweiligen Verfügung für die Zeit vor dem Erlöschen des Schutzrechts aus diesem noch in Anspruch genommen zu werden. Ein dementsprechendes Vorgehen hat sich die Beklagte in der mündlichen Verhandlung auch ausdrücklich vorbehalten.

2. Das Streitpatent ist ohne Weiteres in dem Umfang für nichtig zu erklären, in dem die Beklagte die erteilte Fassung nicht mehr verteidigt und eine zulässige Beschränkung vorliegt, vgl. unten II 4a (BGH, Urteil vom 19. Dezember 2006 - X ZR 236/01, GRUR 2007, 404 - Carvedilol II).

3. Im Übrigen hat die Klage, mit der der in Artikel II § 6 Absatz 1 Nr. 1 IntPatÜG, Artikel 138 Absatz 1 lit. a EPÜ iVm Artikel 54 Absatz 1, 2 und Artikel 56 EPÜ vorgesehene Nichtigkeitsgrund der mangelnden Patentfähigkeit geltend gemacht wird, keinen Erfolg, da das Streitpatent im aus dem Tenor ersichtlichen Umfang Bestand hat. Diese Fassung entspricht dem mit Schriftsatz vom 15. Februar 2012 als Hilfsantrag I vorgelegten Anspruchssatz mit 2 handschriftlich eingefügten Korrekturen offensichtlicher Unrichtigkeiten (vgl. Patentansprüche 5 und 8).

II.

1. Das Streitpatent betrifft eine Vorrichtung für das blockweise Umwandeln eines ersten Digitalblockes in einen zweiten Digitalblock und eine Verwendung dieser Vorrichtung zum Verschlüsseln eines binären Klartextes und/oder zum Entschlüsseln eines binären chiffrierten Textes im Rahmen einer bezüglich der Datensicherheit verbesserten Ver- und Entschlüsselungsprozedur, wie sie beispielsweise im Rahmen des so genannten sicheren Datenverkehrs in Telekommunikationsnetzen zum Einsatz kommt. Hierzu erläutert die Patentschrift, dass zum Zeitpunkt der Anmeldung weltweit in Übertragungsnetzen ein symmetrischer Verschlüsselungsalgorithmus mit der Bezeichnung Data Encryption Standard (DES) im Einsatz sei. Zwar gelte dieser Standard als sehr gutes Verschlüsselungswerkzeug, jedoch sei es eine offen diskutierte Frage, ob der Verschlüsselungsalgorithmus seit seiner Einführung nicht unsicher geworden sei, wobei die relativ geringe Länge des Geheimschlüssels eine wichtige Rolle spiele, denn bei einer frei wählbaren Schlüssellänge von 56 Bit weise er nur eine Gesamtlänge von 64 Bit auf. Daher stelle sich die Aufgabe, ein gegenüber den bekannten Methoden, wie dem DES, verbessertes Blockverschlüsselungsverfahren zu entwickeln, das als europäischer Standard einführbar wäre und das die bekannten Verschlüsselungstechniken der Verwirrung (confusion) und Durchmischung (diffusion) ausnütze und vor allem einen längeren Geheimschlüssel verwende (vgl. **N17**, Spalte 1, Absätze 1, 2 und 6).

Zur Lösung dieser Aufgabe geht das Streitpatent explizit vom DES-Standard aus (vergleiche hierzu die Signalführung im Rahmen der Figur 3 des Streitpatents), verwendet einen längeren Geheimschlüssel (z. B. von insgesamt 128 Bit Schlüssellänge; **N17**, Spalte 3, Zeile 40 und 44) und verknüpft den Eingangsdatenblock mit dem Schlüssel, jedoch in anderer Weise als der DES-Standard. Dies führt beispielsweise am Ende des dergestalt durchgeführten Verschlüsselungsprozesses zu einem resultierenden Chiffriertextdatenblock mit einem höheren Grad der Verschlüsselung, als dies für einen Prozess gemäß DES-Standard der Fall wäre.

2. Der Gegenstand des Streitpatents richtet sich aufgrund der Komplexität der in diesem Zusammenhang durchzuführenden kryptographischen Schritte an einen Diplomingenieur der Nachrichtentechnik oder Informatik mit Universitätsabschluss, der eine mehrjährige Berufserfahrung auf dem Gebiet der Entwicklung und des Einsatzes kryptographischer Methoden in Telekommunikationsnetzen besitzt.

3. Ausgehend vom Fach- und Erfahrungswissen dieses Fachmanns legt der Senat den in den Anspruchsfassungen enthaltenen Begrifflichkeiten jeweils folgendes Verständnis zu Grunde:

Unter einem Digitalblock versteht der Fachmann eine binäre Datenmenge vorgegebener Größe / Länge, z. B. von 64 Bit. Der Digitalblock kann entweder unverschlüsselt als so genannter Klartextblock vorliegen, der chiffriert werden soll, oder bereits verschlüsselt als so genannter Chiffriertextblock, der entschlüsselt werden soll. Jeder Digitalblock wird vor seiner weiteren Behandlung gemäß Streitpatent in mindestens zwei so genannte Teilblöcke gleicher Länge zerlegt, was bei obiger beispielhafter Annahme von 64 Bit für den Digitalblock und einer hälftigen Teilung desselben zu Teilblöcken von jeweils 32 Bit führt.

Die Ver- oder Entschlüsselung der Digitalblöcke erfolgt hierbei in einer Verschlüsselungs-/Entschlüsselungseinheit unter Verwendung eines geheimen binären Schlüsselblocks, der durch eine Schlüsselquelle bereitgestellt und auf einem sicheren Kanal der jeweiligen Einheit zugeführt wird. Ein derartiger Kanal wird durch eine datentechnisch sichere Leitung zwischen der Schlüsselquelle und der Verschlüsselungs-/Entschlüsselungseinheit realisiert.

Aus dem Schlüsselblock wiederum werden für den Verschlüsselungsprozess einzelne Schlüsselteilblöcke und beim Entschlüsselungsprozess einzelne Entschlüsselungsteilblöcke abgeleitet, die als so genannte Steuerblöcke den eigentlichen Ver-/Entschlüsselungsprozess steuern, indem sie mit einem ihnen im weiteren Prozessverlauf zugeordneten Datenpaket korreliert werden. Dazu weisen die Steuerblöcke dieselbe Länge auf wie dieses Datenpaket, beispielsweise ein Teil-

block des Digitalblocks, der seiner ersten Verschlüsselungs- oder Entschlüsselungsoperation zugeführt wird, d. h. gemäß obigem Beispiel ebenfalls 32 Bit.

Die diesen Prozessen / Operationen zuzuführenden binären Datenpakete, seien es zu ver-/entschlüsselnde Daten oder Schlüsselteilblöcke, werden aus der Perspektive des Verfahrensablaufs auch als Eingangsblöcke, die Resultate dieser Prozesse aus derselben Perspektive auch als Ausgangsblöcke bezeichnet.

Die der eigentlichen Ver- und Entschlüsselung zugrundeliegenden Operationen werden unter dem Begriff der logischen Operationen zusammengefasst, die von so genannten Operationseinheiten durchgeführt werden. Diese Operationen bestehen darin, jeweils zwei Eingangsblöcke bestimmter Länge zu einem Ausgangsblock derselben Länge zusammenzufügen, wobei dies mittels dreier unterschiedlicher Sorten von logischen Operationen durchgeführt werden kann. Diese Sorten von logischen Operationen unterscheiden sich jeweils durch die mathematische Vorschrift, mit der aus den einzelnen Bits der jeweiligen beiden Eingangsblöcke die einzelnen Bits des jeweils resultierenden einen Ausgangsblocks gewonnen werden.

Die konkrete Abfolge aller Sorten von logischen Operationen und die hierfür notwendige Festlegung der diesen zuzuweisenden und zu operierenden Teilblöcke im Rahmen eines Ver-/Entschlüsselungsprozesses wird unter dem Begriff Logik zusammengefasst. Diese Logik kann aus mehreren aufeinanderfolgenden einzelnen Logiken aufgebaut sein, wie beispielsweise aus einem Kernbaustein, der als primäre Verschlüsselungslogik bezeichnet wird und die Logik des bekannten DES-Standards widerspiegelt, sowie weiteren Logiken, die auf diesem Kernbaustein aufbauen und diesen zu einer erweiterten Verschlüsselungslogik ausbauen.

4. Die Patentinhaberin verteidigt das Streitpatent in erster Linie mit einem Anspruch 1, der wie folgt gegliedert werden kann:

1.1 Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Datenblockes einer ersten Länge in einen zugeordneten, zweiten binären Datenblock gleicher Länge unter Verwendung von wenigstens einem frei wählbaren, binären Steuerblock,

1.2 mit wenigstens einem ersten Eingang zum Eingeben von wenigstens zwei ersten Teilblöcken einer zweiten Länge, die zusammen den ersten Digitalblock bilden, und

1.3 mit wenigstens einem zweiten Eingang zum Eingeben von wenigsten zwei Steuerblöcken der zweiten Länge,

gekennzeichnet

1.4a durch eine primäre Verschlüsselungslogik, die jeweils vier logische Operationen zweier unterschiedlicher Sorten durchführt,

1.4b wobei durch jede Operation jeweils zwei Eingangsblöcke der zweiten Länge in einen Ausgangsblock dieser Länge umgewandelt werden, wobei nacheinander

1.4c durch die erste Operation der eine erste Teilblock mit dem einen Steuerblock nach einer zweiten Sorte operiert wird

1.4d durch die zweite Operation der andere erste Teilblock mit dem Ausgangsblock der ersten Operation nach einer ersten Sorte operiert wird, und

1.4e durch die dritte Operation der Ausgangsblock der zweiten Operation mit dem anderen Steuerblock nach der zweiten Sorte operiert wird, und

1.4f durch die vierte Operation der Ausgangsblock der ersten Operation und der Ausgangsblock der dritten Operation nach der ersten Sorte operiert wird,

1.5 wobei wenigstens ein Ausgang zum Ausgeben von wenigstens zwei zweiten Teilblöcken vorgesehen ist,

1.6 wobei der eine zweite Teilblock der Ausgangsblock der vierten Operation und der andere zweite Teilblock der Ausgangsblock der dritten Operation ist und der eine zweite Teilblock und der andere zweite Teilblock zusammen den zweiten Digitalblock bilden.

a) Der Anspruch 1 der verteidigten Fassung erweist sich als zulässig.

Er setzt sich im Wesentlichen aus der Kombination des Oberbegriffs des Anspruchs 1 gemäß Streitpatent (Merkmale 1.1 bis 1.3), eines kennzeichnenden Merkmals dieses Anspruchs 1 (Merkmal 1.4b) und des Kennzeichens des Anspruchs 2 gemäß Streitpatent (Merkmale 1.4a, 1.4c bis 1.4f, 1.5, 1.6) zusammen.

Soweit die Klägerin in der geltenden Fassung von Patentanspruch 1 infolge Wegfalls und Umformulierung von Merkmalen eine unzulässige Erweiterung des Schutzbereichs des Streitpatents (Art. 138 Abs. 1 lit. d) EPÜ) sieht, kommt der Senat nach eingehender Würdigung zum gegenteiligen Ergebnis:

Anstelle des im erteilten Anspruch 1 enthaltenen Merkmals, dass von einem allgemein als „Logik“ bezeichneten Vorrichtungsbestandteil „jeweils nacheinander wenigstens vier logische Operationen durchführt" werden, die jedoch nicht weiter spezifiziert sind, wird im verteidigten Anspruch 1 zulässigerweise eine einschränkende Formulierung gewählt, die Anzahl, Art und Reihenfolge der genannten Operationen, sowie den hierfür zur Anwendung kommenden Vorrichtungsbestandteil konkretisiert (Merkmale 1.4a, 1.4c bis 1.4f). Im Einzelnen werden nur noch genau vier logische Operationen zweier bestimmter Sorten - in der Reihenfolge zweite-erste-zweite-erste Sorte - von einem speziellen Bestandteil dieser „Logik“, nämlich der „primären Verschlüsselungslogik“, durchgeführt, was auch von Anspruch 1 gemäß Streitpatent ursprünglich umfasst war.

Durch die konkrete Beanspruchung von Anzahl, Art und Reihenfolge der logischen Operationen gemäß den Merkmalen 1.4c bis 1.4f wird das einen breiteren Schutzumfang aufweisende Merkmal des erteilten Anspruchs 1, dass „die überwiegende Zahl aller Paare unmittelbar aufeinanderfolgender Operationen aus zwei Operationen unterschiedlicher Sorten besteht" (im Kontext der ursprünglich beanspruchten „wenigstens vier logischen Operationen“; Unterstreichungen jeweils hinzugefügt) im verteidigten Anspruch 1 entbehrlich, da als Teilmenge hiervon nur noch vorher erfasste Paare im Rahmen von genau vier Operationen beansprucht werden, in denen die Operationsreihenfolge zweite-erste-zweite-erste Sorte verwirklicht ist. Eine unzulässige Erweiterung ist mit dem Weglassen dieses Merkmals folglich gerade nicht verbunden.

Durch die verarbeitungstechnische Verschaltung gemäß Anspruch 1 des Hauptantrags, die durch die Kausalkette der Merkmale 1.4b bis 1.4f sowie 1.5 und das im zweiten Teil neu formulierte Merkmal 1.6 vorgegeben ist, ist auch das Merkmal „wobei als Eingangsblöcke erste Teilblöcke, Steuerblöcke und/oder Ausgangsblöcke einer jeweils vorhergehenden Operation dienen“ entbehrlich, denn dieses wiederholt den durch die genannten Merkmale bereits beschriebenen Verarbeitungsvorgang nur in allgemeinerer Form durch andere Ausdrücke.

Auch das Teilmerkmal, dass die beanspruchte Vorrichtung gekennzeichnet sei „durch wenigstens einen Ausgang zum Ausgeben von wenigstens zwei, den ersten Teilblöcken zugeordneten, zweiten Teilblöcken der zweiten Länge“, konnte ohne Gefahr einer unzulässigen Erweiterung wegfallen, da ein derartiger Ausgang in Merkmal 1.5 und die Längendefinition der Teilblöcke in Merkmal 1.6 im Kontext mit den gegenüber dem erteilten Anspruch 1 redaktionell angepassten Merkmalen 1.1 bis 1.3 im Anspruch 1 des Hauptantrags bereits beschrieben sind.

Der Anspruch 1 gemäß Hauptantrag stellt folglich im Vergleich zum Anspruch 1 gemäß Streitpatent nun einen Vorrichtungsanspruch dar, der durch die Konkretisierung ursprünglich allgemein gehaltener Funktionsangaben der Vorrichtung mittels detaillierter Angaben zum Ablauf des Ver-/ Entschlüsselungsprozesses und

der hierfür zum Einsatz kommenden Baugruppen, beschränkt wird. Der Sachgehalt des Anspruchs 1 gemäß Hauptantrag war im erteilten Anspruch 1 als Teilmenge bereits enthalten. Die vorgenommenen Änderungen waren ursprünglich offenbart und führen nicht zum Verlassen des ursprünglichen Schutzumfangs des Streitpatents.

b) Der mit dem geltenden Patentanspruch 1 verteidigte Gegenstand gilt als neu und beruht auch auf einer erfinderischen Tätigkeit, da dieser, wie nachfolgend dargelegt, dem Fachmann durch den entgegengehaltenen Stand der Technik nicht nahe gelegt ist

Die Druckschrift EP 0 221 538 A2 (**N1**) beschäftigt sich, wie der Patentgegenstand, mit einer Weiterentwicklung des DES-Standards und beschreibt eine Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Digitalblockes („input data“) einer ersten Länge („16 Bit“) in einen zugeordneten zweiten binären Digitalblock gleicher Länge („output“) unter Verwendung wenigstens eines frei wählbaren Steuerblocks („parameter“) (Figur 7, Spalte 8, Zeilen 6 bis 41), wobei wenigstens ein erster Eingang zum Eingeben von wenigstens zwei ersten Teilblöcken („R1, R2“) einer zweiten Länge („8 Bit“) existiert, die zusammen den ersten Digitalblock („16 Bit“) bilden (Merkmale **1.1, 1.2**). Darüber hinaus existiert auch wenigstens ein zweiter Eingang zum Eingeben von wenigstens zwei Steuerblöcken („P0, P1“) der zweiten Länge („8 Bit“) (Merkmal **1.3**).

Des Weiteren ist eine Logik vorgesehen, die jeweils vier logische Operationen zweier unterschiedlicher Sorten („+ mod 256“, Bezugszeichen 29 bzw. 33, i. V. m. „BIT CIR“, Bezugszeichen 30 bzw. 34, als zweite Sorte; „EOR circuit“, Bezugszeichen 63 und 64, als erste Sorte) durchführt (Spalte 8, Zeilen 30 bis 37 i. V. m. Figur 7; Merkmal **1.4a**), wobei durch jede Operation jeweils zwei Eingangsblöcke der zweiten Länge („8 Bit“) in einen Ausgangsblock dieser Länge („8 Bit“) umgewandelt werden (z. B. Figur 7, Bezugszeichen R1, R2, P0, P1, i. V. m. Spalte 8, Zeilen 38 bis 41; Merkmal **1.4b**) und wobei zunächst nacheinander durch die erste Operation der eine erste Teilblock mit dem einen Steuerblock nach einer zweiten

Sorte („+ mod 256“, Bezugszeichen 29 bzw. 33 i. V. m. „BIT CIR“, Bezugszeichen 30 bzw. 34) bearbeitet wird (Signalverlauf in Figur 7; Merkmal **1.4c**) und durch die zweite Operation der andere erste Teilblock mit dem Ausgangsblock der ersten Operation nach einer ersten Sorte („EOR circuit“, Bezugszeichen 63 und 64) bearbeitet wird (Signalverlauf in Figur 7; Merkmal **1.4d**). Aus der Druckschrift N1 ist auch bekannt, dass durch die dritte Operation der Ausgangsblock der zweiten Operation mit dem anderen Steuerblock nach der zweiten Sorte („+ mod 256“, Bezugszeichen 29 bzw. 33 i. V. m. „BIT CIR“, Bezugszeichen 30 bzw.34) bearbeitet wird (Signalverlauf in Figur 7; Merkmal **1.4e**). Explizit nicht zu entnehmen ist der Druckschrift N1 jedoch, dass - wie beim Streitgegenstand in Merkmal 1.4f vorgesehen - durch die vierte Operation der Ausgangsblock der ersten Operation und der Ausgangsblock der dritten Operation nach der ersten Sorte bearbeitet wird; vielmehr wird mit der dortigen vierten Operation darauf abgestellt, den ersten Teilblock mit dem Ausgangsblock der dritten Operation zu bearbeiten (Signalverlauf in Figur 7).

Wiederum zu entnehmen ist dieser Druckschrift in Spalte 8, Zeilen 38 bis 41, dass zweite Teilblöcke (jeweils zu „8 Bit“), über einen Ausgang ausgegeben werden können („16 Bit output data“ i. V. m. Figur 7, Merkmal **1.5**).

Ein weiterer Unterschied zu dem mit Anspruch 1 gemäß Hauptantrag beanspruchten Gegenstand besteht in Folge des in der Druckschrift N1 nicht verwirklichten Merkmals 1.4f darin, dass zwar der eine zweite Teilblock der Ausgangsblock der vierten Operation ist, der andere zweite Teilblock jedoch der Ausgangsblock der zweiten und nicht der dritten Operation ist. Beide Teilblöcke des Ausgangsblockes bilden aber auch im Rahmen der Druckschrift N1 gemeinsam den zweiten Digitalblock („16 Bit“, Spalte 8, Zeile 38 bis 41, Merkmal **1.6$_{tlw}$**).

Die im verteidigten Anspruch 1 beanspruchte Bearbeitung der Datenblöcke im Rahmen der vierten Operation stellt somit gegenüber der Druckschrift N1 einen neuen Gegenstand dar. Im Gegensatz zur Auffassung der Klägerin sieht der Senat hierin auch einen erfindungsbegründenden Unterschied zum Stand der Tech-

nik und zum fachmännischen Vorgehen des maßgeblichen Fachmanns. Zwar mag der Fachmann, wie die Klägerin zu Recht in der mündlichen Verhandlung angemerkt hat, sich durchaus in Kenntnis der Druckschrift N1 und des dortigen Vorsehens von vier unmittelbar hintereinander auszuführenden Operationen in einem Ver-/Entschlüsselungsprozess aus einer Fülle von logischen Operationen die für seine Zwecke seiner Ansicht nach sinnvollsten aussuchen und verschalten. Jedoch vermag er nach Überzeugung des Senats die mit dem Anspruch 1 gemäß Hauptantrag beanspruchte konkrete Verschaltung der Operationen, die auf eine Optimierung der Verschlüsselungsleistung hin ausgerichtet ist, nicht durch eine beliebige quasi-willkürliche fachmännische Vorgehensweise zu erreichen, sondern es bedarf seinerseits eines analytischen und auf erfinderischen Maßnahmen beruhenden Vorgehens, um zu einer - wie hier beanspruchten - zielgerichteten Verbesserung des bis dahin üblichen DES-Verschlüsselungsalgorithmus zu gelangen.

Insbesondere hat der Fachmann zum Zeitpunkt der Anmeldung weder aus dem Stand der Technik noch aus seinem Fachwissen heraus eine Anregung erhalten, eine Verschaltung zu entwickeln, in der beide Ausgangsblöcke, die sich nach der vierten Operation im Rahmen des verteidigten Anspruchs 1 ergeben, mathematische Funktionen aller Steuer- und Eingangsblöcke sind und nicht nur, wie sich aus dem Signalverlauf in der Figur 7 der Druckschrift N1 ergibt, nur einer der beiden Ausgangsblöcke. Der andere weist nämlich lediglich eine Abhängigkeit von drei der möglichen vier Eingangsblöcke (d. h. der zwei Teilblöcke des Digitalblocks und der zwei Schlüsselteilblöcke) auf. Durch diese kryptographische Maßnahme wird zielgerichtet ein höherer Grad der Verschlüsselung verwirklicht, als durch die Druckschrift N1 vorgegeben wird, ohne dass diese eine Anregung für den Fachmann bietet, so vorzugehen, wie im Anspruch 1 gemäß Hauptantrag beschrieben.

Der Anspruch 1 in der verteidigten Fassung ist somit neu und erfinderisch im Hinblick auf die Druckschrift N1.

Die Druckschrift DE 25 58 206 A1 (**N2**) offenbart eine Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Datenblockes einer ersten Länge (64 Bit) in einen zugeordneten zweiten binären Datenblock gleicher Länge (64 Bit) unter Verwendung von wenigstens einem frei wählbaren Steuerblock („Chiffrierschlüssel“ mit 64 Bit; Seite 5, Absatz 2; Seite 10, Absatz 1, Seite 6, Absatz 2, Zeilen 3 bis 9, Merkmal **1.1**). Wie im weiteren beschrieben, können auch durch den wenigstens einen ersten Eingang Teilblöcke einer zweiten Länge (8 x 8 Aufteilung, also 8 Bit gemäß Seite 5, Absatz 2, Zeile 4 bzw. 32 Bit-Splittung gemäß Seite 5, Absatz 2, Zeile 10 bis Seite 6, Absatz 1 i. V. m. Figur 2) eingegeben werden, die zusammen den ersten Digitalblock bilden (Figur 8 i. V. m. Seite 6, Zeilen 2 bis 4; Merkmal **1.2**). Es ist auch vorgesehen, wie beispielsweise der Figur 2 entnommen werden kann, über wenigstens einen zweiten Eingang (vgl. linker oberer Bereich der Figur 2) Steuerblöcke ausgehend von einem Chiffrierschlüssel mit 64 Bit in einem „externen Register 299“ über ein „oberes Schlüsselregister (UKR) 350“ und ein „niederes Schlüsselregister (LKR) 400“ einzugeben. Jedoch besitzen diese nicht die zweite Länge von 32 Bit, wie die Datenblöcke es bedingen würden, die im „oberen Eingangspuffer (UIB) 100“ und im niederen Eingangspuffer (LIB) 150“ der „Chiffriereinrichtung“ zur Ver-/Entschlüsselung bereitgestellt werden, sondern sie weisen lediglich eine Länge von 28 Bit auf, wie sich aus Seite 6, Absatz 2, Zeilen 11 bis 15 ergibt. Damit ist das Grundprinzip des Streitpatents nicht verwirklicht, nämlich zu ver-/entschlüsselnde Datenblöcke, respektive Teilblöcke einer bestimmten zweiten Länge mit einem Steuerblock derselben zweiten Länge zu bearbeiten (Merkmal **1.3$_{tlw}$**). Folglich kann auch die konkrete Umsetzung der Ver-/Entschlüsselung, wie durch die Merkmale 1.4a bis 1.4f beschrieben, dieser Druckschrift nicht wesensgleich entnommen werden, da laut ihren Verarbeitungsvorschriften zwar zwei Sorten logischer Operationen durchgeführt werden, nämlich mittels der Addierer modulo 2^m und der als Permutation bezeichneten Operation, jedoch die Verarbeitung der Blöcke im Einzelnen (vgl. Signalwege 4, 6, 24 und 32 in der Figur 2; Figur 8) denselben nicht entspricht. Insbesondere durchläuft, wie die Figur 2 zeigt, ein Teilblock des zu ver-/entschlüsselnden Datenblocks insgesamt maximal nur drei Operationen, nämlich eine Addition modulo 2^m, die von einer Permutationsoperation gefolgt wird und mit einer weiteren Operation des Ad-

dierers modulo 2^m als Ver-/Entschlüsselungsmaßnahme abschließt (Merkmale 1.4a bis 1.4f, nicht offenbart). Als direkte Folge hiervon kann die Druckschrift N2 auch die konkrete Zusammensetzung des als Endresultat der Operationen ausgegebenen Digitalblocks nicht in der beanspruchten Form wiedergeben oder einen Hinweis dafür liefern, dass dieser in der beanspruchten Form des Merkmals 1.6 zusammenzusetzen und auszugeben ist. Bei dieser Sachlage ist es letztlich unerheblich, dass auch in der Druckschrift N2 ein Ausgang zum Ausgeben zweiter Teilblöcke vorgesehen ist (z. B. Seite 10, Zeilen 13 bis 15; Merkmal **1.5**), da diese Druckschrift die wesentlichen Teilmerkmale der beanspruchten kryptographischen Signalverarbeitung weder lehrt noch anregt und in Folge ein solches Vorgehen auch nicht nahe legt.

Die Druckschrift DE 32 28 018 C2 (**N3**) liegt weiter ab als die beiden vorgenannten Druckschriften. Lässt man dahingestellt, dass diese nicht vom symmetrischen DES-Standard, sondern vom asymmetrischen RSA-Verfahren ausgeht und beabsichtigt, dieses zu verbessern, ist lediglich eine Vorrichtung für das Umwandeln jeweils eines beliebigen ersten binären Datenblockes (z. B. „M-Register“ / „M ist ein gewöhnlicher Text“, Seite 5, Zeile 6) einer ersten Länge (512 Bit) in einen zugeordneten zweiten binären Datenblock gleicher Länge unter Verwendung von wenigstens einem frei wählbaren Steuerblock bekannt. Wie in der Figur 3 rechts gezeigt, wird über die drei Eingänge, die durch die Eingangssignalleitungen 28_1, 28_2 und 28_3 repräsentiert werden, der zu verschlüsselnde Digitalblock M nicht aufgeteilt übertragen und etwa in zwei Teilblöcke separiert in die Schaltung eingespeist. Auch die zwei Steuerblöcke e und n (jeweils 512 Bit) werden als Ganzes über diese Leitungen der weiteren Nutzung zugeführt. Eine Unterteilung des zu verschlüsselnden Datenblocks M und auch der hierfür nötigen Steuerblöcke e und n findet erst durch die Ablage in den Registern 1_1 bis 1_8, 2_1 bis 2_8und 3_1 bis 3_8 in Teilblöcken von jeweils 64 Bit statt, die von der Schaltung selbst vorgenommen wird (Figur 3 i. V. m. Seite 12, Zeilen 3 bis 12).

Ein Eingeben von wenigstens zwei ersten Teilblöcken des zu verschlüsselnden Datenblocks mit einer zweiten Länge und der hierzu jeweils zugeordneten Steuer-

blöcke derselben Länge, wie es die Merkmale 1.2 und 1.3 des Anspruchs 1 fordern, ist folglich in der Druckschrift N3 nicht realisiert. Da somit für die Ver-/ Entschlüsselung gemäß Anspruch 1 gegenüber der Lehre der Druckschrift N3 ganz andere Ausgangsbedingungen gelten, ergibt sich ein für die weitere Signalverarbeitung so maßgeblicher Unterschied, dass ein etwaiges Vorhandensein der übrigen Merkmale in der Druckschrift N3 die Neuheit insgesamt unberührt ließe. Bei der konkreten Umsetzung der beanspruchten kryptographischen Schritte nach den Merkmalen 1.4a bis 1.4f und 1.6 des Anspruchs 1 sind, wie auch den Signalverläufen in den Figuren 3 und 15 entnommen werden kann, auch diese weiteren Merkmale bei N3 nicht verwirklicht.

Zu diesem Ergebnis gelangt man auch bei Betrachtung der Druckschrift DE 22 31 849 (**N4**), die nach Ansicht des Senats noch weiter abliegt, als die bisher behandelten Druckschriften. Insbesondere werden auch hier nicht die in den Merkmalen 1.4a bis 1.4f und 1.6 des Anspruchs 1 genannten kryptographischen Schritte in der konkret beanspruchten Ausgestaltung verwirklicht.

Auch die Druckschrift DE 33 23 268 A1 (**N12**), zu der die Klägerin erst im Rahmen der mündlichen Verhandlung substantiiert vorgetragen hat, nimmt den Gegenstand des Anspruchs 1 weder vorweg, noch legt sie ihn nahe. Zwar wird im Zusammenhang mit Figur 5 als mögliches Einsatzgebiet der in dieser Druckschrift vorgestellten Verschlüsselungstechnik das Umfeld des DES-Standards thematisiert, jedoch ist auch dort an keiner Stelle ein Vorgehen gezeigt, wie es in den Ver-/Entschlüsselungsoperationen der Merkmale 1.4a bis 1.4f und 1.6 des Anspruchs 1 beschrieben wird.

Die weiteren Druckschriften **N5 bis N11** und **N13 bis N16** kommen dem Streitgegenstand zur Überzeugung des Senats nicht näher als die Vorgenannten und haben daher in der mündlichen Verhandlung keine Rolle gespielt.

c) Die im Rahmen der verteidigten Fassung beanspruchten Vorrichtungsansprüche 2 bis 11 und die nebengeordneten, auf mindestens einen der Vorrichtungsan-

sprüche rückbezogenen Verwendungsansprüche 12 und 13 - mit auf diese rückbezogenen Unteransprüchen 14 und 15 - sind nach Überzeugung des Senats ebenfalls zulässig.

Die Änderungen im geltenden Anspruchssatz ergeben sich durch Anpassungen der ursprünglich erteilten Ansprüche an die verteidigte Fassung des Patentanspruchs 1 und Umnummerierungen sowie daraus folgender Änderungen der Rückbezüge. Diese Änderungen werden von der ursprünglichen Offenbarung umfasst und führen auch nicht zu einer Erweiterung des Schutzbereichs, wobei insoweit auf die Ausführungen oben unter 4a verwiesen wird.

Die genannten Ansprüche sind auch patentfähig. Soweit es sich um untergeordnete Vorrichtungsansprüche handelt, werden sie von der Schutzfähigkeit des verteidigten Patentanspruchs 1 mitgetragen. Nachdem die Verwendungsansprüche (Patentansprüche 12 und 13) alle Merkmale der schutzfähigen Ansprüche aufweisen, auf die sie rückbezogen sind, bestehen auch insoweit keine Zweifel an der Patentfähigkeit.

5. Eines Eingehens auf den Hilfsantrag bedarf es unter diesen Umständen nicht.

III.

Die Kostenentscheidung beruht auf § 84 Abs. 2 PatG i. V. m. § 92 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit auf § 99 Abs. 1 PatG i. V. m. § 709 Satz 1 und 2 ZPO.

Gutermuth Martens Gottstein Kleinschmidt Dr. Wollny

Ko