(19) Deutsches Patent- und Markenamt

(10) **DE 10 2004 039 899 B4** 2010.07.22

(12) # Patentschrift

(21) Aktenzeichen: **10 2004 039 899.2**
(22) Anmeldetag: **17.08.2004**
(43) Offenlegungstag: **20.04.2006**
(45) Veröffentlichungstag
der Patenterteilung: **22.07.2010**

(51) Int Cl.[8]: ***H04L 9/22*** (2006.01)

(73) Patentinhaber:
Korobkov, Dimitri, Prof. Dr.-Ing., 60322 Frankfurt, DE; Scheja, Katharina, Dr., 65812 Bad Soden, DE

(74) Vertreter:
MERH-IP Matias Erny Reichl Hoffmann, 80336 München

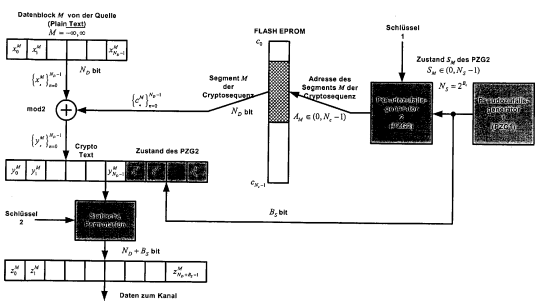
(72) Erfinder:
Korobkov, Dimitri, Prof. Dr.-Ing., 60322 Frankfurt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	**35 18 462**	**A1**
GB	**23 69 800**	**A**
US	**2003/00 26 429**	**A1**
US	**2002/00 02 675**	**A1**
US	**64 45 794**	**B1**
US	**54 40 640**	**A**
US	**48 53 962**	**A**

(54) Bezeichnung: **Verschlüsselungsverfahren**

(57) Hauptanspruch: Verfahren zur Verschlüsselung und/oder Entschlüsselung eines digitalen Datenstroms für die Kommunikation von Kommunikationsgeräten, die eine Schnittstelle für ein austauschbares oder beschreibbares Speichermedium haben, dessen Inhalt auslesbar und duplizierbar ist, wobei auf dem Speichermedium, das mit der Schnittstelle in Verbindung steht, ein Vorrat an Symbolen zur Verschlüsselung abgelegt ist, die anhand einer Adresse auslesbar sind, wobei das Verfahren die Schritte umfasst:
– Erzeugen einer pseudozufälligen Adresse in einem ersten Pseudozufallsgenerator (PZG2) anhand eines Anfangszustands;
– Auslesen eines Symbols aus dem Vorrat an Symbolen an der pseudozufälligen Adresse;
– Verschlüsseln und/oder Entschlüsseln des digitalen Datenstroms der Kommunikationsgeräte auf der Basis des ausgelesenen Symbols;
wobei der Anfangszustand des Pseudozufallsgenerators (PZG2) zur Synchronisation übertragen wird.



Beschreibung

[0001] Die Erfindung betrifft eine Vorrichtung und ein Verfahren zur Verschlüsselung einer digitalen Kommunikation. Insbesondere betrifft die Erfindung ein Verfahren zur Bereitstellung vor Schlüsseln in einem symmetrischen Verschlüsselungsverfahren.

Gebiet der Erfindung:

[0002] Nach Shannon [1, 2] lässt sich die Sicherheit eines Verschlüsselungssystems darstellen als bedingte Entropie der unverschlüsselten Datenfolge, bei bekannter verschlüsselter Datenfolge.

[0003] Die bedingte Entropie kann höchstens so groß sein wie die Länge der zufälligen Schlüsselfolge (Crypto Sequenz) [3].

[0004] Als Folge ist die theoretisch vollkommene Verschlüsselung nur dann zu erreichen, wenn die Schlüsselfolge mindestens so groß ist wie die Datenfolge.

[0005] Hierbei ist die Crypto Sequenz zufällig mit gleichwahrscheinlichen Symbolen und hat die gleiche Länge wie die Datenfolge (Plain Text). Jede Crypto Sequenz wird nur ein einziges Mal verwendet (One Time Pad).

[0006] Der Nachteil an diesem Ansatz ist, dass die vollkommene Verschlüsselung eine sehr lange Schlüsselfolge erfordert.

[0007] In der Praxis wird bislang eine pseudozufällige Crypto Sequenz mit einem Verschlüsselungsautomaten (Cypher) generiert. Zur Erzeugung der pseudozufälligen Crypto Sequenz werden Anfangszustand des Verschlüsselungsautomaten und eine Schlüsselfolge benötigt. Anfangszustand und Schlüsselfolge müssen sowohl beim Verschlüsseln als auch beim Entschlüsseln bekannt sein. In der Regel ist die Schlüsselfolge viel kürzer als die daraus generierte pseudozufällige Crypto Sequenz.

[0008] Die Patentanmeldung US 2002/0002675 A1 beschreibt die Verwendung von one time pads für mobile Telekommunikation. Die Patentanmeldung DE3518462A1 beschreibt die Verschlüsselung von Daten anhand von periodisch wiederkehrender Pseudo-Noise-Folgen. Die Patentanmeldung US 2003/0026429 A1 beschreibt ein one time pad Verschlüsselungssystem. Das US Patent US 6,445,794 B1 beschreibt ein Verfahren zur Generierung von identischen one time pads an verschiedenen Orten.

Überblick über die Erfindung:

[0009] Aufgabe der vorliegenden Erfindung ist es, ein Verfahren und eine Vorrichtung bereitzustellen, die bei einer Kommunikation, wie einer mobilen Kommunikation, eine möglichst optimale Verschlüsselung ermöglicht.

[0010] Diese Aufgabe wird durch die Erfindungen mit den Merkmalen der unabhängigen Ansprüche gelöst. Vorteilhafte Weiterbildungen der Erfindungen sind in den Unteransprüchen gekennzeichnet.

[0011] Im erfindungsgemäßen Verfahren wird die zufällige Crypto Sequenz nicht in einem Verschlüsselungsautomaten erzeugt, sondern aus einem Vorrat gleichwahrscheinlicher Symbole entnommen, die vorzugsweise in einem FLASH-EPROM abgelegt wurden oder auch auf einer FLASH-CARD bzw. einem FLASH-Speicher abgelegt sind. Andere kleine Speichermodule, die unempfindlich sind und in portablen Kommunikationsgeräten eingesetzt werden können, sind ebenfalls denkbar, wie Minidisks oder sehr kleine Festplatten. Holografische Speicher oder Nanospeicherelemente sind ebenfalls denkbar, soweit sie mobil eingesetzt werden können. Da es sich um ein symmetrisches Verfahren handelt, sollte der Inhalt des FLASH-EPROM für Verschlüsselung und Entschlüsselung identisch sein. Somit werden für die Kommunikation zweier Geräte zwei Kopien des FLASH-EPROMs angelegt. Sollten noch mehr Teilnehmer an der Kommunikation teilnehmen (z. B. Polizeifunk), so sind entsprechend viele Kopien bereitzustellen.

[0012] Der Vorrat an entnommener zufälliger Crypto Sequenz vom Speichermedium hat die gleiche Länge wie die zu verschlüsselnde Datenfolge. Damit wird die theoretisch vollkommene Verschlüsselung nach Shannon erreicht.

[0013] Für die Ver- und Entschlüsselung sollte die Anfangsadresse der entnommenen Crypto Sequenz bekannt sein.

[0014] Beim Stand der Technik und somit in konventionellen Verfahren erfolgt eine Synchronisation der Ver- und Entschlüsselung durch Übertragung des Anfangszustandes des Verschlüsselungsautomaten (Cyphers).

[0015] Im erfindungsgemäßen Verfahren, das z. B. Zugriff auf einer großen FLASH-Speicher hat, wird zur Synchronisation die Anfangsadresse der Leseoperation mit übertragen.

[0016] Bei sequentieller Abarbeitung des FLASH-Inhaltes kennzeichnet die Anfangsadresse die Grenze zwischen verbrauchter und unverbrauchter Crypto Sequenz

[0017] In einer weiteren Ausführungsform kann anstelle eines sequentiellen Auslesens des FLASH-Inhaltes ein Auslesen an pseudozufälligen Adressen

durchgeführt werden. Die pseudozufälligen Adressen werden in einem Pseudozufallsgenerator (PZG) anhand eines Anfangszustandes und eines Schlüssels erzeugt. Eine Mehrfachnutzung des FLASH-Inhaltes wird ermöglicht, kann jedoch im Einzelfall auch vermieden werden.

[0018] Zur Synchronisation der Ver- und Entschlüsselung wird in der weiteren Ausführungsform des Verfahrens der Anfangszustand des Pseudozufallsgenerator (PZG) mit übertragen.

[0019] In einer weiteren Ausführungsform, dem so genannten „Fire and Forget"-Verfahren, wird eine Information in Blöcken übermittelt, ohne ein Gedächtnis an vorausgegangene Blöcke.

[0020] Der Empfänger muss anhand eines einzigen empfangenen Blockes in der Lage sein, zu synchronisieren und die Information zu rekonstruieren.

[0021] Im konventionellen Verfahren muss hierbei in jedem Block in einer Präambel der Zustand des Cyphers mit übertragen werden. In der Regel ist die hierzu benötigte Redundanz sehr hoch.

[0022] Im erfindungsgemäßen Verfahren wird in jedem Block in einer Präambel der Zustand des Pseudozufallsgenerators mit übertragen. In der Regel ist die hierzu benötigte Redundanz wesentlich geringer.

[0023] In noch einer weiteren Ausführungsform kann anstelle eines sequentiellen Auslesens des FLASH-Inhaltes ein Auslesen an pseudozufälligen Adressen durchgeführt werden. Die pseudozufälligen Adressen werden in einem Pseudozufallsgenerator (PZG) anhand eines Anfangszustandes und eines Schlüssels erzeugt. Eine Mehrfachnutzung des FLASH-Inhaltes wird ermöglicht.

[0024] Zur Synchronisation wird hierbei anstatt der Adresse der Zustand des PZGs übertragen.

[0025] In einer weiteren alternativen Ausführungsform wird zusätzlich eine Permutation der Daten vorgenommen, um die Positionen der Synchroninformation (Zustand des PZG) zu verstecken.

[0026] Im Folgenden wird die Erfindung anhand von Ausführungsbeispielen näher erläutert, die in den Figuren schematisch dargestellt sind. Gleiche Bezugsziffern in den einzelnen Figuren bezeichnen dabei gleiche Elemente. Im Einzelnen zeigt:

[0027] Fig. 1a, Fig. 1b und Fig. 1c zeigen eine symmetrische Verschlüsselung auf der Basis der Mod2-Operation, wobei ein Cypher die zufällige Crypto Sequenz erzeugt und eine Synchronisation auf der Basis des Anfangszustandes des Cyphers erfolgt;

[0028] Fig. 2a, Fig. 2b und Fig. 2c zeigen das Verfahren auf der Basis der vorliegenden Erfindung, wobei die Symbole aus dem Flash-Eprom verwendet werden, um eine Verschlüsselung durchzuführen; hierbei wird als Anfangszustand die Anfangsadresse übertragen, um dann schließlich diese Adresse voran zuschieben, so dass ein verbrauchter und ein unverbrauchter Bereich entstehen;

[0029] Fig. 3a und Fig. 3b zeigen das erfindungsgemäße Verfahren in einer alternativen Ausführungsform, wobei durch einen Pseudozufallsgenerator (PZG), dessen Zustand anfänglich übertragen wird, die Adresse bestimmt wird, aus der das Symbol vom Speichermedium Flash-Eprom zu lesen ist;

[0030] Fig. 4a und Fig. 4b zeigen Abwandlungen der Verfahren aus den **Fig.** 1 und 3, wobei in regelmäßigen Abständen Synchronisationsinformationen des Chyphers bzw. des PZGs übertragen werden;

[0031] Fig. 5 zeigt den Datenfluss bei einer bevorzugten Ausführungsform, die eine Verschlüsselung vornimmt;

[0032] Fig. 6 zeigt den Datenfluss bei einer bevorzugten Ausführungsform, die eine Entschlüsselung der in Fig. 5 verschlüsselten Daten vornimmt.

[0033] Wie bereits in der Einleitung erwähnt, beschreiben die Fig. 1a bis Fig. 1c ein Verfahren, wie es aus dem Stand der Technik bekannt ist. Ein Chyper (Zufallsgenerator) erzeugt hierbei eine Sequenz, mit der die Daten durch eine Mod2-Operation verschlüsselt werden. Da der Chyper deterministisch ist, kann aufgrund des Zustandes die zukünftige Datenfolge bestimmt werden, wodurch eine Übertragung des Anfangszustandes möglich ist oder, wie aus Fig. 4a ersichtlich ist, eine wiederholte Übertragung des Zustandes eine Synchronisation erlaubt.

[0034] Den Fig. 2a bis Fig. 2c ist die erfindungsgemäße Ausführungsform zu entnehmen. Hierbei werden die Symbole zur Verschlüsselung nicht durch einen Zufallsgenerator erzeugt, sondern liegen auf einem Speicher ab. Aufgrund der Größe der Flash-Speicher kann somit ein kompletter Datenstrom verschlüsselt werden. Anstatt des Zustandes des Chypers wird die Adresse auf dem Speichermedium übertragen.

[0035] Im Folgenden wird ein Beispiel zur Dauer der verschlüsselten Übertragungszeit in Abhängigkeit der FLASH-Größe aufgezeigt. Gegeben sei ein FLASH-EPROM der Größe $N_C = 2^{33}$ bit = 2 GByte Für die Adressierung dieser Speichergröße werden L_C = 33 bit benötigt.

[0036] Angenommen eine digitalisierte Sprachinformation wird mit einer Datenrate R_{VC} = 2400 bit/s über-

tragen, wie es z. B. im GSM-Bereich oder im digitalen Funk der Fall ist, so kann bei einmaligem Auslesen des gesamten FLASH-Inhaltes (OTP: one time pad), d. h. ohne Wiederverwendung einzelner Segmente, eine Gesamtdauer von

$$T_{OTP} = \frac{N_C}{R_{VC}} = 994.2 Stunden = 41.4 Tage$$

verschlüsselt übertragen werden. Da es sich hierbei um eine Netto-Zeit handelt, ist ein Speichermedium für die Verschlüsselung mehr als einen Monat bei sicherer Verschlüsselung einsetzbar. Erst dann sind die Speichermedien aller Beteiligten neu zu beschreiben bzw. zu initialisieren.

[0037] Die **Fig.** 3 zeigt eine weitere Ausführungsform der vorliegenden Erfindung. Bei diesem Ansatz erzeugt ein Zufallsgenerator die Adresse für die Speicherkarte. Anstatt die Anfangsadresse der Karte oder die aktuelle Adresse (**Fig. 4b**) zu übertragen, wird der Zustand des PZGs übertragen. Dadurch ist selbst im Falle des Verlustes einer Karte nicht unmittelbar ein Abhören möglich, da der Zufallsgenerator die Adressen nicht linear bestimmt. Für die Synchronisation wird, wie aus **Fig. 4b** deutlich wird, immer wieder der Zustand des Zufallsgenerators übertragen.

[0038] Nimmt man an, dass ein Vocoder die zu übertragenden Symbole in Rahmen (Frames) der Dauer 20 ms zusammenfasst und dass die Datenrate des Vocoders R_{VC} = 2000 bit/s sei, sodass in einen Rahmen ND = 40 bit übertragen werden. Für die Übertragung der Synchronisationsinformation würden BS = 14 bit zu Verfügung stehen. Hieraus ergibt sich, dass sich $N_S = 2^{B_S}$ = 16384 Segmente der Crypto Sequenz mit einer Länge von je 40 bit adressieren lassen. Dies entspricht der Anzahl der Zustände des Pseudozufallsgenerators.

[0039] Die **Fig. 5** und **Fig. 6** zeigen eine weitere Ausführungsform der vorliegenden Erfindung. Zusätzlich zu den Permutationen der Informationen, bevor sie gesendet werden, wird ein zweiter Zufallsgenerator (PZG1) eingesetzt. PZG1 dient zur Verwürfelung des Zugriffs auf einzelne Segmente der Crypto Sequenz, wenn PZG2 die konkreten Adressen o. g. Segmente bestimmt. Der Zustand des ersten Zufallsgenerators wird genauso im Crypto Text abgelegt wie die verschlüsselten Informationen, die mit den Symbolen an der Adresse des durch den PZG2 bestimmten Bereichs verschlüsselt wurden. Bei der Entschlüsselung wird der Zufallsgenerator anhand des übertragenen Zustandes synchronisiert, um dann das korrekte Segment von der bestimmten Adresse der Speicherkarte zu lesen, auf dessen Basis die Rücktransformation stattfindet. Anschließend wird die Permutation rückgängig gemacht.

Liste der zitierten Literatur:

[1] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J., vol. 27., Part 1. pp. 379–423, Part 2. pp. 623–656, 1948.
[2] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28., pp. 565–715, 1949.
[3] J. L. Massey, An introduction to contemporary cryptology, Proc. IEEE, vol. 76, pp. 533–549, May 1988.

Patentansprüche

1. Verfahren zur Verschlüsselung und/oder Entschlüsselung eines digitalen Datenstroms für die Kommunikation von Kommunikationsgeräten, die eine Schnittstelle für ein austauschbares oder beschreibbares Speichermedium haben, dessen Inhalt auslesbar und duplizierbar ist, wobei auf dem Speichermedium, das mit der Schnittstelle in Verbindung steht, ein Vorrat an Symbolen zur Verschlüsselung abgelegt ist, die anhand einer Adresse auslesbar sind, wobei das Verfahren die Schritte umfasst:
– Erzeugen einer pseudozufälligen Adresse in einem ersten Pseudozufallsgenerator (PZG2) anhand eines Anfangszustands;
– Auslesen eines Symbols aus dem Vorrat an Symbolen an der pseudozufälligen Adresse;
– Verschlüsseln und/oder Entschlüsseln des digitalen Datenstroms der Kommunikationsgeräte auf der Basis des ausgelesenen Symbols;
wobei der Anfangszustand des Pseudozufallsgenerators (PZG2) zur Synchronisation übertragen wird.

2. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, dass die Symbole auf dem Speichermedium nur einmalig verwendet werden und somit ”aufgebraucht” werden.

3. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Symbole mit dem Datenstrom mit Mod2 verschlüsselt und entschlüsselt werden.

4. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich bei dem Kommunikationsgerät um ein Funkgerät, Laptop, PDA und/oder ein mobiles Telefon handelt, die eine Schnittstelle für eine Speicherkarte aufweisen, die unempfindlich sind und in portablen Kommunikationsgeräten eingesetzt werden können.

5. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Speichermedium eine Flash-Speicherkarte, eine Festplatte und/oder eine optische Speicherplatte ist, deren Informationen adressierbar sind.

6. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche dadurch gekennzeichnet, dass ein zweiter Zufallsgenerator (PZG1) vorhanden ist, der eine Verwürfelung des Zugriffs auf einzelne Segmente vornimmt, wenn PZG2 die konkreten Adressen der Segmente bestimmt.

7. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Permutation der digitalen Daten vorgenommen wird, bevor sie übertragen werden.

8. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Speichermedium durch das Rauschen einer analogen Quelle unter Verwendung eines A/D-Konverters beschrieben wird.

9. Kommunikationsgerät, das einen digitalen Datenstrom verschlüsselt,
– mit einer Schnittstelle für ein austauschbares oder beschreibbares Speichermedium, dessen Inhalt auslesbar und duplizierbar ist, wobei auf dem Speichermedium, das mit der Schnittstelle in Verbindung bringbar ist, ein Vorrat an Symbolen zur Verschlüsselung abgelegt ist, die durch Verwendung einer Adresse gelesen werden können,
– mit einer Verschlüsselungseinheit, die so eingerichtet ist, dass sie den Vorrat an Symbolen für die Verschlüsselung und/oder Entschlüsselung des digitalen Datenstroms der Kommunikationsgeräte verwendet, indem durch Adressen auf diesen zugegriffen wird,
– mit einem ersten Zufallsgenerator (PZG2), der anhand eines Anfangszustands die Bestimmung der Adresse auf dem Speichermedium vornimmt, wobei zur Synchronisation der Verschlüsselung der Anfangszustand des Zufallsgenerators übertragen wird.

10. Kommunikationsgerät nach dem vorhergehenden Kommunikationsgeräteanspruch, gekennzeichnet durch eine Einrichtung, die die Symbole auf dem Speichermedium nur einmalig verwendet.

11. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, gekennzeichnet durch ein Rechenwerk, das die Symbole mit dem Datenstrom mit Mod2 verschlüsselt oder entschlüsselt.

12. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass es sich um ein Funkgerät, Laptop, PDA und/oder ein mobiles Telefon handelt, die eine Schnittstelle für eine Speicherkarte aufweisen, wobei die Speicherkarte unempfindlich ist und in portablen Kommunikationsgeräten einsetzbar ist.

13. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass das Speichermedium eine Flash-Speicherkarte, eine Festplatte und/oder eine optische Speicherplatte ist, deren Informationen adressierbar sind.

14. Kommunikationsgerät nach dem vorhergehenden Anspruch, gekennzeichnet durch Mittel, durch die in bestimmten Abständen der Zustand des Zufallsgenerators übertragen wird.

15. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass ein zweiter Zufallsgenerator (PZG1) vorhanden ist, der eine Verwürfelung des Zugriffs auf einzelne Segmente vornimmt, wenn PZG2 die konkreten Adressen der Segmente bestimmt.

16. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, gekennzeichnet durch Mittel, die eine Permutation der digitalen Daten vornehmen, bevor die Daten übertragen werden.

17. Kommunikationsgerät nach einem oder mehreren der vorhergehenden Kommunikationsgeräteansprüche, dadurch gekennzeichnet, dass das Speichermedium durch das Rauschen einer analogen Quelle unter Verwendung eines A/D-Konverters beschrieben ist.

18. Software für ein Kommunikationsgerät, wie ein mobiles Endgerät, gekennzeichnet durch die Implementierung eines Verfahren nach einem oder mehreren der vorhergehenden Verfahrensansprüche.

19. Datenträger für einen Computer, gekennzeichnet durch die Speicherung einer Software nach dem vorhergehenden Softwareanspruch.

20. Computersystem mit einer Kommunikationsschnittstelle, gekennzeichnet durch eine Einrichtung, die den Ablauf eines Verfahrens nach einem oder mehreren der vorhergehenden Verfahrensansprüche erlaubt.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

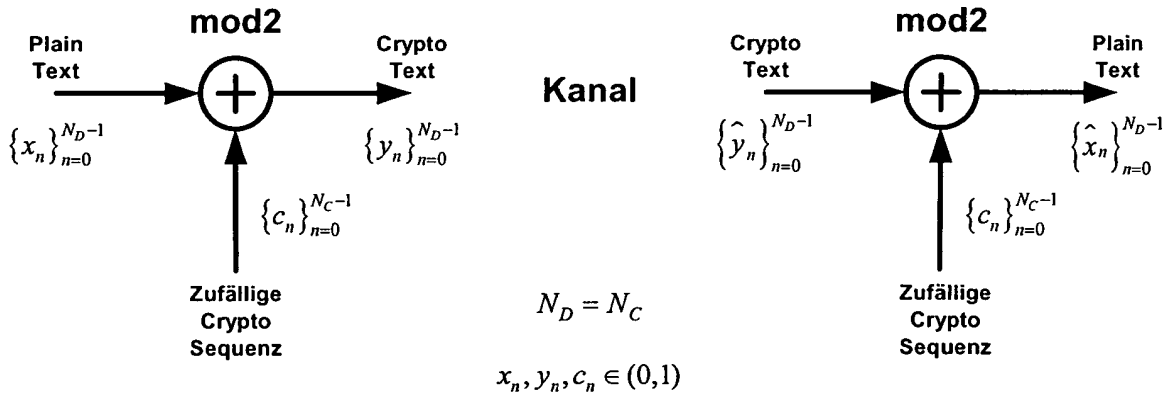


Fig. 1a (Stand der Technik)

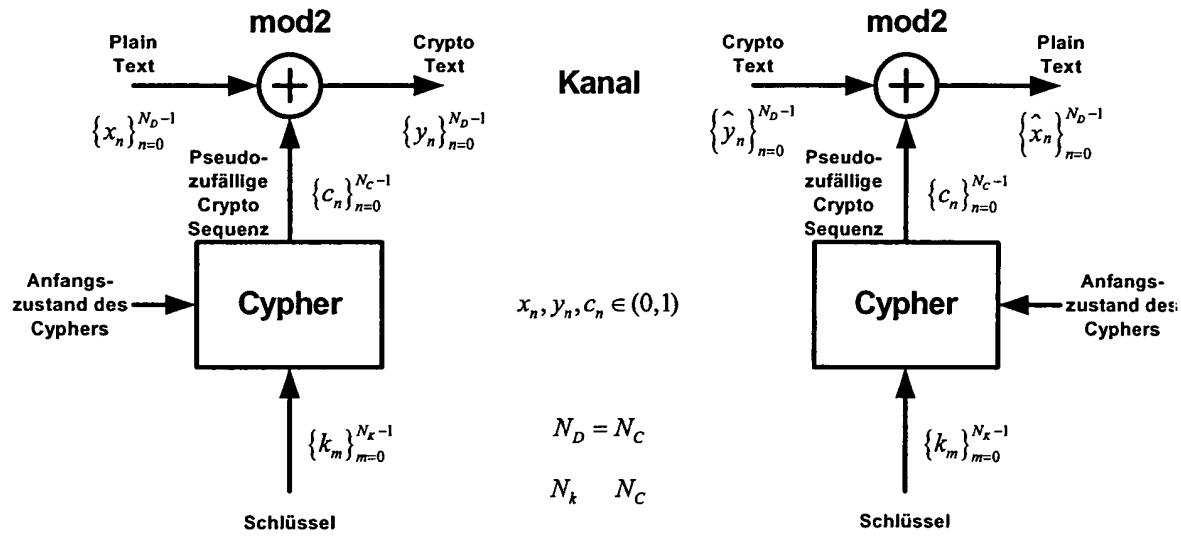


Fig. 1b (Stand der Technik)

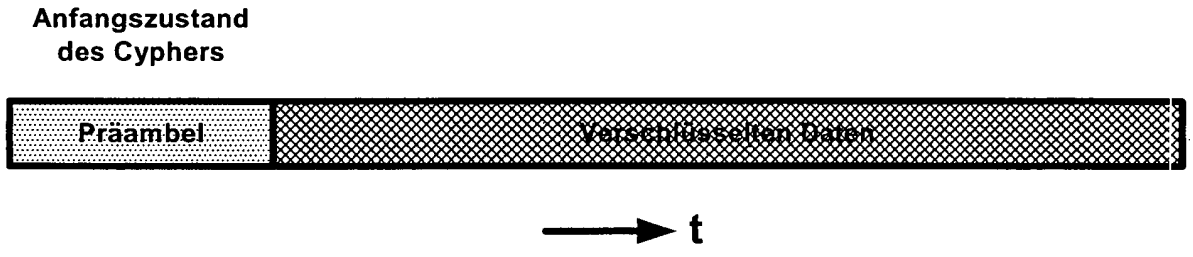


Fig. 1c (Stand der Technik)

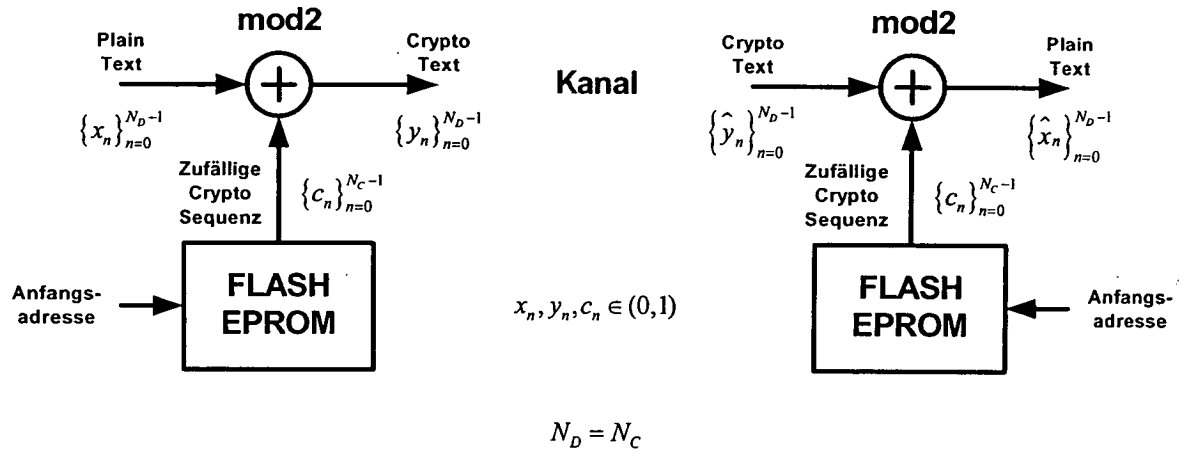


Fig. 2a

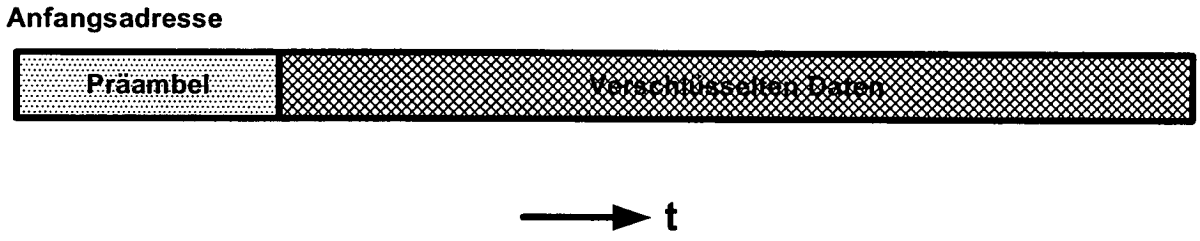


Fig. 2b

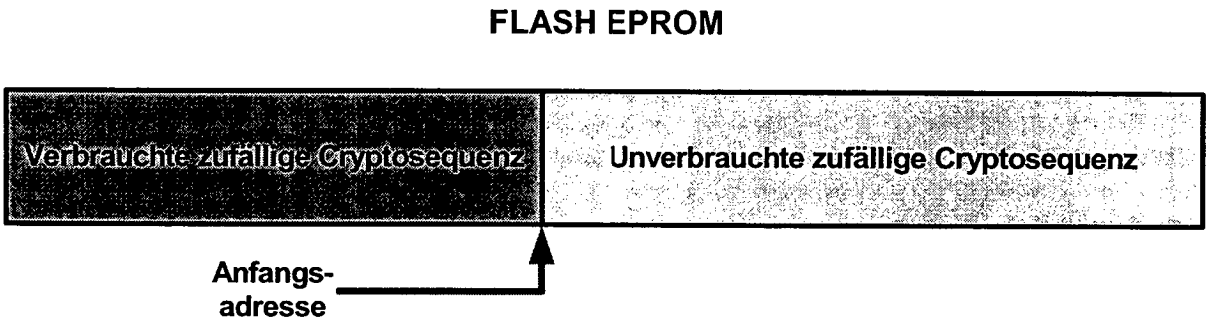


Fig. 2c

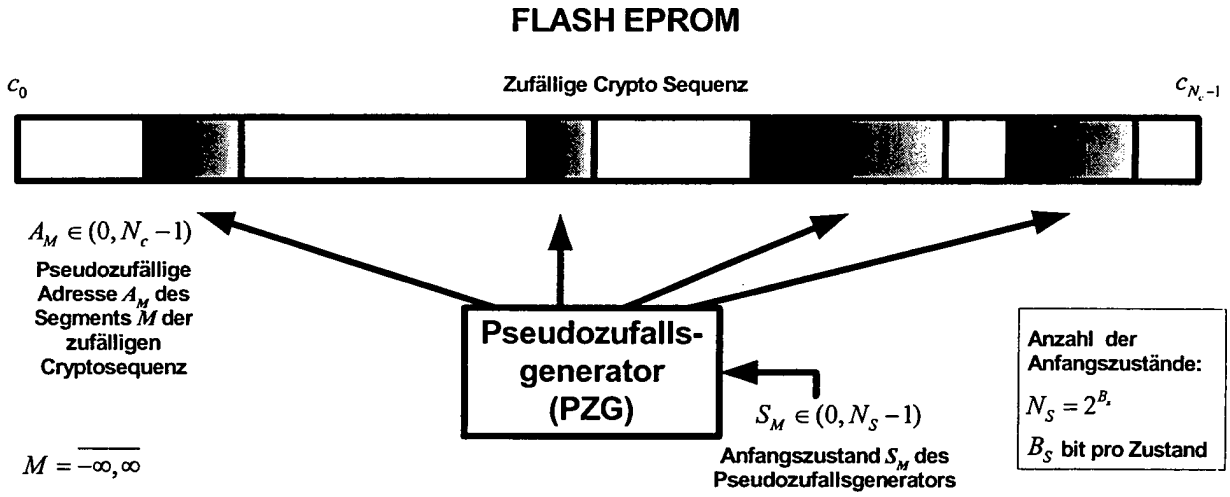

FLASH EPROM
c_0
Zufällige Crypto Sequenz
c_{N_c-1}
$A_M \in (0, N_c - 1)$
Pseudozufällige Adresse A_M des Segments M der zufälligen Cryptosequenz
$M = \overline{-\infty, \infty}$
Pseudozufalls-generator (PZG)
$S_M \in (0, N_S - 1)$
Anfangszustand S_M des Pseudozufallsgenerators
Anzahl der Anfangszustände:
$N_S = 2^{B_S}$
B_S bit pro Zustand

Fig. 3a

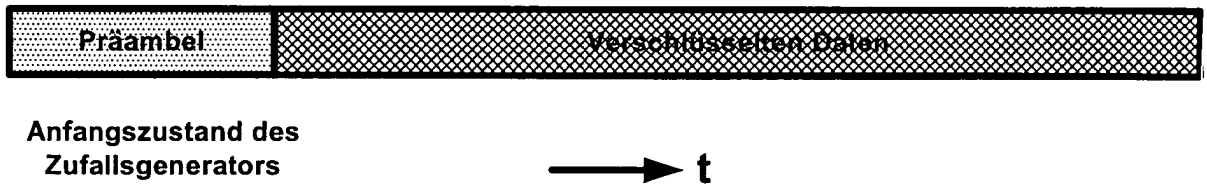

Präambel
Verschlüsselten Daten
Anfangszustand des Zufallsgenerators
t

Fig. 3b

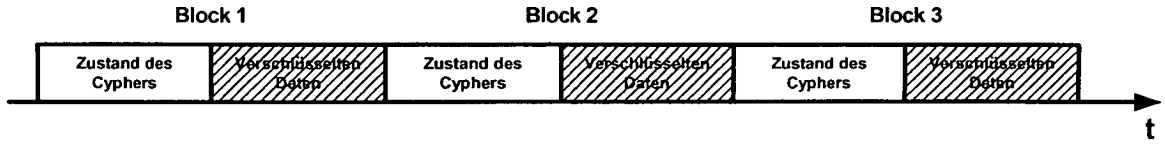


Fig. 4a (Stand der Technik)

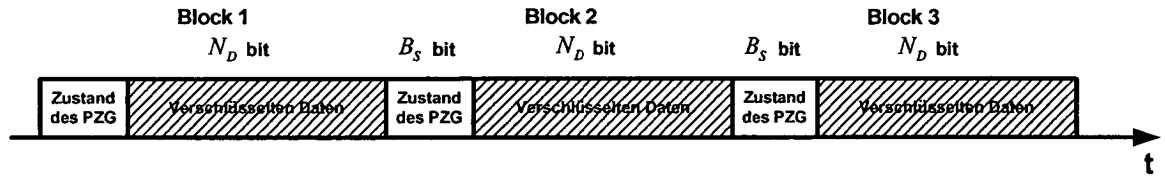


Fig. 4b

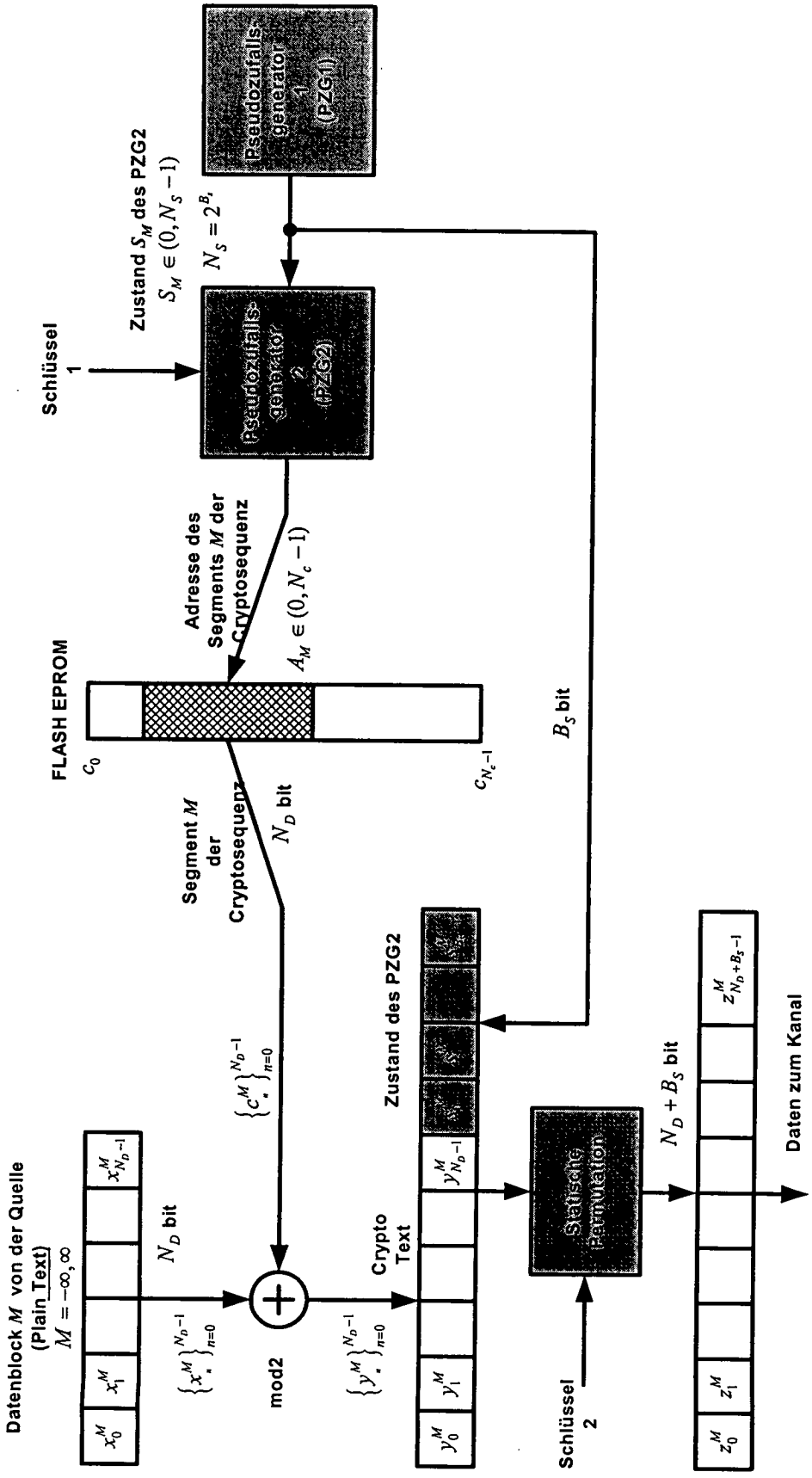

Pseudozufalls-generator 1 (PZG1)
Zustand S_M des PZG2
$S_M \in (0, N_S - 1)$
$N_S = 2^{B_S}$
Schlüssel 1
Pseudozufalls-generator 2 (PZG2)
Adresse des Segments M der Cryptosequenz
$A_M \in (0, N_c - 1)$
FLASH EPROM
c_0
c_{N_c-1}
B_S bit
Segment M der Cryptosequenz
N_D bit
$\{c_*^M\}_{n=0}^{N_D-1}$
Zustand des PZG2
Datenblock M von der Quelle (Plain Text)
$M = -\infty, \infty$
N_D bit
$\{x_*^M\}_{n=0}^{N_D-1}$
mod2
$\{y_*^M\}_{n=0}^{N_D-1}$
Crypto Text
Statische Permutation
Schlüssel 2
$N_D + B_S$ bit
Daten zum Kanal

Fig. 5

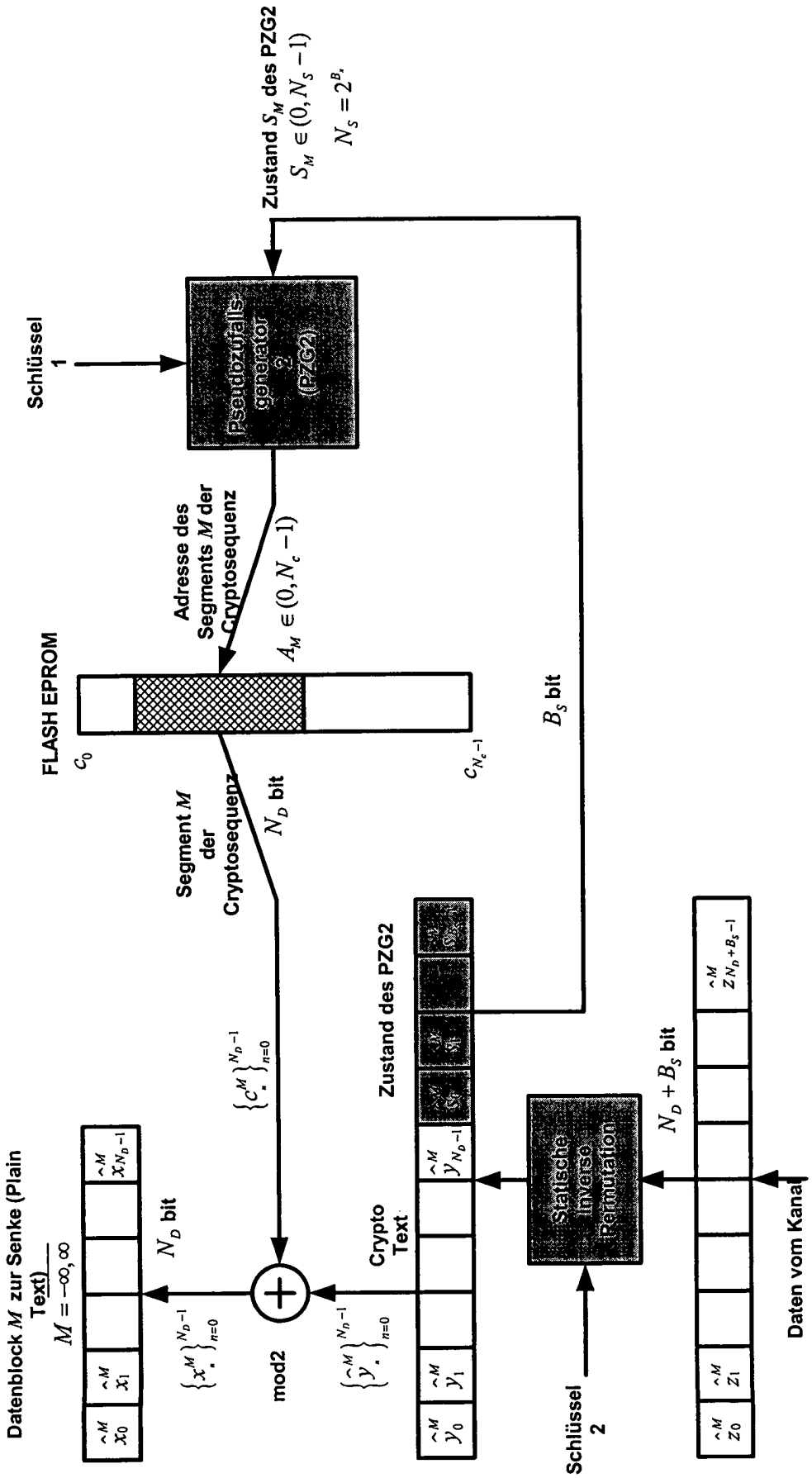

Zustand S_M des PZG2
$S_M \in (0, N_S - 1)$
$N_S = 2^{B_s}$
Schlüssel 1
Pseudozufalls-generator 2 (PZG2)
Adresse des Segments M der Cryptosequenz
$A_M \in (0, N_c - 1)$
FLASH EPROM
c_0
c_{N_c-1}
B_S bit
Segment M der Cryptosequenz
N_D bit
$\{c_\cdot^M\}_{n=0}^{N_D-1}$
Zustand des PZG2
Datenblock M zur Senke (Plain Text)
$M = -\infty, \infty$
N_D bit
$\{x_\cdot^M\}_{n=0}^{N_D-1}$
mod2
$\{\hat{y}_\cdot^M\}_{n=0}^{N_D-1}$
Crypto Text
Statische inverse Permutation
$N_D + B_S$ bit
Schlüssel 2
Daten vom Kanal

Fig. 6