

Kontaktlose Chipkarten



Bild: Giesecke & Devrient

Diese Karten sind unempfindlich gegen Schmutz und Fett. Sie können unabhängig von ihrer Lage zum Auslesen im Portemonnaie des Karteninhabers verbleiben.

Von Klaus Finkenzeller

Eine kontaktlose Chipkarte hat zwar die gleiche Bauform wie eine kontaktbefeete Karte, doch von außen sind keine elektrischen Anschlüsse oder Bauelemente auf den circa 85 x 54 x 0,76 mm großen Karten zu erkennen. Gelangt eine kontaktlose Chipkarte jedoch in die Nähe der Antenne eines Lesegeräts, so tauschen beide wie von Zauberhand Daten aus.

▶ Induktive Kopplung

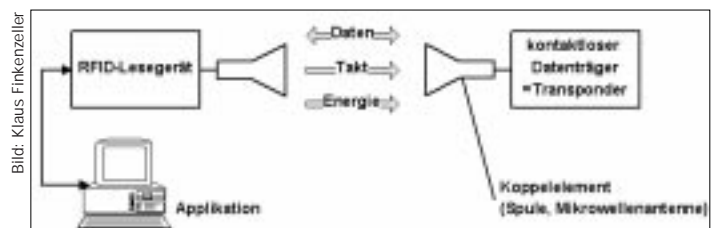
Das Lesegerät überträgt neben den Daten auch Energie durch induktive Kopplung zur Chipkarte. Im Innern der kontaktlosen Chipkarte befindet sich dafür eine großflächige Spule aus mehreren Windungen Draht; typisch sind fünf Windungen bei einer Übertragungsfrequenz 13,56 MHz, und einige 100 Windungen bei 135 kHz.

Zum Betrieb der kontaktlosen Chipkarten erzeugt das Lesegerät zunächst in seiner Antenne ein hochfrequentes Magnetfeld. Die Antenne

Bild oben: Halbtransparente kontaktlose Chipkarte; die Antennenspule sowie der integrierte Chip, rechts unter dem VISA-Logo, sind deutlich zu erkennen

besteht ebenfalls aus einer großflächigen Spule mit mehreren Windungen. Die Frequenz des Magnetfelds kann je nach System bei 13,56 MHz oder auch bei 135 kHz liegen. Hält man nun eine kontaktlose Chipkarte in die Nähe

dieser Leseantenne, so erzeugt das Feld des Lesegerätes eine Spannung in der Spule der Chipkarte. Diese wird gleichgerichtet und dient als Spannungsversorgung der kontaktlosen Chip-



Das Lesegerät versorgt die kontaktlose Chipkarte mit Energie und einem Systemtakt

karte. Die kontaktlose Chipkarte benötigt deshalb keine eigene Batterie.

Parallel zur Induktivität der Chipkartenspule ist im allgemeinen eine Kapazität geschaltet. So entsteht ein Parallelschwingkreis. Die Resonanzfrequenz des Schwingkreises entspricht der Sendefrequenz. Auf 13,56 MHz reicht hierzu in der Regel bereits die Eingangskapazität des Chips aus, auf 135 kHz wird noch ein zusätzliches Kondensatorbauelement benötigt. Die Resonanzüberhöhung in diesem Schwingkreis kann den Wirkungsgrad der Energieübertragung erheblich verbessern. Gleichzeitig wird auch die Antennenspule des Lesegerätes durch einen zusätzlichen Parallelkondensator auf der Sendefrequenz in Resonanz gebracht. Hier soll die Resonanzüberhöhung einen möglichst großen Hochfrequenzstrom, und damit ein ausreichend starkes Magnetfeld zum Betrieb der Chipkarten erzeugen.

▶ Der Informationsfluß

Aus der, in der Chipkartenspule induzierten Wechselfeldspannung, wird zusätzlich eine Taktfrequenz abgeleitet, welche dem Speicherchip oder dem Mikroprozessor der Karte dann als Systemtakt zur Verfügung steht.

Die Datenübertragung von dem Lesegerät zur kontaktlosen Chipkarte, der sogenannte

Downlink, erfolgt im einfachsten Falle durch eine sogenannte Amplitudentastung (ASK - amplitude shift keying), bei der das hochfrequente Magnetfeld ein- und ausgeschaltet wird. Der Chipsatz der Karte kann ein ASK-moduliertes Signal anschließend sehr einfach demodulieren, indem er die in die Kartenspule induzierte Spannung gleichrichtet.

Die umgekehrte Datenübertragung von der Chipkarte zum Lesegerät, der sogenannte Uplink, nutzt die Eigenschaften der transformatorischen Kopplung zwischen der Leserantenne und der Chipkartenspule aus: Eine Änderung des Stroms in der sekundären Spule der kontaktlosen Chipkarte bewirkt auch eine Änderung des Stroms beziehungsweise der Spannung an der primären Spule des Lesegerätes, ganz wie bei einem Transformator. Diese Spannungsänderung an der Leserantenne entspricht in der

INFO

Der Autor Dipl. Ing. (FH) Klaus Finkenzeller ist seit 1989 bei dem Kartenhersteller Giesecke & Devrient beschäftigt. Seit einigen Jahren ist er dort als Technologieverantwortlicher für kontaktlose Chipkarten zuständig. Dazu gehört auch die Mitarbeit in den Normungsgremien SC17/WG8 der ISO, für kontaktlose Chipkarten.

Die Homepage des Autors finden Sie unter ww0.muenchen.org/bm693257/index.htm

Wirkung einer Amplitudenmodulation, jedoch mit einem in der Regel sehr kleinen Modulationsgrad. Durch das Ein- und Ausschalten eines zusätzlichen Lastwiderstands in der Chipkarte im Takt der zu übertragenden Daten, können so Daten an das Lesegerät gesendet werden. Dieser Vorgang wird in der Fachterminologie als Lastmodulation (load modulation) bezeichnet.

Auf Grund der oft sehr geringen magnetischen Kopplung zwischen der Leserantenne und der Chipkartenspule ist mit sehr kleinen Lastmodulationssignalen an der Antenne des Lesegeräts zu rechnen. Die Kopplung ist meist kleiner als zehn Prozent, gelegentlich liegt sie sogar unter einem Prozent. Die Lastmodulationssignale sind in etwa -60 bis -80 dB schwächer als das Trägersignal.

Wie bei jeder Amplitudenmodulation entstehen auch bei der Lastmodulation zwei Seitenbänder um das Trägersignal. Beide Bänder enthalten jeweils die vollständige Information. Um das extrem schwache Signal des Lastmodulators im Empfänger des Lesegeräts besser detektieren zu können, verwendet man bei kontaktlosen Chipkartensystemen im Frequenzbereich 13,56 MHz einen zusätzlichen Hilfsträger mit einer Frequenz von 847 kHz. Hierdurch entstehen an der Leserantenne zwei Modulationsseitenbänder im Abstand von jeweils 847 kHz um die Sendefrequenz des Lesegeräts. Die Daten werden diesem Hilfsträger

in der Chipkarte aufmoduliert, wozu sowohl ASK (amplitude shift keying), FSK (frequency shift keying) als auch BPSK-Verfahren (bi-phase shift keying) zum Einsatz kommen. Der Empfänger des Lesegeräts wird nun auf eines der beiden Seitenbänder abgestimmt. Das starke Eigensignal des Lesegeräts, das ja zur Energieversorgung der Chipkarte immer benötigt wird, kann durch geeignete Filter im Empfänger des Lesegeräts wirkungsvoll unterdrückt werden.

► Anwendungen für die kontaktlosen Karten

Eine der frühesten Anwendungen für kontaktlose Chipkarten war die Zutrittskontrolle zu Gebäuden und Anlagen. Hierzu reichen bereits einfachste Read-Only-Karten aus, da nur eine mehrstellige, eindeutige Seriennummer ausgelesen werden muß. Die Türsteuereinheit prüft die Gültigkeit dieser Nummer. Read-Only-Karten kommen auf Grund der geringen benötigten

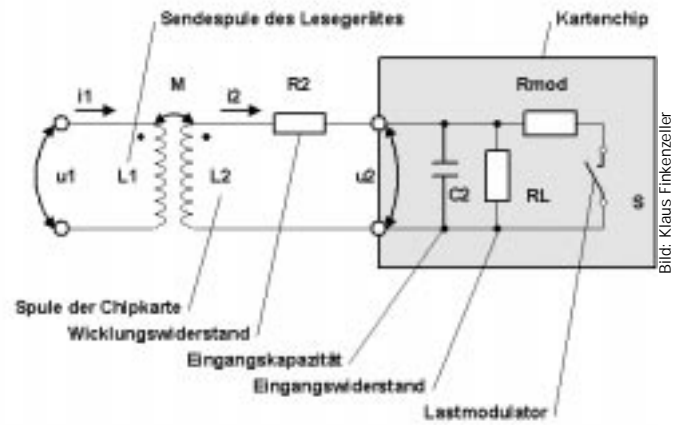


Bild: Klaus Finkenzerler

Ersatzschaltbild der Anordnung von Leseantenne und kontaktloser Chipkarte. Die Leseantenne L1 und die Chipkartenspule L2 sind durch die Gegeninduktivität M miteinander magnetisch gekoppelt. Durch das Ein- und Ausschalten des Lastwiderstandes Rmod können Daten an das Lesegerät gesendet werden

Chipfläche, beziehungsweise auf Grund der geringen Anzahl von Gattern, mit wenig Energie aus. Deshalb lassen sich auch große Reichweiten von über einem Meter realisieren, und der Besitzer muß die Karte nicht mehr in die unmittelbare Nähe eines Lesegeräts halten. Er kann die Karte sogar in der Brusttasche tragen: Auch dort kann sie noch kontaktlos ausgelesen werden („Handsfree-Systeme“).

Eine weit verbreitete Anwendung für kontaktlose Chipkarten ist auch ihr Einsatz als Skiticket. Für den Wintersportler ist es nicht gerade komfortabel vor jeder Liftfahrt, mit klammen Fingern ein vom Schnee aufgeweichtes

ANWENDUNG

RFID - Radio-Frequency Identification

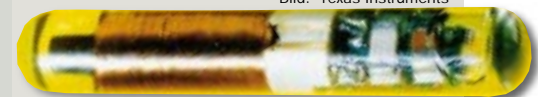
Die Anordnung aus Spule und Mikrochip in einer kontaktlosen Chipkarte wird in der Fachterminologie auch als Transponder bezeichnet. Die Bauform eines solchen Transponders ist jedoch keineswegs auf Chipkarten beschränkt. Tatsächlich stellen die kontaktlosen Chipkarten nur eine kleine Untergruppe der zahlreichen Verfahren zur Identifikation von Gütern, Tieren und Personen mit Radiowellen dar. Alle diese Verfahren bezeichnet man als RFID-Technologie (Radio-Frequency Identification). Rinder, Schafe und Pferde werden beispielsweise durch die Injektion eines in Glas gekapselten Miniaturtransponders manipulationssicher gekennzeichnet. So ist es für Landwirte möglich, die Tiere mit der berührungslosen Identifikation weitgehend automatisch zu füttern und zu überwachen. Darüber hinaus stellt der injizierte Transponder eine fälschungssichere Kennzeichnung in der Tierhaltung dar und ist damit zur Seuchen- und Qualitätskontrolle sowie zur Herkunftssicherung geeignet. Einen wahren Boom erlebte die RFID-Industrie durch die Einführung der elektroni-

scher Wegfahrsperrung in Kraftfahrzeugen. Hier ist der Transponder in den Knauf des Autoschlüssels eingearbeitet – die zugehörige Leseantenne sitzt direkt am Zündschloß. Ausgeklügelte kryptographische Verfahren zur Authentifizierung zwischen Schlüssel und Fahrzeug sichern den Schlüssel. Der Einsatz der RFID-Technologie senkte die Diebstahlrate von Kraftfahrzeugen seit 1994 kontinuierlich, nachdem die Diebstähle seit 1989 stark zugenommen hatten.

Ein weiteres Einsatzgebiet der RFID-Technologie ist die Automation in der industriellen Massenfertigung. Transponder ersetzen hier zunehmend die ursprünglich zur warenbegleitenden Kennzeichnung eingesetzten Strichcode-Etiketten. Besonders vorteilhaft macht sich hier die Unempfindlichkeit gegenüber Umwelteinflüssen oder Verschmutzung bemerkbar, so etwa auch in der Autoindustrie wo sie die Karosserie vom Rohbau bis zur Endprüfung begleiten. Dabei können diese RFID-Systeme auch problemlos in der Lackierstraße eingesetzt werden.

In einigen deutschen Großstädten, unter anderem in Bremen, Köln und Dresden, werden RFID-Systeme zur Abrechnung von Hausmüll eingesetzt. Zu diesem Zweck bringt die dortige Müllabfuhr Transponder an den Mülltonnen an und rüstet die Sammelfahrzeuge mit automatischen Lesesystemen aus. Sobald die Mülltonnen an die Schüttung des Müllfahrzeuges gebracht werden, wird die Kennung ausgelesen und im Bordcomputer des Fahrzeugs zusammen mit dem ermittelten Füllgewicht der

Bild: Texas Instruments



Glas-Transponder werden zur Tieridentifikation eingesetzt. Sie arbeiten ähnlich wie die kontaktlosen Chipkarten

Tonne gespeichert. Die einzelnen Haushalte haben also nicht mehr eine monatliche Pauschale zu zahlen, sondern erhalten ein individuelle Abrechnung, entsprechend der verursachten Müllmenge.

Papierticket aus dem Anorak zu fischen. Kontaktlose Chipkarten als Ski-Ticket sind eine handliche Alternative. Die Lift-Anlagen funktionieren ähnlich wie die beschriebene Zutrittskontrolle zu Gebäuden: Drehkreuze sperren alle Eingänge zum Skilift. Jeder Eingang ist mit einem kontaktlosen Lesegerät ausgestattet. Erkennt die Leseelektronik eine gültige Karte, gibt die Steuerungselektronik das Drehkreuz für eine Person frei. Auch bei dieser Anwendung ist dabei die Lesereichweite so ausgelegt, daß der Skifahrer die Chipkarten zur Kontrolle nicht mehr in die Hand nehmen muß. Im Gegensatz zu den einfachen Firmenausweisen verfügen kontaktlose Ski-Tickets jedoch meist über einen kontaktlos programmierbaren Speicherbereich. Dieser ermöglicht es, die Gültigkeitsdauer der Chipkarten beim Verkauf frei zu programmieren. Die Karten können auch am Ticketschalter nach Benutzung zurückgenommen und erneut programmiert werden. Beim Verkauf der Chipkarten-Tickets wird deshalb vielerorts ein Pfand von 10 bis 20 Mark einbehalten, welches die Liftbetreiber nach Gebrauch der Chipkarten zurückerstatten.

Eines der größten Marktpotentiale für kontaktlose Chipkarten stellt derzeit jedoch der Öffentliche Personennahverkehr (ÖPNV) dar. Der Ersatz der althergebrachten Papierfahrkarte durch ein elektronisches Fahrgeldma-

nagement mit kontaktlosen Chipkarten bietet den Verkehrsunternehmen, den Fahrern und den Fahrgästen gleich mehrere Vorteile.

- Die Einführung eines geschlossenen elektronischen Systems bei dem alle Fahrgäste einen Fahrschein vorzeigen müssen, senkt die Schwarzfahrerquote.
- Die genaue Kenntnis des Tarifs ist für den Fahrgast (Ortsfremde) nicht mehr notwendig, da das System automatisch den richtigen Fahrpreis von der Karte abbucht.
- Monatskarten können an einem beliebigen Tag im Monat beginnen – vorbezahlte elektronische Fahrausweise behalten auch bei Umstellung des Tarifs ihre Gültigkeit.
- Aber auch in der Abfertigungszeit sind die kontaktlosen Chipkarten allen anderen Technologien deutlich überlegen, was eine Untersuchung der Verkehrsbetriebe Helsinki zeigt.

Die Ergebnisse der Finnen stoßen besonders in den asiatischen Millionenmetropolen auf großes Interesse. So ist es auch nicht weiter erstaunlich, daß das bislang größte elektronische Fahrausweissystem mit kontaktlosen Chipkarten 1996 im südkoreanischen Seoul in Betrieb genommen wurde. Die koreanische „Bus-Card“ ist eine vorbezahlte Karte, die mit einem Grundwert von umgerechnet etwa 35 Mark ausgegeben wird. Das Lesegerät bucht bei jeder Busfahrt im Stadtgebiet umgerechnet 0,75



Einsatz von kontaktbehafteten und kontaktlosen Chipkarten im ÖPNV in Deutschland

Mark ab. Die Karte kann jedoch an besonderen Verkaufsstellen beliebig oft wieder aufgeladen werden. Dieses System war so erfolgreich, daß inzwischen bereits etwa 4 Millionen BusCards in Seoul im täglichen Einsatz sind.

► Die Deutschen sind zurückhaltend

Im Vergleich zu den Erfolgen in Asien werden kontaktlose Chipkarten in Deutschland bisher nur wenig eingesetzt. So gibt es vereinzelt Projekte unter anderem auf der Nordseeinsel Norderney, in Lüneburg-Oldenburg und in Marburg. Besondere Anforderungen wer-

ÜBERBLICK

Neue Norm für kontaktlose Mikroprozessor Chipkarten ISO 14443

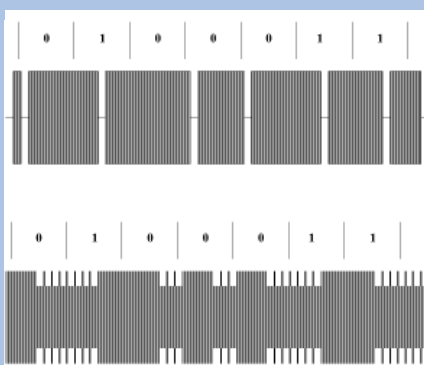


Bild: Klaus Finkenzyller

Signalformen bei der Datenübertragung zwischen der kontaktlosen Chipkarte und dem Lesegerät. ISO 14443 - Typ A: oben Downlink, ASK 100%, Miller-codiert unten Uplink, Hilfsträger 847 kHz, ASK Manchester moduliert

Eine Stärkung des Marktes für kontaktlose Chipkarten erwartet die Branche durch die zukünftige Norm für kontaktlose Mikroprozessor-High-End-Chipkarten: die ISO 14443. Derzeit diskutiert die Arbeitsgruppe JTC1/WG8/TF2 der ISO diese

Norm. Sie soll die physikalischen und datentechnischen Eigenschaften der Übertragungsstrecke zwischen einem Lesegerät und den Chipkarten beschreiben, welche in dieser Norm als Proximity Integrated Circuits Cards (PICC) bezeichnet werden. Der Name soll auf die angestrebte Reichweite von etwa 10 bis 20 cm der PICC-Chipkarten hinweisen. Innerhalb der PICCs wird nocheinmal zwischen den beiden Typen „A“ und „B“ unterschieden, die unterschiedliche Modulationsverfahren einsetzen.

Eine weitere Norm, die in Zukunft voraussichtlich eine wichtige Rolle spielen wird, ist ISO 15693. Sie soll die Eigenschaften von kontaktlosen Low-End-Speicherchipkarten mit einer Reichweite von bis zu einem Meter definieren. Diese Karten werden in der Norm als Vicinity Integrated Circuits Cards (VICC) bezeichnet, um die größere Reichweite dieser Karten im Vergleich zu den PICCs anzudeuten. Das einzige gemeinsame Merkmal der beiden PICC-Typen „A“ und „B“ sowie der VICC ist die einheitliche Sendefrequenz des Lese-

gerätes von 13,56 MHz. Dabei handelt es sich um eine sogenannte ISM-Frequenz (Industry-Science-Medicine), welche in fast allen Ländern der Welt für Funkanwendungen kleiner Leistung zur Verfügung steht.

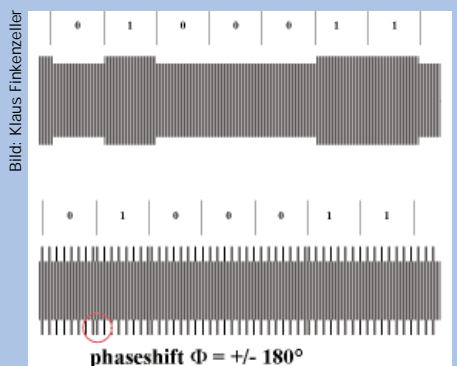


Bild: Klaus Finkenzyller

Signalformen bei der Datenübertragung zwischen der kontaktlosen Chipkarte und dem Lesegerät. ISO 14443 - Typ B: oben Downlink, ASK 10%, NRZ-codiert, unten Uplink, Hilfsträger 847 kHz, BPSK NRZ moduliert

den an Performance und Sicherheit der kontaktlosen Chipkarten im öffentlichen Personennahverkehr gestellt, denn der Geldwert der Karten macht diese auch für mögliche Angreifer interessant. Der Schreib- und Leszugriff auf die Karten ist deshalb nur nach einer gegenseitigen Authentifizierung zwischen der kontaktlosen Chipkarte und dem Lesegerät möglich. Dieser Vorgang überprüft, ob ein geheimer, kryptographischer Schlüssel in der Chipkarte und dem Lesegerät gespeichert ist. Geeignete Algorithmen, wie sie etwa in der ISO-Norm 9798 beschrieben sind, können verhindern, daß ein Angreifer den geheimen Schlüssel ausspäht. Dieser könnte ohne diese Maßnahme die Funkverbindung zwischen der Chipkarte und dem Lesegerät einfach abhören und so den geheimen Schlüssel ausspionieren. Die einer erfolgreichen Authentifizierung folgende Kommunikation zwischen der Karte und dem Lesegerät wird ebenso verschlüsselt, um auch das Abhören und das erneute Einspielen der zu übertragenden Daten zu verhindern.

Bei kontaktbehafteten Chipkarten ist automatisch sichergestellt, daß das Lesegerät immer nur eine einzige Karte gleichzeitig anspricht. Bei kontaktlosen Karten ist es dagegen nicht zu verhindern, daß sich zur selben Zeit mehrere Karten im Ansprechbereich des Lesegeräts befinden. Um für diesen Fall eine Datenkollision zwischen den einzelnen Karten zu verhindern, entwickelten die Herstellerfirmen unterschiedliche Antikollisionsverfahren. Diese Verfahren erlauben es, gezielt eine kontaktlose Chipkarte unter mehreren auszuwählen und anzusprechen. Hierbei kommen vor allem Zeitmultiplexverfahren mit unterschiedlichen

Auswahlalgorithmen („Binärer Suchbaum“, „Slotted Aloha“) zur Anwendung.

► *Perspektiven*

Die Entwicklung kontaktloser Chipkarten bleibt nicht stehen. Eine sehr interessante und aktuelle Weiterentwicklung ist die Kombination der kontaktlosen und der kontaktbehafteten Technik auf einer einzigen Chipkarte. Diese sogenannte Dual-Interface-Card, auch Combi-Card genannt, kann damit wahlweise über die kontaktlose oder auch über die kontaktbehaftete Schnittstelle angesprochen werden. Die Philosophie hinter dieser Idee ist eine völlige Unabhängigkeit zwischen dem Chipkarteninterface, beispielsweise kontaktbehaftet, kontaktlos und Infrarot, und der Chipkartenlogik beziehungsweise der Chipkartenanwendung. Das Interface wird damit für die zu übertragenden Daten transparent, so daß aus Sicht der Anwendungssoftware das verwendete Interface schließlich keine Bedeutung mehr hat. Hierdurch ergeben sich Möglichkeiten, um neue Anwendungen einzuführen. Es kann nämlich auf bereits bestehende Infrastrukturen zurückgegriffen werden. Denkbar ist etwa die Kombination der flächendeckend eingeführten EC-Karte mit einem ÖPNV-System auf einer Karte. Zum Bezahlen einer Fahrt könnte der Fahrpreis über das kontaktlose Interface der Dual-Interface-Card automatisch abgebucht werden, während die Karte auf dem herkömmlichen Wege in einem EC-Kartenterminal aufgeladen werden könnte. Dies ist nur eine von sehr vielen neuen Anwendungen, die sich durch die Dual-Interface-Technologie realisieren lassen.

(TZ)

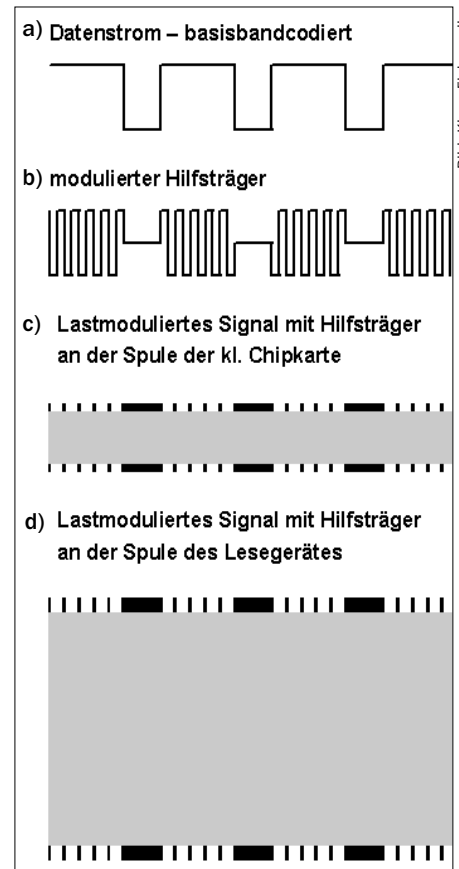


Bild: Klaus Finkenzerler

So entsteht eine Lastmodulation mit Hilfsträger:
 a) Der Basisbandcodierte Datenstrom (z. B. NRZ oder Manchester-Code).
 b) Beispiel für ein Hilfsträgersignal nach ASK-Modulation mit Signal a.
 c) Spannungsverlauf an der Transponderspule nach einer Lastmodulation mit Signal b.
 d) Empfangssignal an der Antennenspule des Lesegerätes (nicht maßstabsgerecht)