无触点芯片卡

作者克劳斯·芬肯策乐自1989年以来就职于世界著名制卡厂商德国捷德公司，近年来主要负责该公司无触点芯片卡技术方面的工作，同时参与ISO SC17/WG8专家组为无触点芯片卡制定标准。

（题图，Y. Z. 半透明无触点芯片卡；维萨-VISA-标记的右下侧可见天线线圈和芯片）

此类卡不怕油污。读卡时不必虑及卡的方位，不必从持卡人的钱包中掏出。

无触点芯片卡与有触点卡的结构形式基本相同，但在规格为85×54×0,76mm卡表面没有触点或其它接触元件。当无触点芯片卡接近读写器天线周围时，二者之间就有如由一只魔手操纵一般开始交换数据。

电感性耦合

读写器通过电感性耦合向芯片卡传输数据，提供电能。芯片卡内部有一个由数圈丝线缠绕的大线圈：载频（传输频率？）为13,56MHz时，线圈通常由五圈丝线缠绕；载频为135kHz时，线圈由几百圈纤细丝线缠绕而成。

读写器先在其内部，同样由数圈丝线缠绕而成的大线圈天线内产生一个高频磁场以驱动无触点芯片卡。磁场频率根据不同的系统可为13,56MHz或135kHz。无触点芯片卡位于读卡器天线周围时，读写器的磁场在芯片卡的线圈内产生电压。电压经过整流为无触点芯片卡提供工作电压。无触点芯片卡因而无需电池供电。

（插图：读写器向无触点芯片卡提供电能和系统脉冲）

与芯片卡线圈上的电感性并行通常也接通一个电容，并行谐振电路由此而来。谐振电路的谐振频率与发射频率等同。载频为13,56MHz时，卡的输入电容通常已经足够；载频为135kHz时一般需要添加一只电容元件。谐振电路里的谐振超高(Resonanzüberhöhung)可极大地改善电能传输。同时通过在读写器另外并联一只电容器使读写器天线线圈与发射频率谐振。由此谐振超高将产生最大值高频电流。提供足够的磁场强度用以驱动芯片卡。

信息数据流

脉冲频率(Taktfrequenz)也产生于芯片卡线圈上的感应交变应力，这一脉冲频率用于卡上存储芯片或微处理器的系统脉冲(Systemtakt)。

在最简单的情况下数据由读写器向无触点芯片卡传输，即所谓的下联（downlink），通过振幅键控(ASK - amplitude shift keying)开启或关闭高频磁

场进行. 卡的电路通过对卡上线圈的电感电压进行整流而很容易地向经由ASK调制的信号进行反调制.

与此相反, 数据由卡体向读写器传输, 即所谓的上联(uplink), 利用读写器线圈和卡体线圈之间的变压耦合特性: 与变压器的工作原理类似,无触点芯片卡中次级线圈电流的变动造成读写器内初级线圈电流或电压的变动. 读写器线圈上电压的变动在作用上与振幅调制相同, 但通常调制的幅度很小. 通过以传输数据的节奏来关闭或开启卡内一只附加的负载电阻, 就可将数据送入读写器中. 专业术语称这一过程为负载调制(load modulation).

(插图: 读写器天线线圈和无触点芯片卡线圈电路示意图. 读写器天线L1 和芯片卡线圈L2之间通过相互电感性M形成电磁耦合. 用开启或关闭负载电阻Rmod 可将数据发至读写器)

读写器天线和芯片卡线圈之间出现的电磁耦合现象一般极微弱, 因而须考虑达到读写器天线上的负载调制信号也极微弱. 耦合通常小于百分之十, 有时甚至在百分之一以下. 负载调制信号一般比载波信号低 -60到 -80 dB.

与所有的振幅调制一样, 负载调制的载波信号周围也出现二个各自含有完整信息的边带. 为了使读写器内的接收器能够更好地检测极端微弱的负载调制信号, 在载频为13,56MHz 的无触点芯片卡系统内一般添加频率为847 kHz 的辅助载波. 由此在读写器天线线圈发射频率的周围产生二个调制边带, 距离各为847 kHz. 芯片卡中的数据将通过使用ASK, FSK (frequency shift keying) 和 BPSK (bi-phase shift keying) 为辅助载波调制好. 读写器中的接收器以这二个边带之一为准调谐. 读写器用以向芯片卡持续供电的较强的自身信号可通过读写器接收器内的合适的滤波器得到有效的抑制.

无触点芯片卡的应用

无触点芯片卡的最早的应用之一为门禁控制. 由于只要读出一个明确的多位序列号即可, 最简单的只读卡(read-only-card) 就足以满足这一用途. 门的控制设施检查一个号码的有效性. 只读卡所需的芯片面积小, 门电路少 (电路简单), 因而只要很少的电能. 作用距离可以达到一米以上. 持卡人不必将卡置于读卡器前. 放在胸前衣袋里的卡也可无接触地由读写器读出 (Handsfree-System).

另外, 无触点卡广泛用来作滑雪卡. 对冬季运动爱好者来说, 每次乘缆车时用冻得僵直的手指从大衣兜里掏出被雪水浸得湿漉漉的纸票来, 并不是一件舒服的事. 用无触点卡来替代纸票就方便多了. 缆车设施的运作方式同上述的门禁控制系统大致相同: 转闸门封闭了所有通往滑雪缆车的入口. 每一入口处安上一个无触点读写器. 电子读写器每识别出一片有效卡, 电子转闸门就让一个人通过. 在设置读写器的有效作用距离时, 同样考虑到不必让滑雪者将卡拿在手中以备检查. 与普通公司证件卡不同之处在于, 无触点滑雪票卡大多具备非接触, 可编程的存储区间. 在发售滑雪票时可通过编程决定票的有效期. 滑雪票也

可在用过之后由售票处收回用来重新编程. 许多地方在出售芯片卡滑雪票时即收十至二十马克的押金, 票用完收回后即退回押金.

目前无触点卡的最大市场潜力在于城区近程公共交通. 用电子货币系统, 无触点芯片卡来替代长期以来使用的纸质车票会无疑同时给公交公司, 司机和乘客带来诸多好处.

启用一个全封闭的电子系统, 所有的乘客都必须出示车票, 将大幅度降低无票乘车的比率.

由于系统能自动准确地将票价从卡上扣除, (外地)乘客不必详细了解各类票价.

月票可以从一个月中的任何一天开始 - 即便票价调整, 预付的电子票仍不失其有效性.

赫尔辛基的几家交通公司所做的调查表明, 无触点芯片卡车票在检票时间上较之其余所有技术明显优越.

芬兰的积极经验引起了亚洲人口密集区城市的极大兴趣. 毫不足怪, 迄今为止规模最大的采用无触点芯片卡的电子车票系统于1996年在南韩汉城投入运行使用. 韩国的"车票卡"是一种预付卡, 预付金额约为35马克. 每次乘车时读卡器将大约0,75马克的金额从卡上扣除. 车票卡可在指定的售票处加值. 系统运转极为成功, 目前汉城每日约4百万人次使用车票卡.

德国人较为谨慎

同亚洲的成就相比, 无触点芯片卡在德国用得较少, 仅有几个零星的项目如北海小岛Norderney, 绿纳堡 - 奥尔登堡和玛尔堡. 在城市公共交通中的应用中, 人们向无触点芯片卡的效率和安全性能提出了特别的要求, 卡的现金价值可能会使一些潜在的攻击者对其感兴趣. 只有经过无触点芯片卡和读卡器之间的相互认证才可有权对卡进行读写. 认证过程检验芯片卡和读写器之间是否存储加密密钥. 采用适当的, 如ISO-9798所描述的算法可防止攻击者窃取密钥. 若不采取这一措施, 攻击者只要通过窃听芯片卡和读卡器之间的无线电联系就可探得密钥. 经过成功认证, 卡与读写器之间的通讯也需经过加密, 以免窃取和再次使用传输数据.

使用接触式芯片卡时, 读写器自然而然一次只能和一张卡进行通讯. 但在使用无触点芯片卡时, 可有许多片卡同时进入读写器的通讯范围. 这种情况下为避免几张卡之间的数据冲撞, 制卡商们开发了不同的防冲撞方法. 这些方法可使读写器有目的地从几片无触点芯片卡中仅选一片来并与之通讯. 此处应用时间区分电路方法和防冲撞算法(„Binärer Suchbaum", „Slotted Aloha").

远景

目前无触点芯片卡尚在发展中. 目前最有意义的发展动态是在一个芯片上联合非接触和有接触两种技术. 这种双接口卡, 亦称联合卡

(Combicard) 既可通过非接触接口又可通过接触接口进行通讯. 这个发展方向背后的基本想法是使卡的接口 - 无论是接触, 非接触或是红外线 - 与芯片卡的逻辑和应用相脱离. 这样卡的接口对所传输的数据完全透明, 即从应用软件的角度来看所使用的接口不再起任何作用. 由此可以在现成的基本结构上开发新应用. 比方可以设想在广泛分布的欧洲支票卡(ec-Card)上添加公共交通票系统. 乘车时票价由双接口卡的无触点接口自动从卡上被扣除, 而卡又可在传统的欧洲支票卡终端加值. 这只是双接口技术可实现的诸多新应用之一.

(图型解说 - Y. Z)
a) 数据流 - 编码基带 b) 经调制的辅助载波 c) 无触点芯片卡线圈上带辅助载波的负载调制信号 d) 读写器线圈上带辅助载波的负载调制信号.

带辅助载波的负载调制运作如下:
a) 编码基带的数据流 (如NRZ或Manchester- 码)
b) 凡例: 辅助载波信号, 由ASK调制a信号形成
c) Transponder 线圈上的应力分布, 由b 信号经负载调制产生
d) 读写器天线线圈上的接收信号 (未按原比例)

应用

射频识别, Radio-Frequency Identification

无触点芯片卡上的线圈和芯片的组件在技术术语中称为Transponder. Transponder 的组成形式却不仅限于芯片卡. 在众多应用无线电电波进行识别货物, 动物和人员的方法中, 无触点芯片卡其实只是一个很小的例子. 人们称所有这些方法为RFID - 技术 (Radio-Frequency Identification, 射频识别). 例如人们将封闭在玻璃器皿里的微型Transponder 作为一种无法行骗的标记注射入牛、羊和马体内. 农户因而可以无需触摸而识别动物, 实行自动化饲养和看管. 另外注入动物体内的Transponder 是一种有效的防伪标记, 特别适用于疫情、质量控制以及明确动物产地. 将电子车锁用于机动车辆之后, RFID - 工业经历了真正迅猛的发展. 人们将Transponder 安到车钥匙柄上, 与此相关的天线则直接装在车的引擎上. 同时采用精心设计的加密方法来进行车钥匙和车之间的认证, 以保证钥匙的安全. 1989年之后的几年中汽车失窃量增加很快, 自1994年在汽车工业中采用RFID - 技术之后机动车辆失窃率持续下降.

另外, RFID - 技术也用于制造业中自动化大批量生产. Transponder日益取代一向使用的, 用以标识一件商品在整个生产流程中的条码. Transponder 表现出的极大优点在于不受周围环境影响, 不怕油污, 比方在汽车工业中可从一辆车的车壳粗加工一直伴随到车的最后检验. RFID - 系统也可毫无问题地在油漆生产线中使用.

在几个德国的大城市如不来梅, 科隆和得累斯顿, RFID - 系统用于运送日常垃圾的结帐. 垃圾清运公司将Transponder安在垃圾桶内, 运送垃圾的车辆装配上自动读出系统. 由垃圾桶向垃圾车倾倒垃圾时, 垃圾桶

内的Transponder 标记被读出，垃圾车上的计算机自动存储垃圾桶的装载重量. 这样各家各户不必每月付一笔固定数额的垃圾清运费，而是造成多少垃圾付多少钱。

概述

无触点卡中的微处理器

（左侧信号图，Y．Z）

无触点芯片卡和读写器之间数据传输的信号形式。ISO 14443－A型：上图为下联 (Downlink) ASK 100%, Miller 码；下图为上联(Uplink)，辅助载波: 847kHz, ASK Manchester 调制.

（右侧信号图，Y．Z）

无触点芯片可和读写器之间数据传输的信号形式。ISO 14443－B型：上图为下联(Downlink) ASK 10%, NRZ－码．下图为上联(Uplink)，辅助载波: 847kHz, BPSK NRZ 调制.

制卡业正期待着高品质无触点微处理器芯片卡标准(ISO 14443)的出台，并希翼此标准能加强无触点芯片卡的市场．目前ISO的JTC1/WG8/TF2工作组正在进行该标准的制定工作．此标准将描述读写器和芯片卡之间传输距离的物理及信息技术的特性．?????在此标准中被称作Proximity Integrated Circuits Cards (PICC)．这一名称描述PICC卡的约为10cm至20cm的设计作用距离．PICC卡本身根据不同的调制方式又可分为A型和B型。

另外一个预计将起重要作用的标准为ISO 15693．该标准将定义作用距离为1米左右的一般性无触点存储芯片卡．此类卡在标准中被称为Vicinity Integrated Circuits Cards (VICC)，以表明这类卡的作用距离比PICC大。PICC卡的A、B型以及VICC卡的唯一共同之处在于读写器的发射频率一致为13,56mhz．这一频率实际上指的是所谓ISM－频率（Industry-Science-Medicine)，世界上几乎所有国家都将这一频率用于小功率的无线电信号传输.

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 kontaktbehaftete 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 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 Chipkarte. 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 Wechselspannung, 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

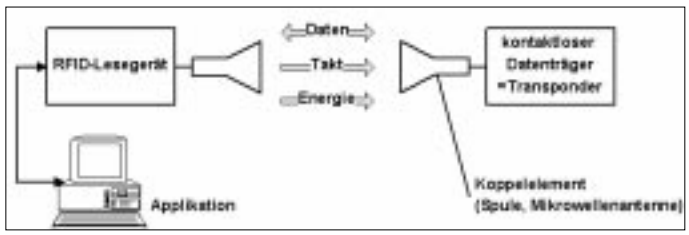


Bild: Klaus Finkenzeller

Das Lesegerät versorgt die kontaktlose Chipkarte mit Energie und einem Systemtakt

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

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

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 Lesegerätes 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 Lesegerätes wirkungsvoll unterdrückt werden.

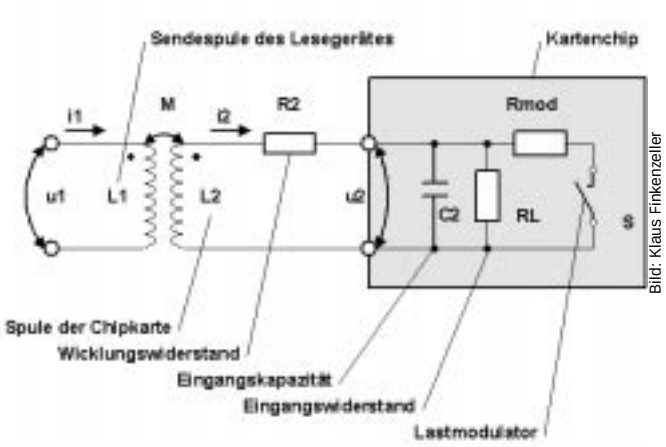


Bild: Klaus Finkenzeller

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

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 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 Ski-Ticket. Für den Wintersportler ist es nicht gerade komfortabel vor jeder Liftfahrt, mit klammen Fingern ein vom Schnee aufgeweichtes

ANWENDUNG

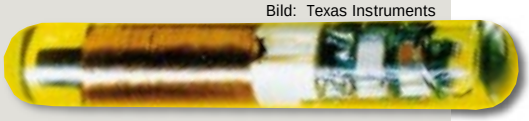
RFID - Radio-Frequency Identification

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 elektronischer Wegfahrsperre 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



Glastransponder 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 kontaklosen Lesegerät ausgestattet. Erkennt die Leseelektronik eine gültige Karte, gibt die Steuerungselektonik 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 Papierfahrscheine durch ein elektronisches Fahrgeldmanagement 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 kontaklosen 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 „BusCard“ 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 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.

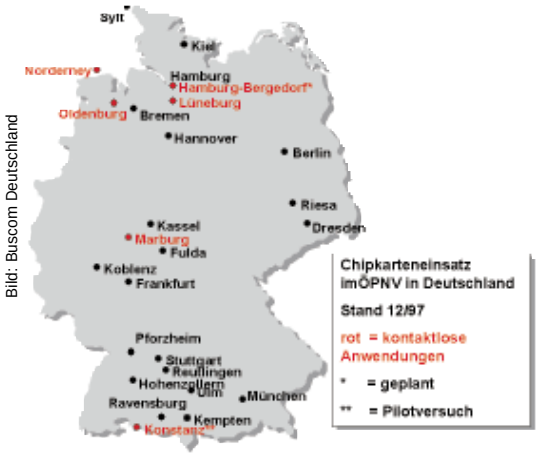


Bild: Buscom Deutschland

Einsatz von kontaktbehafteten und kontaktlosen Chipkarten im ÖPNV in Deutschland

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

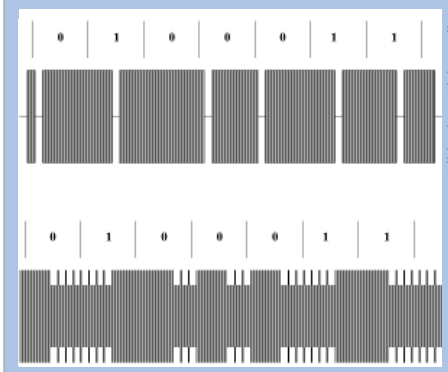


Bild: Klaus Finkenzeller

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 Lesegerätes 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.

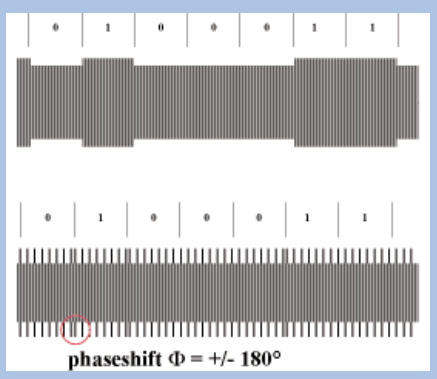


Bild: Klaus Finkenzeller

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 kontaklosen Chipkarten im öffentlichen Personennahverkehr gestellt, denn der Geldwert der Karten macht diese auch für mögliche Angreifer interessant. Der Schreib- und Lesezugriff 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)*

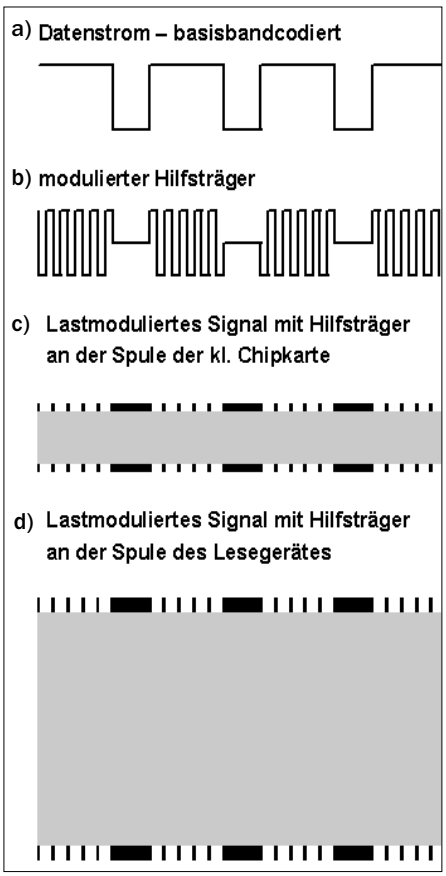


Bild: Klaus Finkenzeller

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)