从安全性方面看门禁系统的发展

曹湛江　刘真真
（中国电子科技集团公司第二十二研究所，山东 青岛 266000）

摘　要　门禁系统在重要场所出口管控方面发挥着至关重要的作用，本文介绍了市面上几种热门的门禁系统，简析其原理和现状，分析各类门禁在安全性等方面固有的不足，揭示部署实施造成的常见缺陷隐患，并对各类门禁的优劣进行评析，展望门禁系统的发展与未来。

关键词　有卡门禁系统　非接触式 IC 卡　无卡门禁系统　门禁安全
中图分类号：TP311.13　　**文献标识码**：A　　**文章编号**：1007-0745(2022)07-0125-03

门禁系统（Access Control System，ACS）是对出入口通道进行管理控制的应用系统，门禁系统不仅管控有人进出的门，还管理车辆通道、物流通道等。门禁系统的管理技术早已超越了出入口授权的管控，现已发展出整套出入管理，在人员考勤、工作环境安全等场合起到了承载的关键环节。不断追求更安全可靠、准确稳定的门禁系统，设计生产出更便捷、更安全的新型门禁系统，是多年来国内外炙手可热的研究方向之一。

对门的管控技术从门锁演化而来，传统的机械锁只涉及机械设备，无论材料多么结实，结构多么精巧，总有技术措施开锁。人员众多的出入口（像写字楼、宾馆房间等）钥匙的管控会很复杂，遇到丢钥匙和换人的情况，都要更换锁具和钥匙。人员众多出入口（像办公大楼、宾馆房间等）钥匙的管控将十分复杂，遇到丢钥匙以及换人，都得把锁具和钥匙换新。为了解决这些繁琐事项，电子门禁系统应运而生，是解决重要场所出入管控、落实安全防范的有力办法，非常适用于银行、机房、工厂、酒店、重点库房、智能小区等各种需要保护的重要场所。

1 有卡门禁系统

1.1 条码卡

最早使用的门禁卡是条码卡，门禁读卡器读取卡片上的条形码作为鉴别方式。条码卡成本低廉，复制容易（理论上使用普通的复印机即可完成复制），在门禁系统中很快被取代。目前主要应用在成本限制较严的中小型机构（如中小型图书馆）以及条码一次性使用场所（如超市的自助存包柜）等。

1.2 磁卡

磁卡卡片的一面有一个涂磁区，该区域内设置了数条可写磁性信息的轨道（磁轨），在磁轨上记录有磁信息（包括检测数据、固定数据、可变数据等）。有时为提高数据安全性，也能通过特定方式把多种信息内容（可变、固定等）混写。刷卡读取时，磁卡和磁头以一定的速度相对移动，通过电磁感应的方式还原出磁卡记录的磁信息。若卡片使用时，刷卡器和磁卡的相对速度过慢、速度不稳，则读出的数据就易出错。因为磁卡价格经济，使用容易，便于管理，又有一定的安全特性，得到很好的推广。但也因其结构简单易被复制，操作使用不便，较易磨损、消磁等原因，在门禁系统中很快被 RFID 感应卡所替代，目前仅部分自助银行门禁系统仍在使用。在支付领域，2016 年 6 月我国的中央银行发布了特急通知，明确要求：自 2017 年 5 月，全面关闭芯片磁条复合卡中的磁条交易功能。

1.3 接触式 IC 卡

接触式 IC 卡内嵌一枚微电子芯片，卡片表面留有金属触点，使用时通过金属触点连接卡内部芯片集成电路和外部的读卡器及应用设备，进行通讯和数据交换。使用 IC 卡做门禁系统，读卡过程不怕电磁干扰，与非接触式 IC 卡或生理特征识别方式相比更具有安全性，可单机独立运行，工作可靠性高。但使用前必须先将其从卡包、卡套中取出，并按指定方向将卡片插入读卡器才能完成刷卡，不能享受非接触式感应卡隔着包“挥一挥”开门的便利性，且容易受卡面污渍、粘贴物等影响，目前很少使用。

1.4 非接触式 IC 卡

目前有卡门禁中，非接触 IC 卡已基本全面取代磁卡和接触式 IC 卡，成为自动识别卡中的主流，目前用作门禁卡的非接触式 IC 卡的主要分为两大类，125kHz 低频只读卡(ID 卡)和 13.56MHz 高频读写卡(M1 卡、CPU 卡)。

1.ID（Identification Card）卡。ID 卡是一种非接触式的感应卡，卡内没留写入用户数据的空间，只存有固定的卡号，ID 卡主要有台湾 SYRIS 的 EM 格式等卡型。门禁系统的读卡器通过非接触感应方式读出 ID 中存有的卡号后，控制器对该卡号在系统的指定点位是

否已登记授权来进行判断，决定运行还是禁止通行。ID 卡上市后在门禁领域就基本上替代了早期的磁卡或接触式 IC 卡，但因为 ID 卡只能在生产厂商一次性写入卡号信息，不可写入用户数据，实际应用时也仅有卡号的辨识，如需实现消费等功能需完全依赖网络平台数据库的支持，不适合做离线支付的消费卡，无法实现具备门禁、储值消费等多种功能合一的一卡通。且由于 ID 卡中存储的内容仅存卡号，门禁系统也仅使用卡号作为判断依据，十分容易被复制，安全性低，目前属于淘汰技术产品，因此通常仅安全性要求不突出的普通住宅区院门楼门等环境，不适用于重要单位、需要严密保护的场所。

2.M1 卡（逻辑加密卡，门禁行业俗称 IC 卡）。M1 卡的出现改变了原有 ID 卡的格局，生产 M1 卡的厂家主要有三个，一个是飞利浦下属公司恩智浦，另外一个是西门子，再一个是复旦微电子，目前复旦 M1 卡在国内使用量较大。M1 卡分为 16 个扇区（第 0 区 – 第 15 区），每个扇区对应 4 块（块 0– 块 3），第 0 扇区的第 0 块由生产厂商预置数据，设置了一个独一无二的 UID，以及 UID 校验位和厂商预置内容，按规范生产出的 M1 卡，该段在出厂时已被写保护，只许读取禁止写入。第 1–15 扇区的 0–2 块用来放置用户数据，块 3 用来保存密码和存取控制。

M1 卡系统价格低廉，结构简单，易实现小额储值交易等功能，迅速得到广大用户的接受，全国各领域累计发卡量已达数亿张。M1 卡不仅是目前应用最广的门禁卡之一，由于卡片中的不同扇区可以在不同的应用系统上设置不同的密码限制该区段的读写权限，理论上可以多套独立的计费系统上分别存储数据，容易实现一卡通，通常用来作为身份鉴别卡、小额电子钱包、学校一卡通等。M1 卡内设有加密逻辑电路，可使用校验密码的方式来保护卡中信息，判断是否开放外部访问，可以简化理解为有密码保护功能的 U 盘，有密码来保护卡内的数据信息，安全等级明细提高，能实现低层次的安全保护，但在防范专业的技术攻击破解上来说还是有漏洞缺陷。

2008 年 M1 卡被技术破解的消息轰动了全球门禁界，互联网上“M1 卡破解”的技术文章非常丰富详细，根据文章提供的方法，随便一个不具备计算机专业技术的人都可以不到几小时就破解复制普通的 M1 公交卡。用作储值交易使用的 M1 卡，被不法分子利用，谋取私利，非法充值或复制。2009 年 4 月，工信部发文《关于做好应对部分 IC 卡出现严重安全漏洞工作的通知》，通知各地各机关和部门开展对 IC 卡使用管理的相关处置工作。2013 年 12 月，住建部的 IC 卡中心发文《关于采取若干措施促进城市一卡通系统升级及加快 CPU 卡替换 M1 卡的通知》，要求自 2014 年起，仍使用 M1 卡的城市一卡通运营单位，新采购安全认证卡统一设置 M1 卡控制时效，时效截止 2018 年底，2019 年起安全认证卡仅支持 CPU 卡应用 [1]。

3.CPU 卡。CPU 卡中的集成电路包含微处理器、程序存储单元、数据存储单元、加密处理器以及芯片操作系统。非常适合放在需要卡片防伪效果突出、数据安全性高可靠的场合中，十分有效地杜绝了仿冒卡片的行为，防止非法读写、篡改卡上的存储内容，在鉴别和支付方面，用于部署高安全可靠性的卡应用系统。M1 卡破解事件暴露之后，有关部门强化了政府和企业等重要部门门禁系统的管控，要求重要门禁系统的加密算法使用国密算法，门禁产品纳入国家商用密码管理体系管理 [2]。

如果说逻辑加密卡（M1 卡）相当于一个设置了密码的 U 盘的话，带有芯片操作系统的 CPU 卡就相当于一台完整的电脑，自身不仅拥有其他卡型的数据存储，同时带有独立数据运算功能、命令处理和数据安全保护等能力。

2 非接触式 IC 卡复制现状

ID 卡内仅存有卡号，完全不防复制，只要去配锁店或自行购买空白 ID 卡和复卡器，秒等可取。M1 卡虽支持一定的加密措施，但 2008 年已被破解，且破解技术公开，即使加密，仍难逃被复制的命运。

大多数 M1 卡并未设置密码，仅需一部带有 NFC 功能的手机，几秒钟就能复制成门禁卡，在专业配锁店的复制速度更快。原因在于我国的门禁产业虽经过自身近二十年的迭代改进，从最初的“山寨”到逐步拥有自主知识产权，经过从磁卡、条码卡、ID 卡发展到 M1 卡门禁系统时，因为早期产品的开发理念是从国外拿来，我国多数生产商一直也都沿用国外方案，ID 卡门禁产品中仅校验卡号的鉴别方式，作为历史安全缺陷一直延续到带有逻辑加密的 M1 卡上，这种惯性习惯长期影响着广大的门禁市场，门禁卡的最终使用人员也难以针对性地了解其中的技术要素，这才是隐蔽在广大门禁系统中最大的安全隐患。

现在国内仍有八成的门禁系统仅靠读取 M1 卡的原厂 UID 号或 ID 卡的 ID 号来判断，作为门禁系统的唯一鉴别，缺少卡片与门禁机具间的加密认证，没有开发设置专用密钥，到最终用户手中的门禁卡密码为空，被复制时不需要“解密”环节，其风险值远大于 M1 卡的解密破解，非法复制者只用两步简单的操作（读取原卡的卡号，写入到空白卡内），一张复制卡完成诞生。由于这种生产部署过程的“偷工”，此类门禁卡可以在擦肩而过的瞬间被读走卡号，接下来即可制作出复制卡，卡的复制比传统配钥匙过程更简单 [3]。随着

NFC 功能在智能手机上逐渐普及，手机复制小区门禁、手机复制电梯卡、手机复制门禁考勤卡日益普遍，甚至已逐渐成为一种新型的“时尚”。

3 无卡门禁系统

有卡门禁系统无论系统或卡多么先进，如果身份鉴别用的卡被复制、遗失、被盗，未及时挂失都很难完全阻止被非法冒用。无丢卡烦恼，不受忘带卡影响的无卡门禁系统应运而生。

3.1 电子密码门禁

电子密码门禁系统比较传统，从传统密码文件柜、密码保险柜、密码门锁演变而来，广泛用于银行、商超的员工通道出入口等。密码键盘通常分为固定（顺序）键盘和无序键盘，固定键盘使用时需特别注意防窥视，容易被他人模仿，对于使用时间长且密码很少更改的电子密码门禁，他人甚至可能通过观察个别按键磨损或脏污的情况猜测密码，存在安全风险。电子密码门禁系统的主要优点是安全性较高，不需要使用者惦记携带卡片来操作，入门方便轻松，即时需要临时增加用户也只需口授密码即可。

3.2 生理特征识别门禁

利用人的生理特征进行身份识别的技术措施已成为现在信息安全领域的科研热点，相应的识别技术随着计算机图像处理等技术的突飞猛进发展已取得巨大成果，各种更安全、更便捷、更准确的生物识别技术层出不穷。生理特征识别被认为是高可靠性的身份鉴别方式，优势是无需携带任何载体，也不用背诵密码，不但快捷、方便，而且准确、可靠；缺点是系统的安装和配置的成本较高，有时识别成功率较低，部分早期型号版本鉴别时易被仿冒假体欺骗。

1. 指纹识别。指纹识别对人类手指末端皮肤上的凹凸纹理，处理分析后进行身份鉴别，是目前应用最为广泛，使用方便，技术相对成熟的生理特征识别技术，广泛用于门禁、考勤、手机支付等方面。但也存在一些问题，如识别时需保持手指干燥，指纹磨损或有蜕皮现象时，识别成功率会较低，且有可能被复制指模等方式欺骗。

2. 人脸识别。人脸识别对数字影像设备捕获到的，含有人脸画面的照片或视频，进行检测和跟踪，并根据个体面部特征进行身份鉴别。人脸信息属于个人生物信息，具有独特性、不可更改性，人脸数据采集过程不需要被识别个体特别配合即可完成，具有易采集性。人脸识别应用在门禁领域非常利于实现“防尾随”功能，人脸识别除技术层面需要进一步攻克角度、遮挡物（如口罩）等困难外，对人脸识别采集到数据的管控使用已上升至法律层面，人脸数据一旦泄露，被采集者无法通过挂失改密等方式弥补，毕竟脸是换不了的。

3. 虹膜识别。虹膜识别对人眼虹膜的特征来进行身份鉴别，具有很高的精度和稳定性，已广泛应用在金融、边防和门禁等领域，但在假体辨识上仍有进一步改进空间 [4]。

4. 静脉识别。静脉识别是通过静脉识别设备（红外线摄像机等）捕获被采集人的静脉分布图像，使用专用的图像处理比对算法，将特征信息从静脉分布图像中计算得出，并存储特征值。身份鉴别时，将新采集到的静脉特性信息与存有的信息库进行比对，鉴别判断被采集人是否已授权。静脉识别中指静脉识别最为普遍，静脉识别主要长处在于属人体内部信息，不受表皮粗糙度、温湿度等干扰、检测操作容易，并且在适用性和精准度方面有优势，无法仿冒。优势虽突出，部署费用高，制造难度大，且采集设备要求特殊，目前还未能大范围推广 [5]。

5. 声纹识别。声纹识别技术通过提取个体话音中的特征图谱，利用计算机信息识别技术，鉴别区分当前说话者的身份。在网络支付、监听反恐、生存认证等方面有较好的应用，目前仍有不少技术难题待解决，是身份鉴别有效的辅助手段 [6]。

4 门禁安全的展望

单种身份鉴别措施的门禁系统多有部分不足的地方，为了更加有效地对重要场所的人员出入进行管控，杜绝窥视模仿、伪造、冒用等违规风险，“卡加密码”“生理特征识别加密码”的门禁系统有效地取长补短，弥补了意外风险的短板。

未来的门禁系统，除在加密技术、鉴别精度等方面不断改进提高外，会结束其现有单线发展的孤独状态，将成为安防大系统的核心子系统，汇聚形成效能强大的安全技术防范系统，为智慧安防事业贡献自身的关键力量。

参考文献：

[1] 卢希 .M1 公交卡被克隆篡改频频发生 存量 M1 卡转换刻不融缓 [J]. 中国建设信息化 ,2018(09):38-39.
[2] 张少华 . 后 M1 时代门禁一卡通系统非接触 IC 卡技术的新发展 [J]. 中国安防 ,2010(09):93-95.
[3] 梁穗詠 . 国内门禁市场产品的安全探讨 [J]. 中国安防 ,2011(06):63-65.
[4] 李海青 , 孙哲南 , 谭铁牛 . 虹膜识别技术进展与趋势 [J]. 信息安全研究 ,2016(01):40-43.
[5] 赵宇 . 浅谈门禁系统发展及技术趋势 [J]. 中国公共安全 ,2016(05):67-70.
[6] 郑方 , 李蓝天 , 张慧 , 等 . 声纹识别技术及其应用现状 [J]. 信息安全研究 ,2016(01):44-57.