**علی خواجه**

# حملات رایج بر کارت های هوشمند

## تاریخچه کارت های هوشمند

براساس گزارش های منتشر شده، اولین کارت هوشمند حاوی یک ریزپردازنده، در سال 1967 میلادی و توسط دو مهندس آلمانی ابداع شد. این اختراع منتشر نشد تا اینکه یک روزنامه نگار فرانسوی در سال 1974 م، اختراع کارت هوشمند را در فرانسه به ثبت رساند و خبر ظهور این فناوری را منتشر کرد.

با رشد فناوری ساخت و تولید، هزینه تولید یک کارت هوشمند به شدت کاهش یافت تا اینکه در سال 1984 م، با بهره گیری اداره های پست و مخابرات فرانسه ازکارت های تلفن، واقعه مهمی به ثبت رسید. از این تاریخ به بعد، انحصار کارت های هوشمند تنها به عنوان کارت های بانکی، شکسته شد و امروزه کاربردهای گسترده ای از این نوع کارت ها در جامعه مشاهده می گردد.

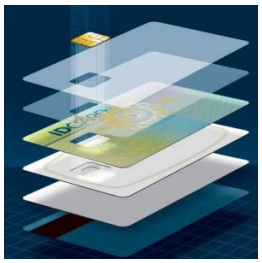
## کارت هوشمند چیست

كارتهاي هوشمند (SMART CARD) كارتهايي هستند كه از يك قسمت پلاستيكي تشكيل گرديده اند كه در داخل آنها يك چيپ ميكروپروسسور (MICROPROCESSORCHIP ) قرار دارد و اطلاعات لازم روي اين چيپها قرار مي گيرند. ميزان و تنوع اطلاعاتي كه در كارت ذخيره مي گردد، به توانايي چيپ داخل آن بستگي دارد . یک نوع حافظه یا ریزپردازنده که دادهها را ذخیره و منتقل میکند. اینها معمولاً حاوی اعتبار یا اطلاعات و گاهی هردو میباشند و در تراشه کارت، ذخیره و پردازش میشود. دادههای درون کارت از طریق یک کارتخوان که بخشی از یک سیستم محاسباتی است خوانده میشود

## ساختمان کارت

اکثر کارتهای تراشه از لایه هایی با مواد مختلف ساخته شدهاند، یا لایه هایی که بطور صحیح به هم وصل شده و باعث میشود به کارت دوام و قابلیت خاصی بدهد. امروزه کارت معمولی از ماده ،PVCپلی استر یا پلی کرنت ساخته می شود. ابتدا لایه های کارت چاپ می شوند سپس بصورت ورقه ورقه با فشار زیاد رویهم

قرار میگیرند. مرحله بعدی بلنکینگ و برش زنی است. این کار پس از اضافه کردن یک تراشه و بعد از افزودن دادهها به کارت است. بطور کلی، ممکن است 30مرحله برای ساخت یک کارت وجود داشته باشد. همه اجزاء، شامل نرم افزار و پلاستیکها، احتمالاً تعداد 12آیتم جداگانه، همه در یک پکیج واحد قرار میگیرند که برای کاربر مانند یک وسیله ساده بنظر می رسد



انواع مختلف كارتهاي هوشمند كه امروزه استفاده مي شود، كارتهاي تماسي ، بدون تماسي و كارتهاي تركيبي هستند .

**كارتهاي هوشمند تماسي** بايستي در داخل يك كارت خوان قرار داده شوند. اين كارتها يك محل تماس روي صفحه دارند كه تماسهاي الكترونيكي را براي خواندن ونوشتن روي چيپ (زماني كه در داخل كارت خوان قرار دارد)، فراهم مي آورد.

**كارتهاي بدون تماس** ، يك آنتن سيم پيچي درون خود دارا هستند كه همانند چيپ درداخل كارت ، گنجانده شده است . اين آنتن دروني اجازه انجام ارتباطات و ردوبدل كردن اطلاعات را فراهم مي آورد. براي چنين ارتباطي ، بايستي علاوه بر اينكه زمان ارتباط كاهش يابد، راحتي نيز افزايش پيدا كند. مزيتي كه اين كارت نسبت به حالت قبل دارد اين است كه نياز به كارت خوان ندارد اما بايد توجه داشت كه در اين مورد بايستي ارتباط اوليه توسط آنتن حتما برقرار گردد، درغير اين صورت نمي توان از كارت استفاده كرد .

**كارتهاي تركيبي** ، به عنوان هم كارتهاي تماسي و هم كارتهاي بدون تماس عمل مي كنند و در حقيقت داخل اين نوع كارتها هم چيپ الكترونيكي و هم آنتن وجود دارد وچنانچه كارت خوان وجود داشته باشد از كارت خوان مي توان استفاده كرد و چنانچه وجود نداشته باشد ، از آنتن كارت مي توان ارتباط را برقرار كرد.

شايد اين سوال پيش آيد كه چرا از كارتهاي هوشمند (كارتهاي حافظه دار) به جاي كارتهاي مغناطيسي استفاده مي شود ؟

پاسخ این است که ذخیره سازي اطلاعات در کارتهاي هوشمند هزار مرتبه بیشتر ازکارتهاي مغناطیسي است . مزیت دیگر اینکه این کارتها از سرعت ذخیره سازي بالا ومکانیسم هاي ایمني قویتري برخوردارند.

**چرا کارت هوشمند**

کارتهای هوشمند امنیت هر نوع معامله را بهبود میبخشند. امکان دستکاری کاربر در ذخیره سازی و شناسایی حساب در این کارتها وجود ندارد. ثابت شده است که سیستمهای کارت هوشمند قابل اعتمادتر از دیگر کارتهای ماشینخوان، نظیر نوارمغناطیسی و بارکد هستند.

ویژگیهاي کارت هوشمند

- صداقت (LOYALITY )
- کنترل دسترسي
- میزان حافظه
- امکان برنامه نویسي

**مشخصات فیزیکی کارت هوشمند**

ابعاد معمول 54 mm*85/6 mm مدتهاست که برای کارتهای هوشمند استفاده می شود.تقریبا تمام کارتها در این فرمت تولید می شود .این فرمت ID-1 نام دارد و سایز آن در استاندارد ISO 7810 آمده است .این استاندارد در سال 1985 بوجود آمد و در آن هیچ ایده ای از قرار دادن تراشه در کارت وجود ندارد .

بخاطر تنوع در ابعاد کارتهای در دسترس اغلب سخت است که تعیین کرد یک کارت خاص واقعا یک کارت هوشمند ID-1 است. علاوه بر تراشه یکی از بهترین مشخصه های شناسایی , ضخامت کارت می باشد.اگر ضخامت یک کارت حدود 0/76mm باشد وکارت حاوی یک میکدو کنترلر باشد می توان آن کارت را با استفاده از استاندارد ISO یک کارت هوشمند در نظر گرفت.

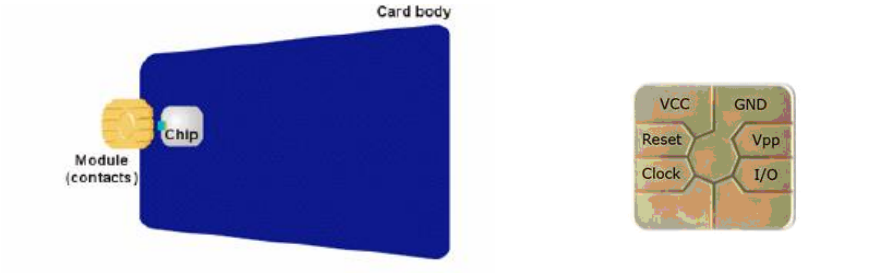
مزیت فرمت ID-1 سادگی کاربرد عملی آن است.این فرمت آن قدر بزرگ نیست که نتواند در یک کیف بقلی قرار گیردو آنقدر کوچک نیست که گم شود.بعلاوه انعطاف پذیری آن یک مشخصه مهم است . با این همه این فرمت برای تمام کاربردها مناسب نیست.برای کاربرد هایی که به قطعات کوچکتری نیاز داریم از فرمتهای دیگری تعریف می شود.

**دسته بندی های کارت هوشمند**

دسته بندی بر اساس سطح تماسی ،دسته بندی براساس نوع تراشه

**کارت‌هاي هوشمند تماسي(Contact Smart Card)**

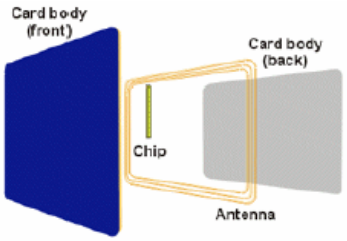
براي استفاده از اين قبيل کارت‌ها، بايد اتصال فيزيکي بين کارت و دستگاه کارت‌خوان برقرار گردد. داده‌هاي موجود برروي کارت به صورت سريال به کارت‌خوان ارسال مي‌شود و پس از پردازش، اطلاعات جديد از طريق همان پورت به روي کارت منتقل مي‌شود. به عنوان نمونه، کارت‌هاي تلفن عمومي جزو اين دسته محسوب مي‌شوند. مشکل اصلي اين قبيل کارت‌ها، خراب شدن کنتاکت‌هاي فلزي (محل‌هاي تماس) بر اثر عوامل خارجي نظير ضربه و شرايط فيزيکي محيط است




قسمت‌هاي مختلف محل‌هاي تماس کارت‌هوشمند با کارت‌خوان

**کارت‌هاي هوشمند غيرتماسي(Contactless Smart Card)**

در اين نوع کارت هوشمند، ارتباط بين کارت و کارت‌خوان به‌صورت فيزيکي بر قرار نمي‌شود؛ بلکه از طريق ميدان‌هاي الکترومغناطيسي و يا امواج RF صورت مي‌گيرد. براي برقراري ارتباط، آنتن مخصوصي بين تراشه‌هاي کارت قرار داده شده است که در فاصله‌هاي کم، تا حدود 50 سانتيمتر، مي‌تواند ارتباط ايجاد کند. کاربرد اصلي اين قبيل کارت‌ها در مواردي است که عمليات مورد نظر بايد سريع انجام گيرد، به عنوان نمونه مي‌توان به کارت‌هاي مترو اشاره کرد. مزيت اصلي اين قبيل کارت‌ها علاوه بر سهولت استفاده، عمر طولاني‌تر و ضريب ايمني بالاتر آن است؛ زيرا در اين نوع کارت، تراشه به همراه آنتن در ميان لايه‌هاي تشکيل‌دهندة کارت قرار مي‌گيرد. در شکل زير نمونه از اين کارتها نشان داده شده است.



**كارت‌هاي هوشمند تركيبي(Dual-Interface Smart Card)**

اين نوع كارت تركيبي از كارت‌هاي هوشمند تماسي و غيرتماسي است كه با هر دو نوع دستگاه‌هاي كارت‌خوان سازگار است. از اين نوع كارت‌ها براي ساخت كارت‌هاي چندمنظوره استفاده مي شود. .

**برنامه پویا سیستم عامل کارت**

این نوع سیستم عامل، که شامل کارت جاوا و انواع کارت اختصاصی MULTOSهستند سازندگان را قادر میسازند تا برنامه های کاربردی ایمن روی کارت را بسازند و پس از آزمایش بکار برند. زیرا سیستم عامل و برنامه های کاربردی بیشتر جدا هستند بروز رسانی امکان پذیر است

**کارت هوشمند خوان ها و ترمینالها**

کارت ها و ترمینالها با کارتهای هوشمند راه اندازی می شوند تا اطلاعات کارت جهت اجرا تراکنش را دریافت کنند. بطور کلی، یک کارتخوان با یک PCارتباط برقرار میکند تا آنچه را که مورد نیاز است، پردازش کند. ترمینال یک دستگاه خود پردازشگر است. کارت خان ها و ترمینال ارتها بر روی کارت های هوشمند کار نوشتن و خواندن را انجام میدهند

**دسته بندی بر اساس نوع تراشه**

**انواع تراشه های کارت هوشمند**

تراشه های دارای حافظه (Memory Chips) , مدارات مجتمع خاص منظوره,تراشه های دارای ریز پردازنده (microprocessor chips).

**تراشه های دارای حافظه**

این نوع کارت شامل واحد های حافظه است و توسط یک سیستم امنیتی سخت افزاری محافظت می شودو ساده ترین نوع تراشه هستند که تنها حجم کمی داده را در خود ذخیره می کنند و قابلیت پردازش ندارند.در حافظه ROM این کارتها اطلاعات ایستا مانند نام یا شناسه و در حافظه EEPROMاطلاعاتی که در طول زمان تغییر می یابد ذخیره می گردد.از جمله کاربرد های این کارتها می توان به کارت تلفن همگانی ،سیستم کنترل و شناسایی اشاره کرد.

**مدارهای مجتمع خاص منظوره**

این تراشه ها قابلیت نگاه داشتن داده و برخی عملیات پردازشی را دارند.این قابلیت پردازش این تراشه ها را در مقایسه با تراشه های دارای حافظه بسیار قدرتمند می سازد و علاوه بر امکان پردازش ساده،امکان رمزنگاری ایست ومحدودی را فراهم می سازند.این تراشه ها برای انجام کاری خاص برنامه ریزی شده اند و مانند تراشه های دارای حافظه  قابل برنامه ریزی شدن نیستند.

**تراشه های دارای ریز پردازنده**

پیچیده ترین و قدرتمند ترین نوع در این سه رده ،تراشه های دارای ریز پردازنده (CPU+Memory)هستند و عملکرد این پردازنده ها شبیه کامپیوتر با سطحی پایین تر از انعطاف پذیری نرم افزاری هستندو قدرت پردازش اطلاعات و انجام محاسبات را داراند.این تراشه ها مانند دو نوع قبلی می توانند داده ها را در خود نگه دارند.نقش هر یک از واحدها ی حافظه در این نوع کارتها به این صورت است:

MASK ROM :نگهداری سیستم عامل کارت هوشمند

RAM :نگهداری موقت داده ها

EEPROM :نگهداری داده های کاربردی و داده های مرتبط با آن

واحد واسطه (interface)این کارت ممکن است به یکی از صورتهای تماسی ،غیر تماسی و یا ترکیبی باشد که وظیفه برقراری  ارتباط با محیط خارج از کارت را بر عهده دارد.

**اجزای اصلی کارت**

**چاپ و برچسب گذاری-  برجسته سازی- تصویر سه بعدی- قاب نشانگر- اجزای لمسی- علامت مغناطیسی- پیمانه تراشه- انتن**

**ریز کنترل کننده های کارت هوشمند**

**پردازشگر–  حافظه (ROM- SRAM-DRAM-EPROM- Flash & EEPROM )-سخت افزار تکمیلی (کمکی)-**

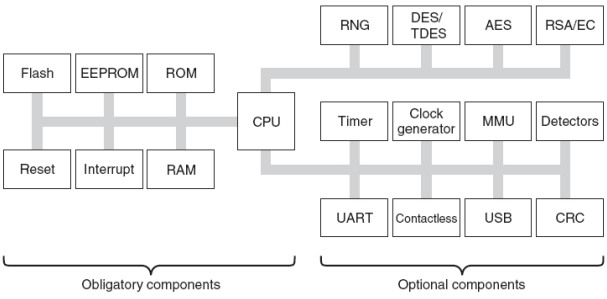
**پردازشگر**

برچسب های فروش ریزکنترل کننده های کارت هوشمند فعلی را نگاه کنید خواهید دید که بیشتر انها همچنان یک سی پی یو 8 بیتی دارند این معمولا یک سی پی یو 8051 ساده است  قدرت پردازش چنین سی پی یویی برای تمام سیستم های عملیاتی که مفسر ندارند کافی است. با این حال اگر سیستم عملیاتی باید یک مفسر جاوا ایجاد کند، اولویت مجزایی برای ریزکنترل کننده های با پردازش گر های 16 بیتی وجود دارد. برخی از این پردازشگر ها نیز بر اساس ارایش و ساختار 8051 اصلاح شده هستند.

چند ریزکنترل کننده کارت هوشمند هم هستند که بر اساس گروههای پردازشگر 32 بیتی معروف هستند: از قبیل ARM 7 یا MIPS. عامل محدود کننده برای استفاده از چنین پردازشگر های با کارایی بالا ناحیه تراشه انهاست. رابطه کم و بیش مستقیمی بین ناحیه تراشه و قیمت وجود دارد و یک پردازشگر 32 بیتی یک ناحیه بمراتب بزرگتری نسبت به یک پردازنده 8 بیتی اشغال می کند. اغلب به صرفه تر این است که در بهینه سازی سرعت نرم افزار سرمایه گذاری کرد تا اینکه از پردازشگری استفاده کرد که به ناحیه تراشه بیشتری نیازمند است

**سخت افزار تکمیلی (کمکی)**

علاوه بر یک پردازشگر و حافظه مرتبط ان ریزکنترل کننده های کارت هوشمند انواع گوناگونی از سخت افزار های کمکی تشکیل می دهند. علامت زمان سنجی که مستلزمه کارت هوشمند است معمولا توسط خروجی ایجاد می شود. با این حال همینکه استانداردهای مرتبط بسامد این علامت زمان سنجی را تا یک بازه 1 تا 5 مگاهرتز محدود می کنند، بتدریج ریزکنترل کننده های بیشتری تقویت کننده زمان سنج درونی یا مدارات مولد زمان سنجی را در بر می گیرند.




نمودار قالب یک ریزکنترل کننده کارت هوشمند با

گزینش اجزای رایج امروزی که از طریق یک ادرس مشترک دادها و گذرگاه های (کانال های الکترونیکی برای انتقال داده ها) کنترلی به سی پی یو متصل می شوند. در صورتی که از حافظه فلش استفاده شود حافظه های رام و ایپرام در برخی از گونه های ریزکنترل کننده ها ممکن است حذف شوند.

**حافظه**

علاوه بر یک پردازشگر هر ریزکنترل کننده به چندین نوع حافظه با ویژگی های مختلف نیاز دارد. نوع اصلی حافظه ی غیر فراری که در ریزکنترل کننده های کارت هوشمند استفاده می شوند، رام می باشد. در صورتی که اطلاعاتی که در حافظه قرار دارند در عمل باید اصلاح شوند، از حافظه پاک شدنی الکترونیکی (ایپرام) استفاده می شوند.

در کنار ریزکنترل کننده های با رام و ایپرام، از شمار پیوسته روز افزونی از تراشه ها با حافظه فلش (فلش ممووری) نیز استفاده می شود. حافظه فلش نوعی ایپرام با ابعاد پیلی و سلولی کوچک شده است، اما بر خلاف ایپرام نمی توان انرا بصورت بایتی پاک کرد یا رایت کرد. حافظه فلش می تواند نقش ها و وظایف رام و ایپرام را بر عهده گیرد.

در حال حاضر، زمان پاک کردن و رایت کردن بطور نمونه هر کدام 3.5 هزارم ثانیه و تعداد تضمینی چنین دسترسی هایی 500000 است. این امر تاثیر بزرگی روی طراحی سیستم عملیاتی و نرم افزار کاربردی دارد.

رم ایستا بعنوان حافظه فرار برای ذخیره اطلاعات در طول عملیات استفاده می شود.

انواع مختلف حافظه هاي الكترونيك وجود دارند مشخصه هاي كلاسيك اندازه حافظه زمان دسترسي به داده هاي ذخيره شده درآن ، الگوهاي دسترسي و غيره هستند . براساس يك نوع طبقه بندي حافظه ها به سه دسته تقسيم مي شوند : حافظه خواندني نوشتني ( RWM ) ، حافظه غير قرار خواندني نوشتني (NVRWM) و حافظه هاي خواندني ( ROM)

**ROM**

حافظه هاي ROM توليد انبوه دارند زيرا ساده ترين شكل حافظه نيمه رسانا هستند اين حافظه بيشتر براي سيستمهاي عامل يا ذخيره دستورالعملها يا ثوابتي براي كارتهاي هوشمند استفاده مي شود درحافظه هاي ROM كلاسيك فقط خط كلمه مي تواند در يك زمان بالا باشد . ما مي بينيم كه وقتي R1 بالا مي رود ستون C5, C3 , C1 پايين مي آيد . ترانزيستور در بخش بالايي عكس شبيه L هاي طويلي هستند كه به بالا كشيده شده اند . خطهاي ستوني C4, C2 از ميان L طويل ترانزيستور بالا كشيده مي شوند اگر اطلاعاتي كه در حافظه قرار است ذخيره شود ناآشنا و جديد است ، هر آرايه حافظه با يك كانال ترانزيستور به

ازاي هر فصل مشترك يك رديف و يك خط ستون سخته مي شود حافظه توسط قطع ارتباط بين يكي ازسه ترمينال ترانزيستور و ستون خطي برنامه نويسي مي شود.

**حملات رایج بر کارت های هوشمند**

**حملات از طریق خروجی به دارنده کارت و مالک کارت**

این طبقه حمله همچنین با نام **مشکل خروجی موثق** شناخته می شود. دارنده کارت باید تا حدی به خروجی مطمئن باشد که خروجی همان کاری را که دارنده کارت می خواهد انجام دهد. این نکته در سیستم تعیین هویت الکترونیک به دلیل خدمات امضای دیجیتالی بسیار مهم است. در صورتی که دارنده کارت می خواهد اطلاعاتی را امضا کند او باید به نوعی اعتماد داشته باشد که خروجی هیچ چیز دیگری به جز اطلاعات و داده های درخواست شده را امضا نمی کند. مورد بالا با کارت های مغناطیسی قدیمی علامت دار حمله با این نوع است. خروجی طوری کارت را کپی کرد که دارنده کارت متوجه هیچ چیز نشد.

**حملات از طریق دارنده کارت به خروجی**

این نوع حمله با جعل و تقلب انجام می شود یا اینکه کارت های اصلاح شده را با نرم افزاری گول زن اجرا می کنند. هدف اینست که استاندارد تبادل اطلاعات بین کارت و خروجی را بشکنند

**حملات از طریق دارنده کارت به مالک اطلاعات**

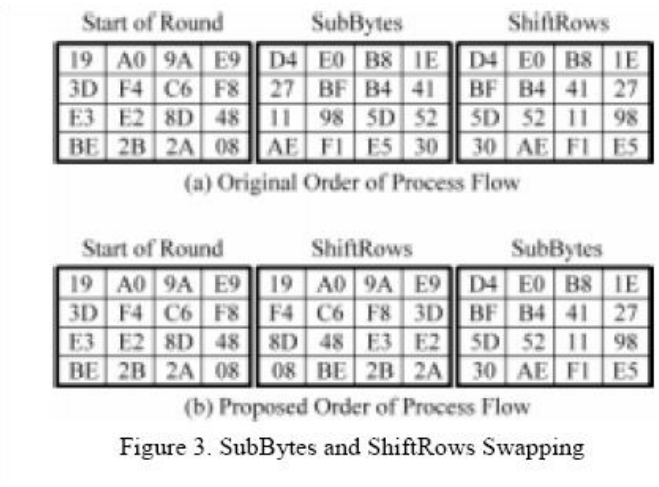
با کارت های تعیین هویت الکترونیک، این نوع حملات تنها در صورتی که کارت دزدیده شده است مربوط به ان است. مالک اطلاعات باید تنها کسی باشد که پین کد برای داده ها و اطلاعات (کلید رمز) را می داند بنابراین دارنده جدید کارت تلاش می کند تا اطلاعات را از طریق دیگری بدست اورد یا اصلاح کند. تکنیک های زیر تاکنون با موفقیت بزرگی در برابر برخی کارت های شبکه های تلویزیونی (پرداختی) و کارت های تلفن همگانی استفاده شده است. همچنین برخی از کارت های هوشمند اولیه با موفقیت هک شده اند حمله کننده ممکن است همچنین تلاش کند مستقیما حمله ای به کارت داشته باشد مثل جابجا کردن اجزای امنیتی ان یا سوزاندن برخی قسمت های حافظه. ممکن است که جابجا کردن و برداشتن ای سی از کارت چندان انجنان که ممکن است تصور شود مشکل نباشد. مدار می تواند در برخی از کارت ها با تجهیزات ازمایشگاه خانگی کاملا ارزان بشود با موفقیت انرا جابجا کرد یا برداشت بنابراین این نوع از حمله حتی با حمله کننده طبقه 1 می تواند اجرا شود.

**حملات از طرف صادر کننده علیه دارنده کارت- حملات از طریق تولید کننده علیه صاحب اطلاعات**

**Swap SubByte and ShiftRow**

بهترین ترکیب کدها و استمرا استفاده از حافظه در فرآیند Shift و Byte در شکل 2 نشان داده شده است. تعداد زمانهای خواندن ونوشتن از حافظه کاهش یافته است.در این مدل سرعت محاسبه افزایش یافته بدون به خطر افتادن نتایج واقعی ونتیجه ی کلی رضایت بخش است.

نتایج فرآیند اصلی در شکل 3(a) برابر با اولین پردازش با swapped process در شکل 3(b)است.



| Start of Round | | | | SubBytes | | | | ShiftRows | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 19 | A0 | 9A | E9 | D4 | E0 | B8 | 1E | D4 | E0 | B8 | 1E |
| 3D | F4 | C6 | F8 | 27 | BF | B4 | 41 | BF | B4 | 41 | 27 |
| E3 | E2 | 8D | 48 | 11 | 98 | 5D | 52 | 5D | 52 | 11 | 98 |
| BE | 2B | 2A | 08 | AE | F1 | E5 | 30 | 30 | AE | F1 | E5 |

(a) Original Order of Process Flow

| Start of Round | | | | ShiftRows | | | | SubBytes | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 19 | A0 | 9A | E9 | 19 | A0 | 9A | E9 | D4 | E0 | B8 | 1E |
| 3D | F4 | C6 | F8 | F4 | C6 | F8 | 3D | BF | B4 | 41 | 27 |
| E3 | E2 | 8D | 48 | 8D | 48 | E3 | E2 | 5D | 52 | 11 | 98 |
| BE | 2B | 2A | 08 | 08 | BE | 2B | 2A | 30 | AE | F1 | E5 |

(b) Proposed Order of Process Flow

Figure 3. SubBytes and ShiftRows Swapping

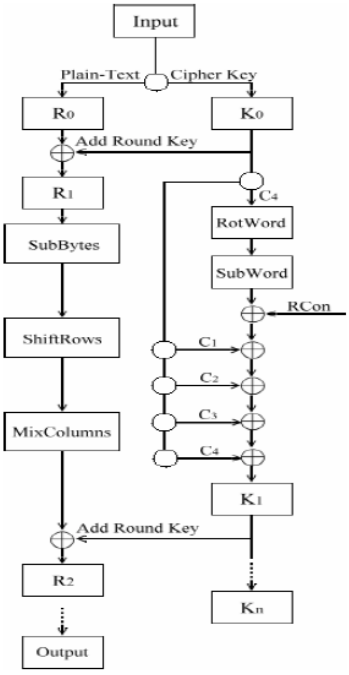



Figure 2. AES Computation Flow

**طراحی اصولی پردازشگرهای کارت هوشمند مقاوم در برابر دستکاری**

روشهایی برای استخراج نرم افزار حراست شده و داده ها از پردازشگر کارت هوشمند

تکنیکهای دستکاری

تکنیکهای ریز یابشگری را می توان جهت دسترسی مستقیم به سطح تراشه بکار برد ،بنابراین ما می توانیم این مدار همبسته را مشاهده و دستکاری کنیم.

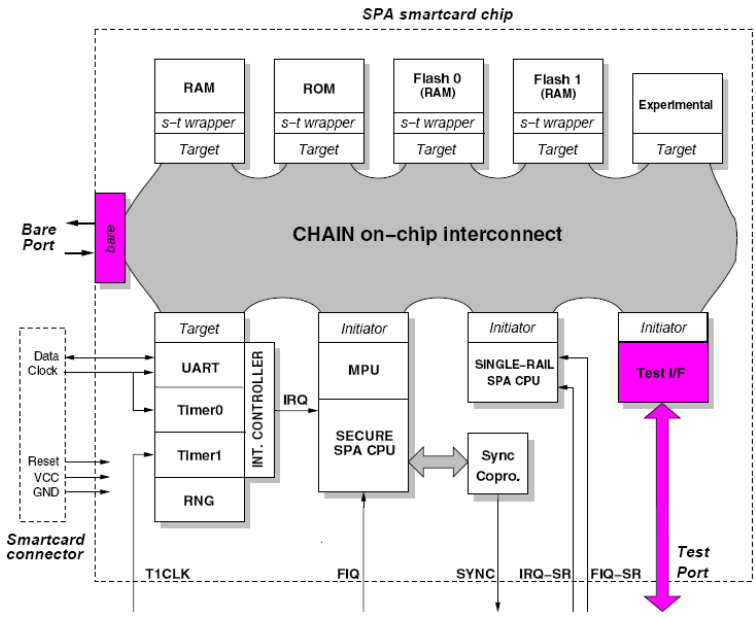
حملات نرم افزاری از رابط ارتباطی نرمال کارت هوشمند استفاده می کند و ازآسیب پذیری امنیتی یافت شده در این پروتکل ها ،الگوریتمهای رمز نگاری و اجرای آنها بهره برداری می کند

تکنیکهای استراق سمع با واکافت زمانی بالا،ویژگیهای آنالوگ تمام ارتباطات کهنه و هم کنشگر و هر تشعشع الکترو مغناطیس دیگر بوجود آمده بوسیله این پردازشگر در طول عملیات نرمال را کنترل می کند.

تکنیکهای تولید خطا شراط محیطی غیر عادی را جهت ایجاد اختلال در عملکرد این پردازشگرها بکار می برد که دسترسی اضافه ای را فراهم می کند. تمامی تکنیکهای ریز یابشگری حملات هجومی می باشند

**حملات هجومی**

**باز کردن بسته بندی کارت هوشمند- بازسازی طرح- ریزیابشگری دستی- تکنیکهای بازخوانی حافظه- تکنیکهای پرتوی ذره**




ساختار سیستم کارت هوشمند

**کاربردهای کارت هوشمند**

- **اندازه**: اندازه اين قبيل كارت كوچك است و نياز به حمل مدارك و پول را برطرف مي‌سازد.

- **امنيت**: به دليل وجود سيستم‌هاي حفاظتي روي كارت نظير رمزنگاري، از داده‌هاي موجود بر روي آن به خوبي محافظت مي‌شود.

- **حجم اطلاعات قابل‌حمل**: كارت‌هاي هوشمند قادرند حجم زيادتري از اطلاعات را در مقايسه با كارت‌هاي مغناطيسي درخود ذخيره كنند

**کاربردهاي کارت‌هاي هوشمند**

- کارت تلفن از نوع Contact
- سیم کارت موبایل
- بانکداری ( کارت های پرداخت Credit و Debit )
- کارت خرید
- پرداخت هزینه کانال های تلویزیونی
- حمل و نقل
- کارت‌هاي شناسايي

**چیپ یا تراش داخل کار ملی چیست**

تراشه هایی که در کارت های هوشمند استفاده می شوند، به دو دسته «حافظه» و «میکروپروسسور» تقسیم می شوند . این چیپ ها وظیفه ذخیره اطلاعات از اطلاعات شخصی و هویتی افراد مانند قد، وزن و شماره شناسنامه تا امضای دیجیتال را دارند و باعث هویت بخشی به صاحب کارت دردنیای واقعی و مجازی می شوند. گفته می شود این تراشه ها قابلیت ذخیره تا 84 کیلوبایت اطلاعات را دارند.

**کارت سوخت** ازنوع چیپ هائی است که دارای CPU داخلی هستنداین CPU مانند دیگر انواع متداول دارای فیوز بیت هستندهنگام ارتبا ط با دستگاه خارجی ابتدا تغذیه کارت روشن میشود سپس پسورد از سیستم درخواست میشود ودر صورت درست بودن پسورد اطلاعات کارت ارسال میشودپس ارسال اطلاعات توسط کارت مشروط به ارسال درست پسورد توسط دستگاه ریدر است واز طرفی با سوزاندن فیوز بیت مربوط عملا امکان نوشتن اطلاعات روی کارت غیر ممکن میشود توجه کنید این پسورد با پسورد خارجی که توسط کاربر انتخاب میشود فرق میکند این پسورد اتوماتیک وار با اتصال کارت به ریدر از طریق بوتلودر واحد پردازشگر کارت از دستگاه درخواست میشود وکارتخون اونو ارسال میکنه وبه همین علته که وقتی کارتی وارد شبکه شد دیگه خود سازمان هم نمیتونه اطلاعات اونو دستکاری کنه و تنها کار سوزاندن ( خارج کردن از سیستم ) و برنامه ریزی یک کارت جدیدبگذارید

# کارت های هوشمند رایج

| کارت | EEPROM ذخیره سازی | امکانات |
|---|---|---|
| SLE4418 | کیلوبایت 1 | حفاظت بتویس |
| SLE4428 | کیلوبایت 1 | حفاظت از نوشتن، کد امنیتی 2 بایت |
| SLE4432 | 256B | یکبار نوشتن Bحافظه 32 |
| SLE4436 | 221b | رام 24 بیتی، پروم 40 بیتی |
| SLE4442 | 256B | کد امنیتی 3 بایت، حافظه یک بار نوشتن 32 بایت |
| ACOS1 - 1k | کیلوبایت 1 | سه گانه، احراز هویت، پین 8 بایتی DES |
| ACOS1 - 8k | کیلوبایت 8 | سه گانه، احراز هویت، پین 8 بایتی DES |