کارت های هوشمند و بررسی امنیت آنها

فهرست مطالب

- بررسی کارتهای هوشمند (مروری بر جنبه های سخت افزاری)
- امنیت در کارتهای هوشمند

تاریخچه

- نخستین بار در سال ۱۹۷۶ توسط دانشمند آلمانی هلوت گروتپ و همکارش یورگن تهلوف اختراع شد.
- در سال ۱۹۸۲ به ثبت رسید.
- نخستین استفاده عمومی و گسترده از کارت هوشمند در ۱۹۸۳ برای پرداخت های الکترونیکی تلفن های اعتباری فرانسه به وقوع پیوست.
- در اوایل دهه ۹۰ میلادی استفاده از کارت هوشمند در کشورهای مختلف رواج پیدا کرد.

جنس کارت هوشمند

- از نوعی پلاستیک (PVC) با ابعاد حدودا ۵/۵ در ۸/۵ سانتیمتر
- یک یا چند تراشه بصورت مدار مجتمع در روی آن قرار دارد.
- این تراشه ها که عمدتا میکروپروسسور هستند مقدار زیادی اطلاعات را بصورت آنلاین و یا آفلاین ***ذخیره*** ، ***پردازش*** و ***منتقل*** میکنند.

استاندارد ایزو ۷۸۱۶

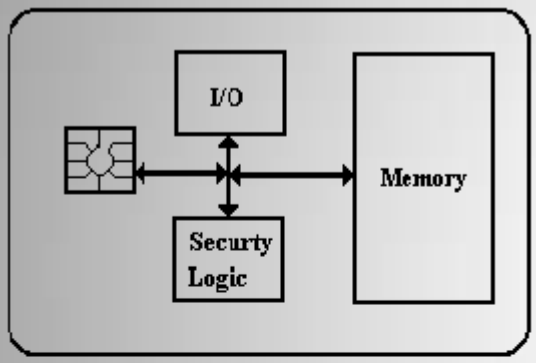
ISO 7816 در سه بعد به استاندارد سازی کارت هوشمند میپردازد:

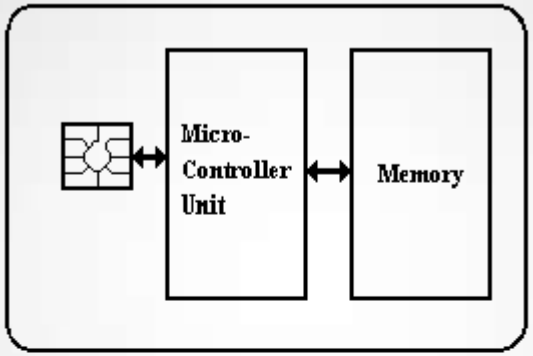
۱. **ISO 7816-1** معرف مشخصه های فیزیکی

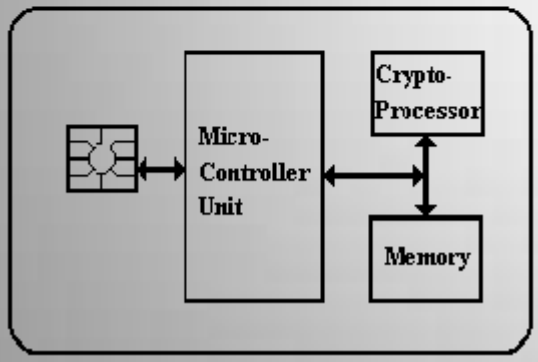
۲. **ISO 7816-2** معرف لوکیشن های پارامتر های روی کارت است.

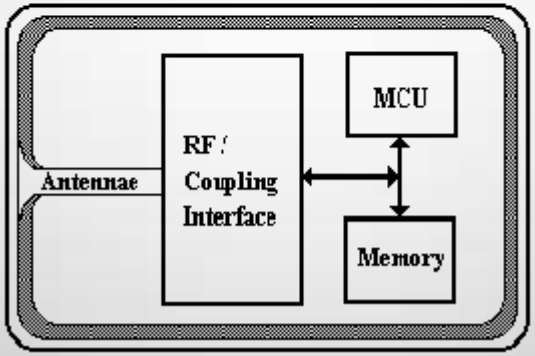
۳. **ISO 7816-3** معرف سیگنالهای الکتریکی و پروتکل های ارتباطی کارت است.

انواع کارتهای هوشمند





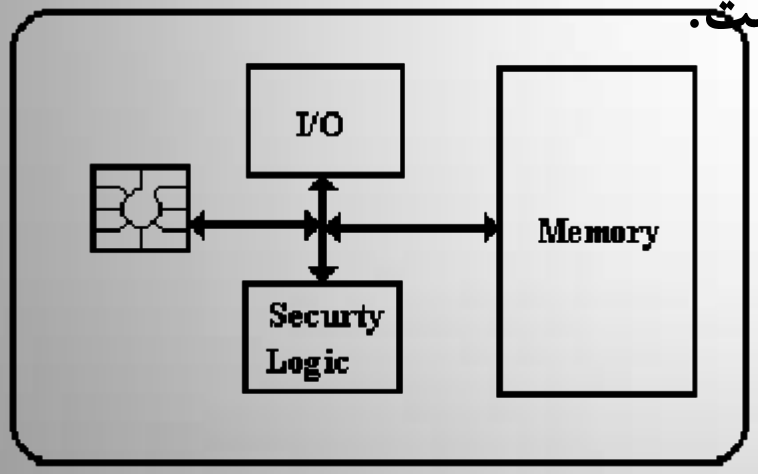




- کارت حافظه
- کارتهای دارای پردازنده
- کارتهای دارای پردازنده به همراه کمک پردازنده
- کارتهای بدون تماس

کارت های هوشمند حافظه ای

- صرفا جهت نگهداری اطلاعات مورد استفاده هستند و هیچ پردازشی روی آنها انجام نمیشود
- ارتباط بین کارت و کارت خوان (بدون وجود پردازنده) از طریق یک کانال ارتباطی که کاملا تحت کنترل دستگاه کارت خوان است هدایت میگردد.
- حافظه کارت‌های هوشمند از نوع EEPROM است.



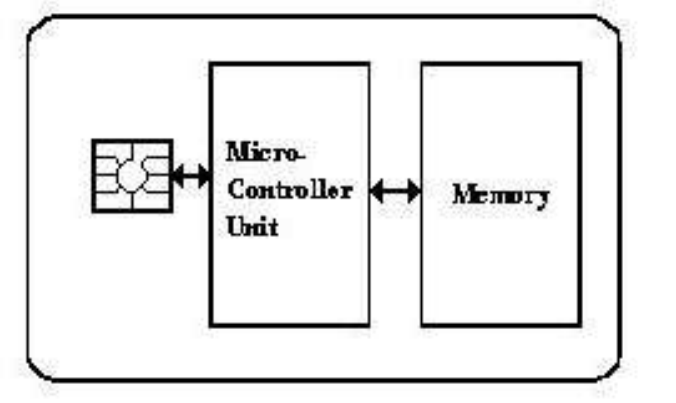
کارتهای هوشمند دارای پردازنده:

پردازنده این کارت ها از نوع میکروکنترلر می باشد که این میکرو از نوع 8051 ، PIC

و یا AVR میباشد.

پردازنده ها ۸ ، ۱۶، ۳۲ و حتی ۶۴ بیتی میباشند.

علاوه بر وجود پردازنده در آنها مقداری EEPROM , ROM,RAM و پورت IO وجود دارد.

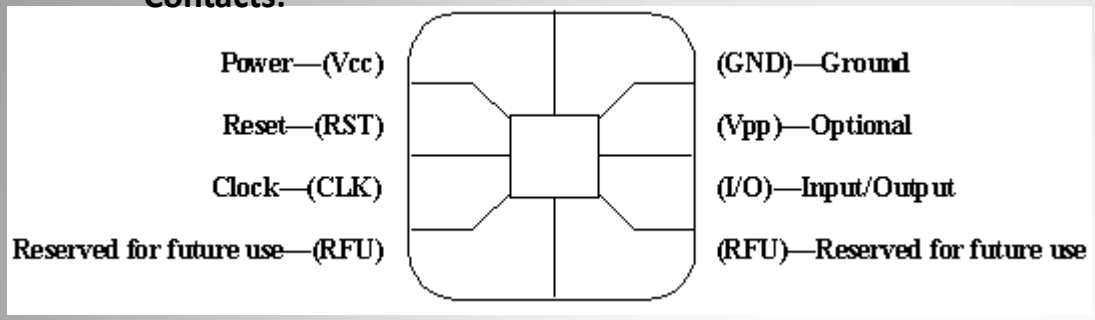


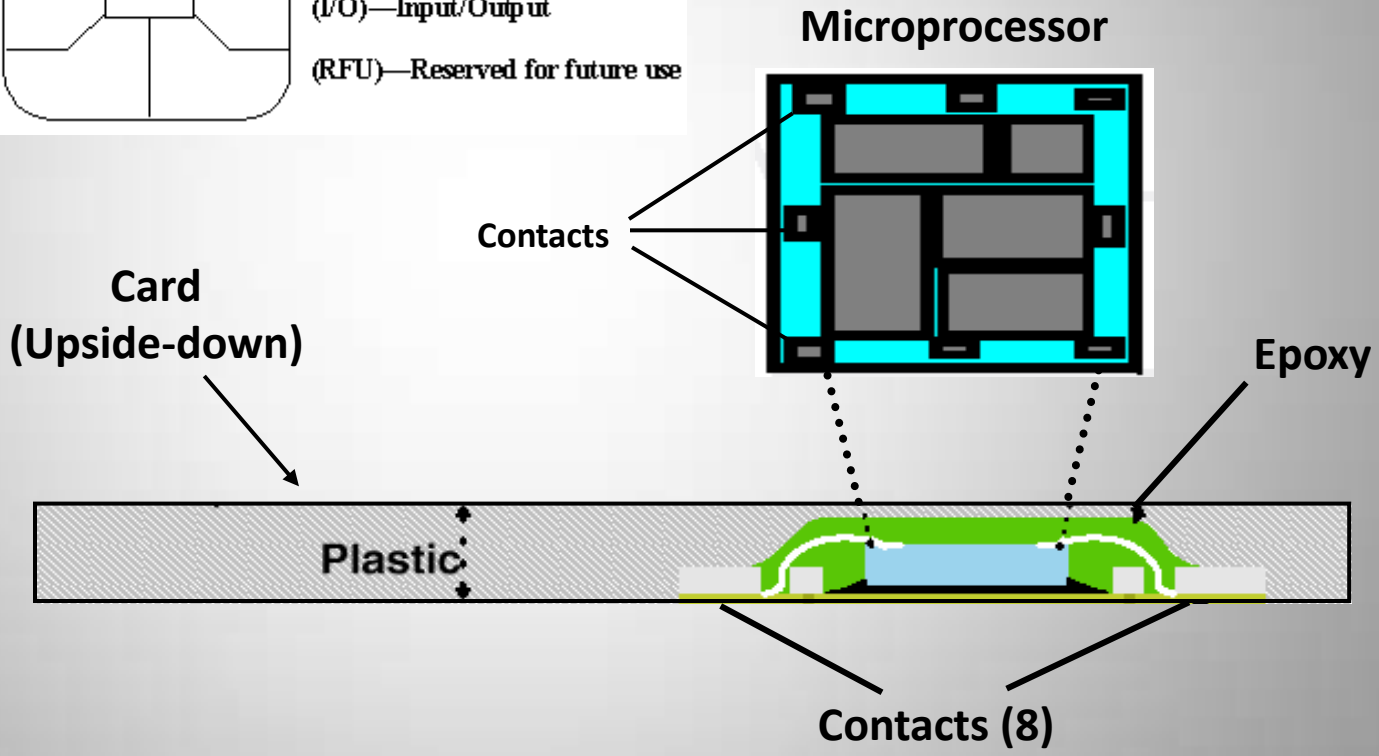
اجزای کارتهای هوشمند دارای پردازنده:

- ROM: محل قرار گیری سیستم عامل کارت هوشمند است که در طول حیات آن تغییر نخواهد کرد. حدود ۲ تا ۱۶ کیلو بایت.
- EEPROM: محل ذخیره و بازیابی داده های روی کارت است.مثلا قرار دادن یک سری کدهای اجرایی. حدود ۲ تا ۳۲ کیلوبایت .
- RAM: به عنوان حافظه موقت برای اجرای عملیات پردازشی در اختیار ریز پردازنده است. از چند بایت تا چند کیلو بایت میباشد.
- I/O Interface: یک واسط I/O ، عمل تبدیل داده های موازی داخل کارت را به داده های سری برای ارسال به کارت خوان را بر عهده دارد.
- بخش I/O: بطور معمول دارای دو خط برای تغذیه ، یک خط برای راه اندازی مجدد(Reset) ، یک خط کلاک و یک خط برای ورود و خروج داده های سریال است.

معماری کارت هوشمند پردازنده دار

Contacts:

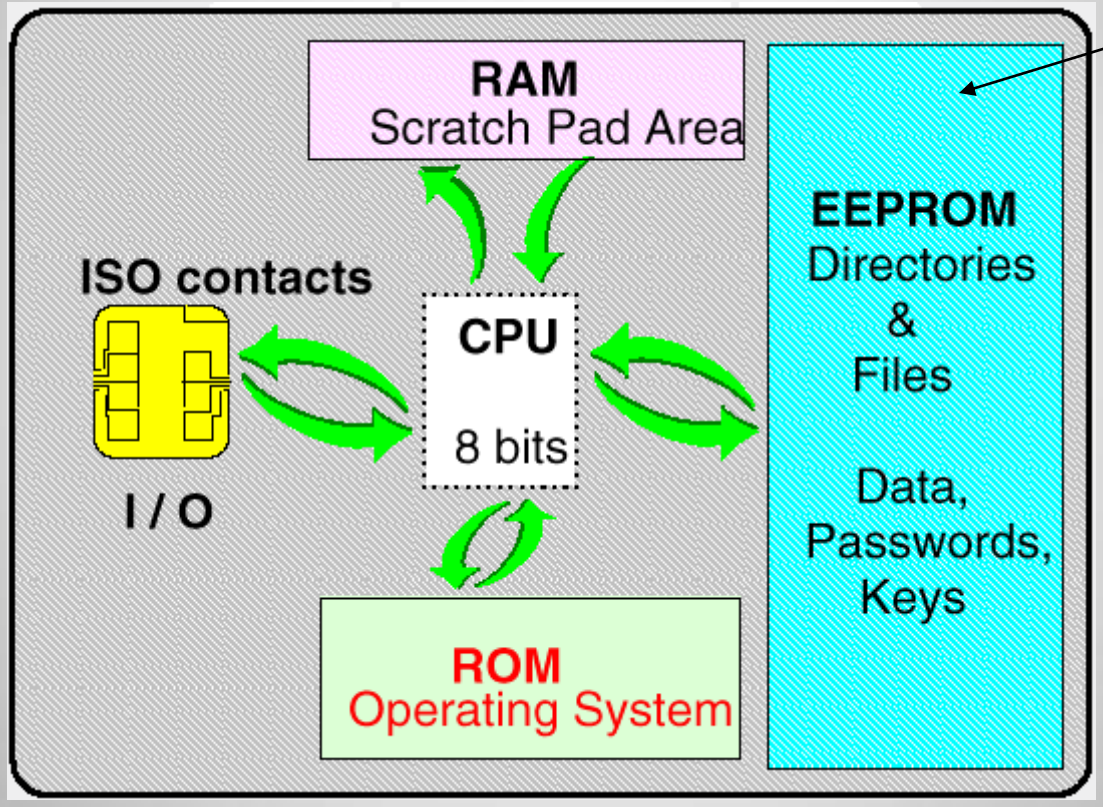




انواع پردازنده های موجود :

- پردازنده های ۸ بیتی با فرکانس 5MHZ (کارتهای قدیمی)
- پردازنده های ۱۶ بیتی با فرکانس 50-100MHZ
- پردازنده های ۳۲ بیتی با فرکانس 300MHZ
- پردازنده های ۶۴ بیتی با فرکانس 600MHZ (کارتهای جدید)

معماری کارتهای هوشمند (هشت بیتی) قدیمی



EEPROM:
Electrically
Erasable
Programmable
Read-Only
Memory

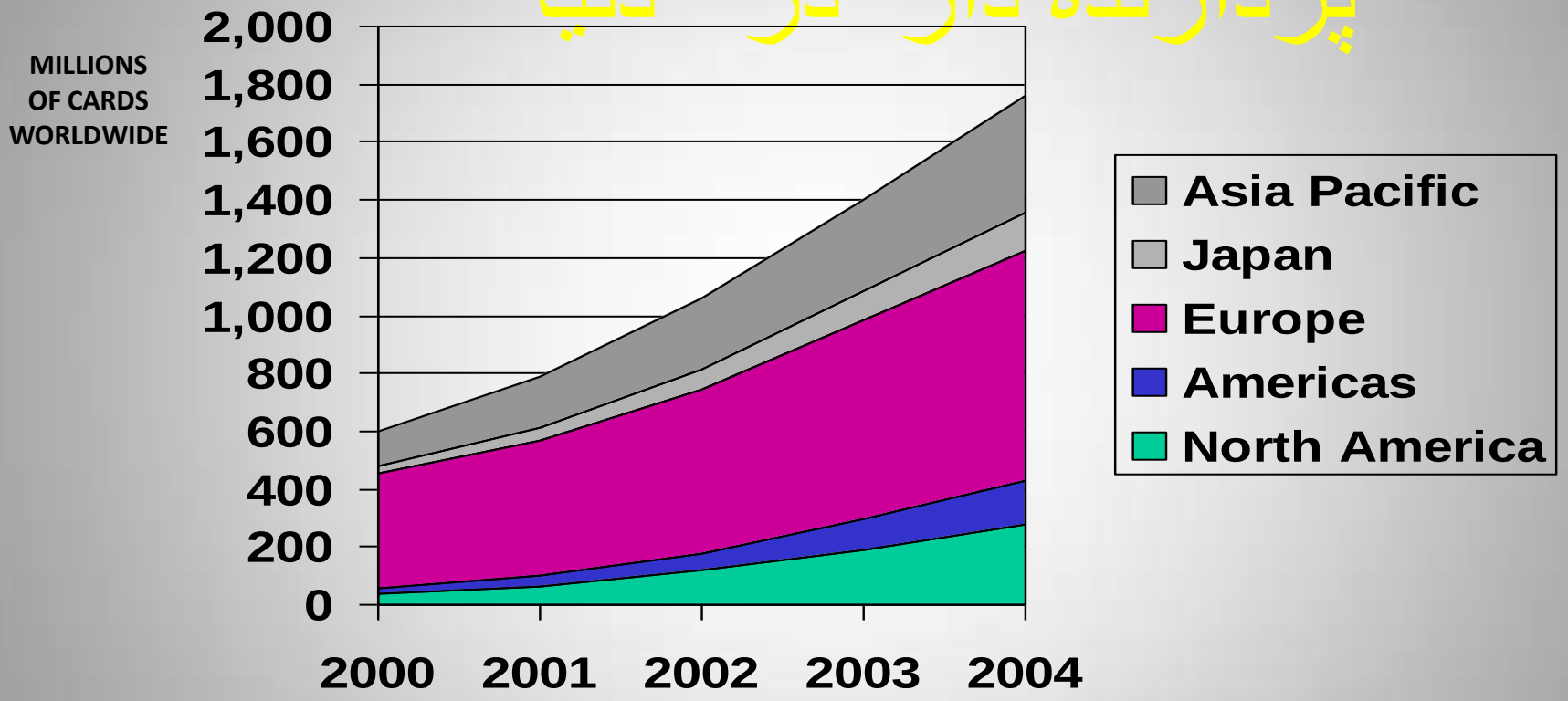
SOURCE: SMART CARD FORUM

ولتاژ کاری کارتهای هوشمند :

با پیشرفت فناوری ولتاژ کاری روز به روز در حال کاهش است. میکروها در این راستا به سه کلاس طبقه بندی میشوند:

گروه	ولتاژ	جریان مصرفی
گروه A	5 v	حداکثر 60 mA
گروه B	3 v	حداکثر 40 mA
گروه C	1.5 v	حداکثر 30 mA

تب استفاده از کارتهای هوشمند پردازنده دار در دنیا

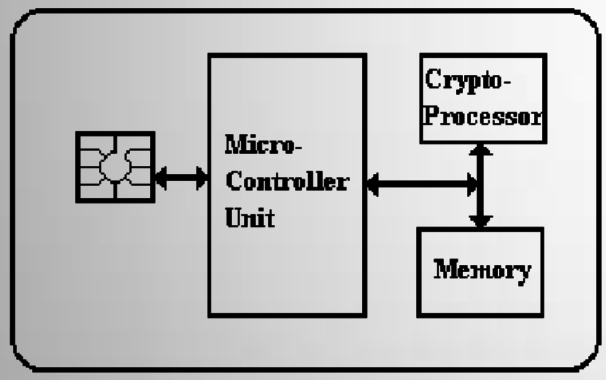


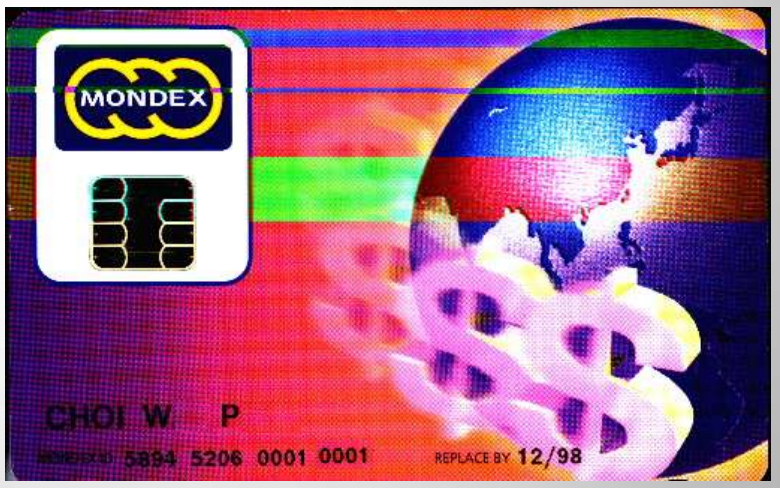
1999: 500 M microprocessor cards

2004: 1750 M microprocessor cards

کارتهای هوشمند دارای ریزپردازنده و کمک پردازنده

در کارتهای پیشرفته تر ، کمک پردازنده (یا کمک پردازنده هایی) جهت شتابدهی به برخی فرآیندها وجود دارد.





برخی از انواع کمک پردازنده ها:

۱. کمک پردازنده های رمزنگاری

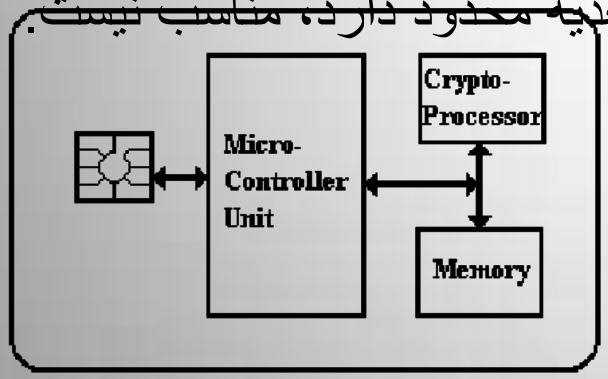
۲. کمک پردازنده های مولد عدد تصادفی

۳. کمک پردازنده های ناظر

کمک پردازنده رمز نگاری :

- برای سیستم های مالی در ارتباطات راه دور تا به حال از شیوه رمزنگاریDES استفاده شده است. و کمک پردازنده سریع و کوچکی برای آن موجوداست. در روش AES هم ، کمک پردازنده وجود دارد. برای روش های نامتقارن چون RSA و منحنی های بیضوی هم تمهیدات لازم دیده شده است.

- در حال حاضر سکوهای کارت خوان های جاوا ، نرم افزاری برای محاسبه رمز نگاری های متقارن و نامتقارن را در بردارد و اضافه کردن هم پردازنده ها به اندازه چیپ و مصرف برق آن می افزایدو برای محیطهایی که منبع تغذیه محدود دارد مناسب نیست.



کمک پردازنده مولد عدد تصادفی :

- در پروتکل هایی که پایانه های کارتهای هوشمند هویت همدیگر را احراز می کنند.
- کیفیت این اعداد تصادفی مهمند و نباید تحت تاثیر حرارت و ولتاژ قرار گیرند.
- چرا که می تواند تاثیر مهمی روی عملیات رمزنگاری بگذارد و نباید یک عدد بایاس شده در دماهای بالا یا پایین تولید شود. (این مدارات هادی هستند پس با افزایش درجه حرارت ممکن است خوب کارنکنند)
- اگر تولید عدد تصادفی زیاد حیاتی نباشد از مولدهای شبه تصادفی که معمولا سخت افزاری هستند استفاده می شود.

کمک پردازنده ناظر :

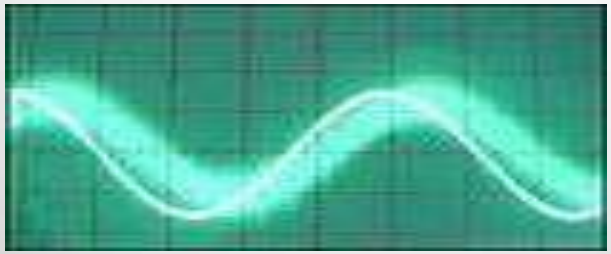
- از دیگر اجزای لازم برای یک کارت هوشمند وجود ناظران ناهنجاری است که در متوقف کردن کارت هوشمند در شرایط حاد محیطی به کار می روند.
- به این منظور حسگرهایی برای درک تغییرات نامعمول در ولتاژ یا کلاک و حرارت و .. به کار می رود. البته امنیت کارت هوشمند نباید وابسته به این حسگرها باشد.

برخی از انواع کمک پردازند های ناظر

- کمک پردازنده های ناظر بر فرکانس
- کمک پردازنده های ناظر بر ولتاژ
- کمک پردازنده های ناظر بر دما

کمک پردازنده ناظر بر فرکانس:

- حمله های تحلیل قدرت و حمله های الکترومغناطیس از فرکانس استفاده می کنند.ناظر فرکانس های بالا و پایین با کاهش سرعت کلاک به سطوح غیر مجاز در چیپ به کار می رود.وقتی فرکانس به زیر ۵۰۰ کیلو هرتز می رسد و یا وقتی به بالای ۷ مگا هرتزمی رسد، آشکار ساز کارت هوشمند را خاموش می کند .
- آشکار ساز را هم باید محافظت کرد که فرکانس آن را دستکاری نکنند.



کمک پردازنده ناظر بر ولتاژ:

- ناظر ولتاژ، اگر ولتاژ از حد بالا یا پایین عدول کرد کارت هوشمند را خاموش می کند.
- اگر چنین نباشد ممکن است با حمله های DPA کلید مخفی فاش شود.

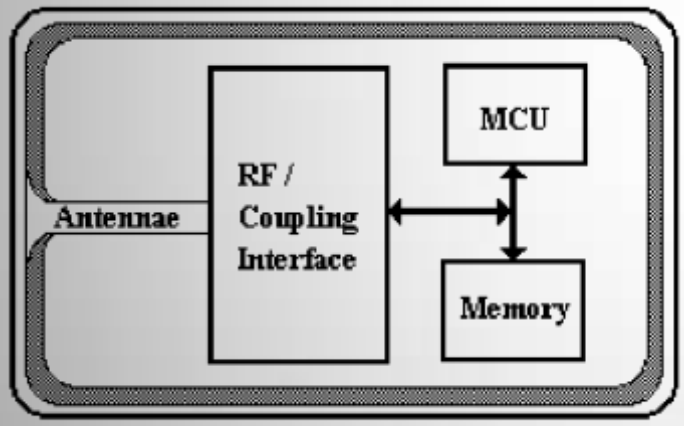
- خود این ناظران هم باید محافظت شوند.چون بعضا حمله کننده ها برای از کار انداختن ناظر کارت هوشمند، ولتاژ آن را در سطح طبیعی نگه می دارند.
- بعضی از کارت های هوشمند آشکار ساز رو ل از روشن کردن کارت ، آماده بودن شرایط را کنترل می

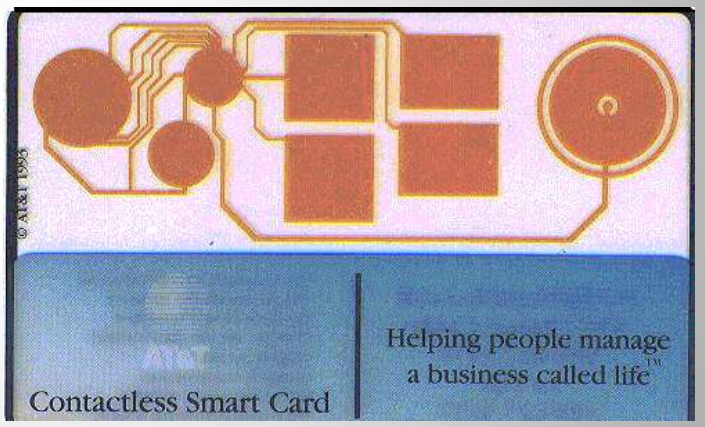
کمک پردازنده ناظر بر دما:

- سنسورهای حرارتی در بعضی چیپ ها به کار می رود.مزیت چنین حسگرهایی بحثی در میان کارشناسان برانگیخته است.
- عدول از دمای مجاز تا حدودی برای کارت قابل تحمل است و خاموش کردن کارت به این دلیل سرعت شکست ها را بالا می برد. اما بعضی حمله کنندگان از این روش برای دستکاری تولید عدد تصادفی استفاده می کنند.

کارتهای هوشمند بدون تماس

Contactless Smart Card





Radio Frequency Identification

نسل جدید کارتهای هوشمند بدون تماس هستند و با استفاده از تکنولوژی RFID با دستگاه کارت خوان ارتباط برقرار میکنند

استاندارد ISO 14443 استاندارد جهانی این کارتهاست.

ساختار کارتهای هوشمند بدون تماس:

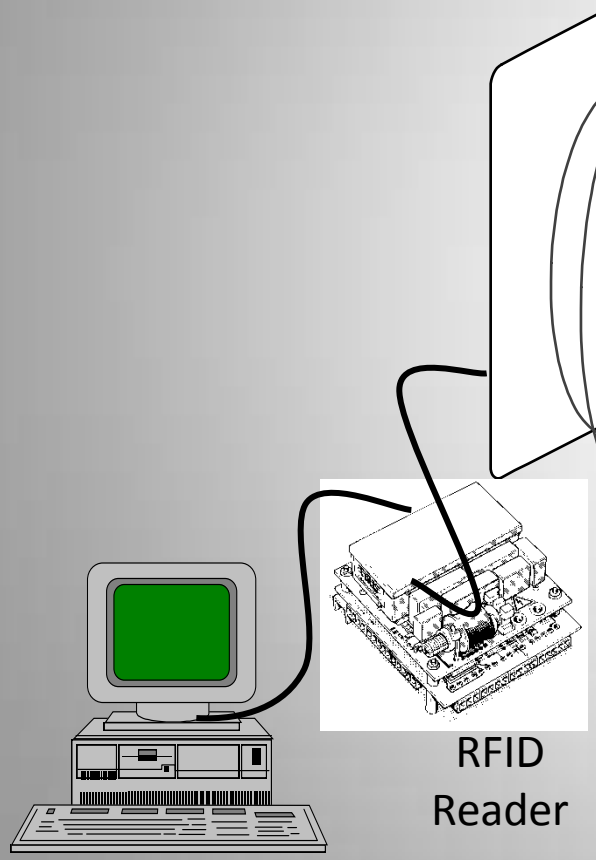
این کارتها بر اساس ارتباط فرکانسی بین گیرنده و فرستنده کار میکند.

این ارتباط بر سه نوع کوپلاژ استوار است

۱. کوپلاژ خازنی

۲. کوپلاژ سلفی

۳. کوپلاژ الکترومغناطیسی



ساختار کارتهای هوشمند بدون تماس:

کوپلاژ خازنی: بر اساس میدان الکتریکی و در رنج های فرکانسی پایین استفاده میشود و دارای کاربرد زیاد است.

کوپلاژ الکترومغناطیسی: در فرکانسهای بسیار زیاد در حد بیشتر از مگاهرتز و گیگا هرتز از آن استفاده میشود که کاربرد زیادی ندارد.

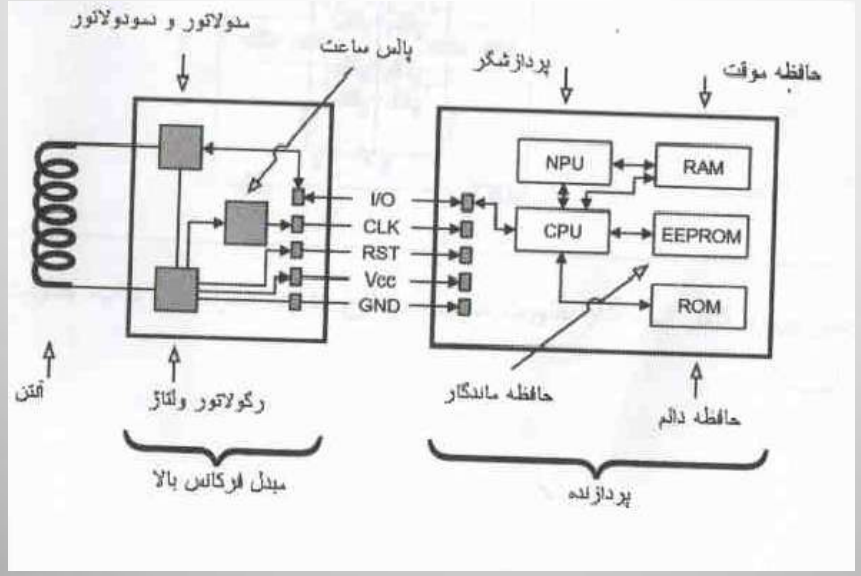
SONY RC-S833
CONTACTLESS SMART CARD

کوپلاژ سلفی:

بر اساس میدان مغناطیسی عمل کرده و اطلاعات را توسط آنتن مبادله میکند.

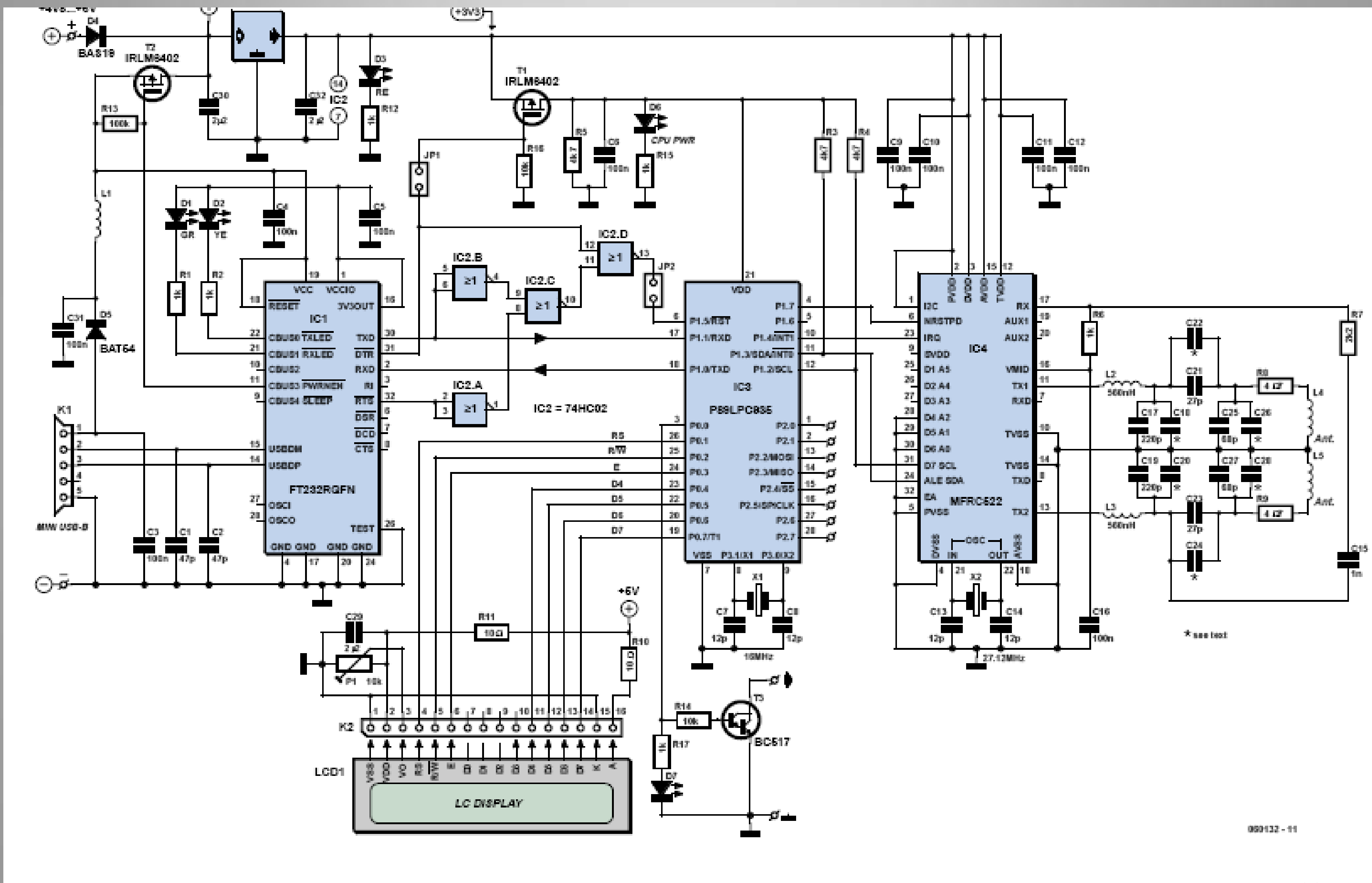
فرکانس این نوع انتقال برابر ۱۲۵ یا ۱۳۵ کیلو هرتز میباشد.

آنتن بکار رفته درداخل کارت جاسازی شده است و بیشترین کاربرد را دارد.



سخت افزار ارتباطی با کارت های RFID:

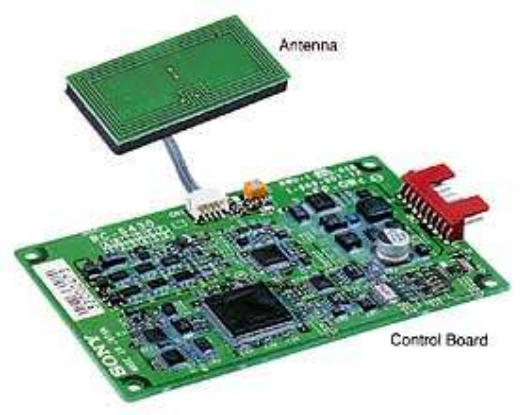
برد شماتیک سخت افزار ارتباطی با کارت RFID به نقل از مجله Elector Electronics در شکل بعد مشخص میباشد:



IC1
FT232RQFN
IC3
P89LPC935
IC4
MFRC522
IC2 = 74HC02
IC2.A
IC2.B
IC2.C
IC2.D
LC DISPLAY
LCD1
K1
K2
BAS19
IRLM6402
BAT64
BC517
+3V3
+5V
10MHz
27.12MHz
* see text
060132 - 11

تبادل اطلاعات در کارتهای هوشمند

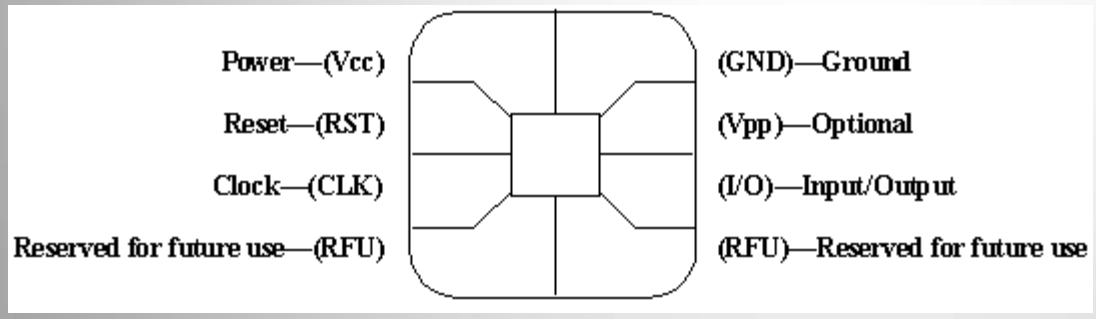
ارتباط بین دستگاه کارت خوان و کارت یک ارتباط Half duplex میباشد . یعنی در تبادل اطلاعات نوبت باید رعایت گردد.(ایده Full duplex شدن این ارتباط میتواند به عنوان یک طرح برای آینده بحساب آید.)



تبادل اطلاعات در کارتهای هوشمند:

برای برقراری ارتباط موجود حداقل ۵ پایه روی کارت ضروری است:

- ✓ Vcc /Gnd: تغذیه چیپ
- ✓ I/O: خط ارتباطی اطلاعات
- ✓ CLK: سیگنال کلاک چیپ
- ✓ RST : ریست کردن کارت



تبادل اطلاعات در کارتهای هوشمند:

هنگام ورود یک کارت به کارت خوان ابتدا یک ارتباط فیزیکی با کارت خوان توسط کنتاکت های موجود روی کارت برقرار میشود. سپس ۵ مرحله برای تبادل اطلاعات انجام میشود:

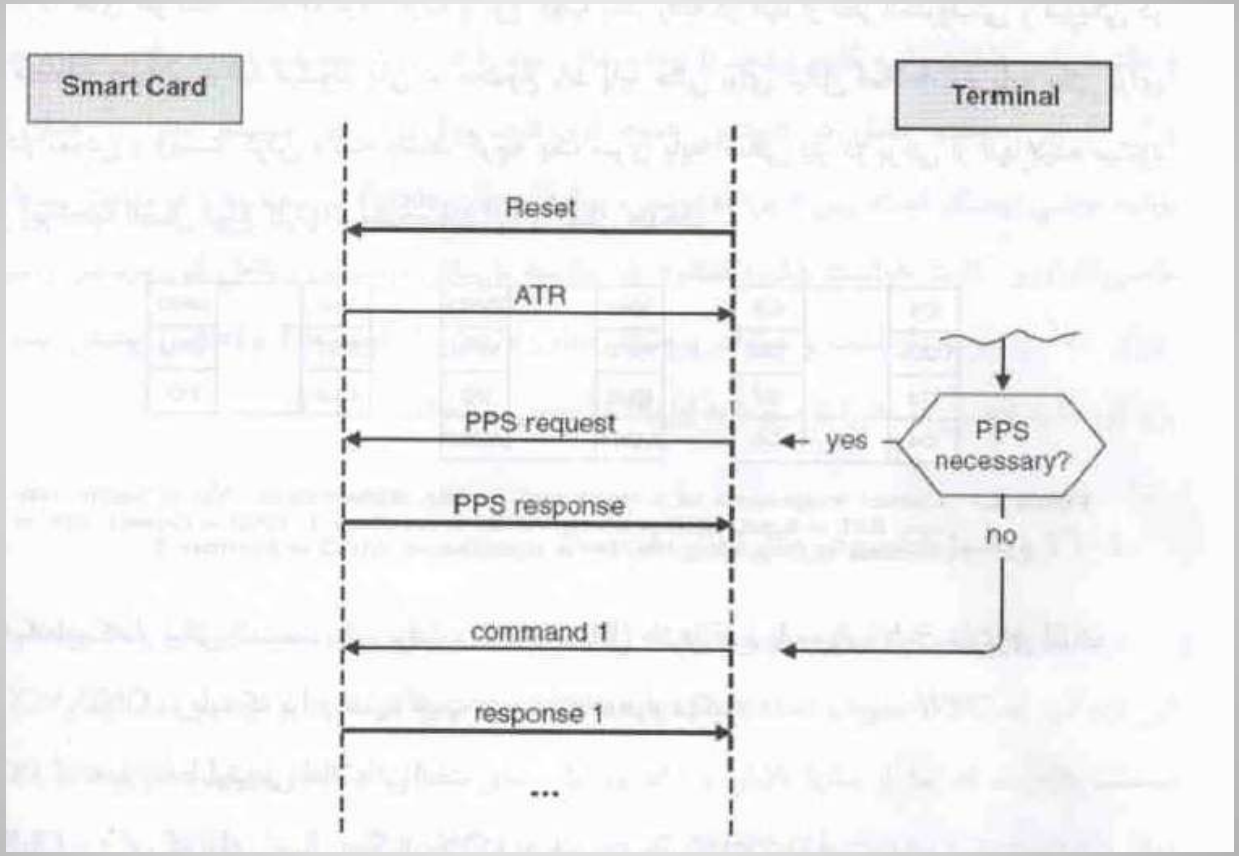
تبادل اطلاعات در کارتهای هوشمند:

- کنتاکت های فیزیکی با دستگاه کارت خوان ارتباط برقرا ر میکنند.
- سپس کارت ریست شده و سیگنال ATR(Answer To Reset) به دستگاه کارت خوان ارسال میشود.
- کارت خوان پس از دریافت ATR اولین دستور را ارسال میکند.
- کارت این دستور را گرفته و پس از تجزیه وتحلیل، جواب متناسب با آن را برمیگرداند.
- تبادل اطلاعات و داد وستد ادامه می یابد تا کارت غیر فعال شود.

در خلال ارسال ATR و دستور اول سیگنال های PPS جهت شناسایی پروتکل ارتباطی هم از سمت کارت و هم از سمت کارت خوان ارسال میشود.

Protocol Parameter Selection

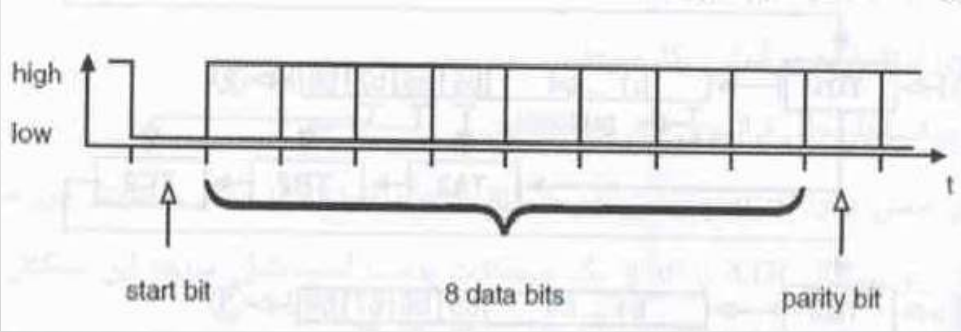
تبادل اطلاعات در کارتهای هوشمند :



تبادل اطلاعات در کارتهای هوشمند

این تبادل اطلاعات کاملا سریال ، دیجیتالی و آسنکرون است.

برای همزمانی یک استارت بیت در ابتدای بایت و برای کنترل صحت ارسال یک بیت توازن در انتهای بایت ارسال می شود.



سیگنال ATR:

ATR بسته به پروتکل ارتباطی دارای اطلاعات متفاوتی است و حداکثر ۳۲ بایت دارد.
هر کارت، ATR مربوط به خود رادارد که هرکدام از بایت های آن معرف کمیتی است. مثلا نوع پروتکل ارتباطی، شماره سریال کارت، شماره سریال چیپ و... برخی پارامترهای ATR در زیر لیست شده اند:

Ts: کاراکتر آغازین

T0: کاراکتر فرمت

TA1,TB1,TC1,..: کاراکترهای واسط

T1,T2,T3,... Tk : کاراکترهای هیستوریکال

Tck: کاراکتر بررسی

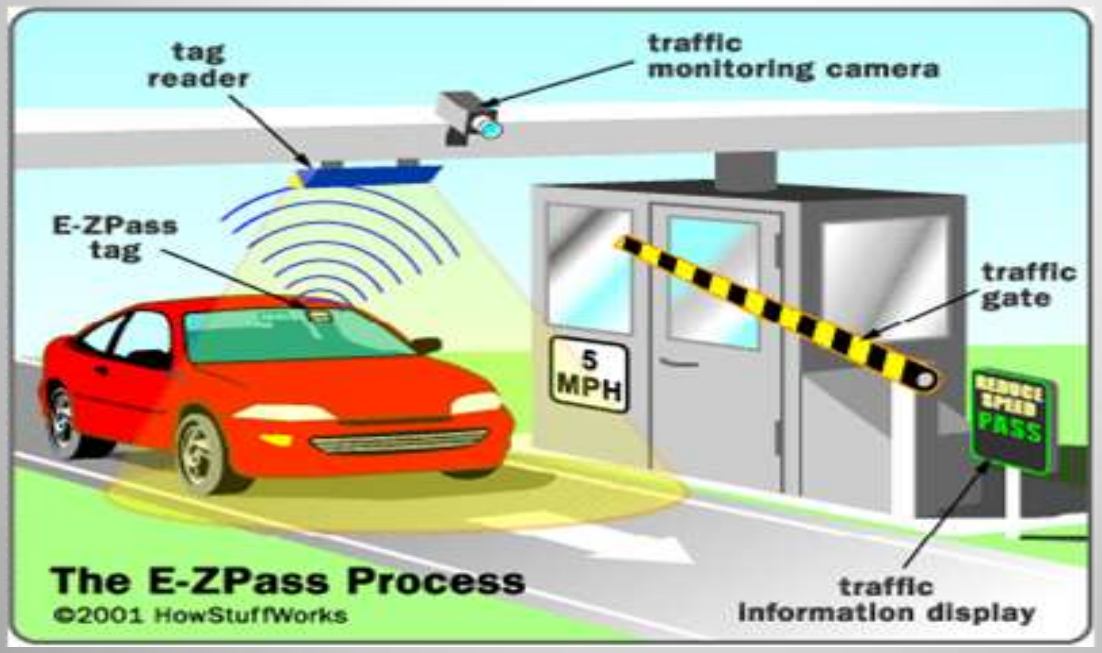
و غیره

که هرکدام از پارامترهای فوق کاربرد وتعریف خاص خود را دارا هستند. مثلا Ts:

کاراکتر Ts:

کاراکتر TSاولین کاراکتر در ATR است که نشان دهنده نوع ارتباط و عدد مقسم (Divider) برای تعیین نرخ ارسال اطلاعات است که در استاندارد ISO 7816 قرار دارد.

در عمل هر چه تعداد بایت های ATR کمتر باشد سرعت تبادل بالاتر میرود و در برخی از کاربردها سرعت بسیار مهم می باشد. نظیر جایگاههای عوارضی در اتوبان ها که رانندگان هر چه سریعتر از آن باید عبور کنند



پروتکل های ارسال اطلاعات

سیگنال دومی که به سوی ترمینال ارسال میشود PPS نام داشت. که برای تعیین نوع پروتکل ارتباطی بکار برده میشود.

پروتکلها طبق ISO- 7816 با حرف T آغاز شده و مهمترین آنها عبارتند از:

T0,T1,T2...,T14

پروتکل های ارسال اطلاعات

T0 : تعریف شده در ISO 7816-3 بصورت Byte Oriented و Half duplex و آسنکرون

T1: تعریف شده در ISO 7816-3 بصورت Block Oriented و Half duplex و آسنکرون

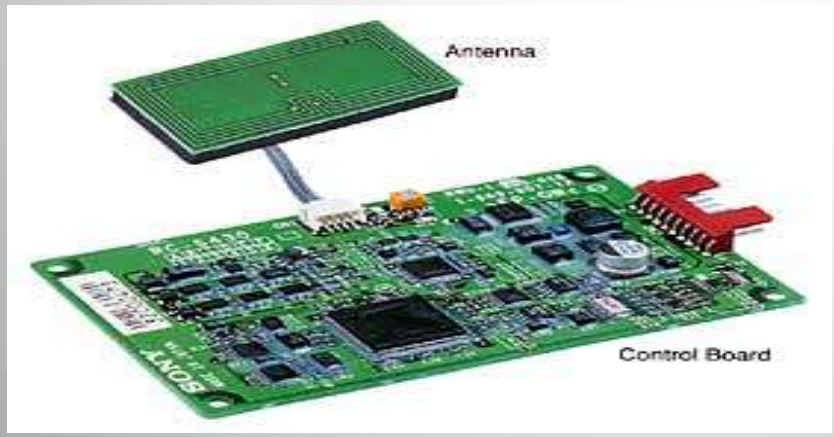
T2: تعریف شده در ISO 10536-4 بصورت Block Oriented و Full duplex و آسنکرون

T14: برای برخی کاربردهای خاص که توسط ایزو استاندارد نشده است.

امروزه T0 و T1 در سطح جهانی کاربرد دارند.

سخت افزارهای ارتباطی با کارتهای هوشمند

قطعات و دستگاههای متعددی به همراه درایورها و نرم افزار هایشان برای ارتباط با انواع کارت هوشمند وجود دارد که برخی از آنها بصورت عمومی و برخی دیگر به یک منظور خاص و برای ارتباط با یک کارت خاص طراحی شده اند که به بررسی چند مورد میپردازیم.



گذرگاه IICBUS:

Inter Integrated Circuit Bus

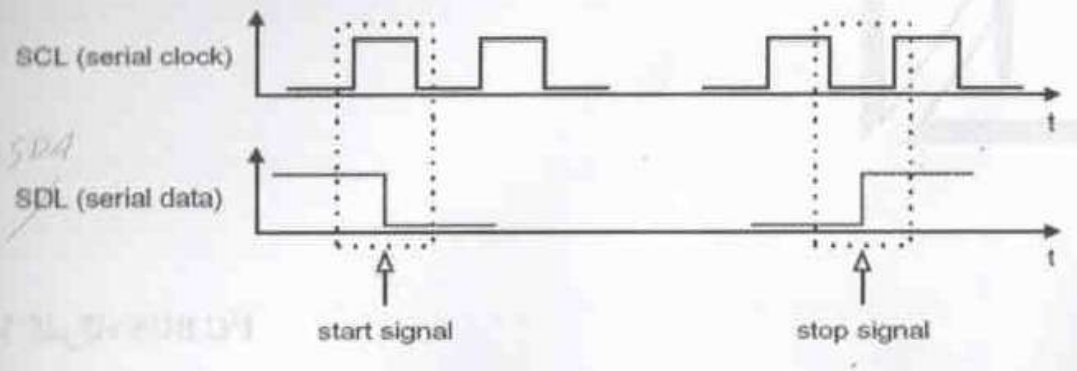
پروتکل ساده ارتباطی است که در سال ۱۹۹۰ از طریق شرکت فیلیپس ارائه شد. اساس ارتباط در آن استفاده از دو سیم یکی برای کلاک سریال (SCL) و دیگری برای دیتای سریال (SDA)میباشد.

زمانیکه کارتهای هوشمند ارائه شدند ارتباط با آنها از طریق این پروتکل کاربرد زیادی یافت.

Serial Clock & Serial Data

گذرگاه IICBUS:

هر ارسال دیتا روی باس با یک سیگنال استارت آغاز و با یک استاپ متوقف می گردد.
زمانیکه پالس ساعت یک باشد، لبه پایین رونده در سیگنال دیتا نشانگر استارت است .
زمانیکه پالس ساعت صفر باشد، لبه بالا رونده در سیگنال دیتا نشانگر استاپ است .
روی باس دیتا دو نوع کمیت باید ارسال شود: آدرس محل حافظه و مقداری که باید ردو بدل شود.
در نوع آدرس : هفت بیت اول آدرس محل حافظه و بیت آخر نوشتنی یا خواندنی بودن دیتای مورد مبادله را مشخص میکند.



پروتکل ارتباطی USB

جدیدا از ارتباط سریال عمومی (Universal Serial Bus) برای تبادل اطلاعات با کارتهای هوشمند استفاده میگردد.

برای این نوع ارتباط میکروکنترلرها نیز باید قابلیت سخت افزاری مناسب را دارا باشد.

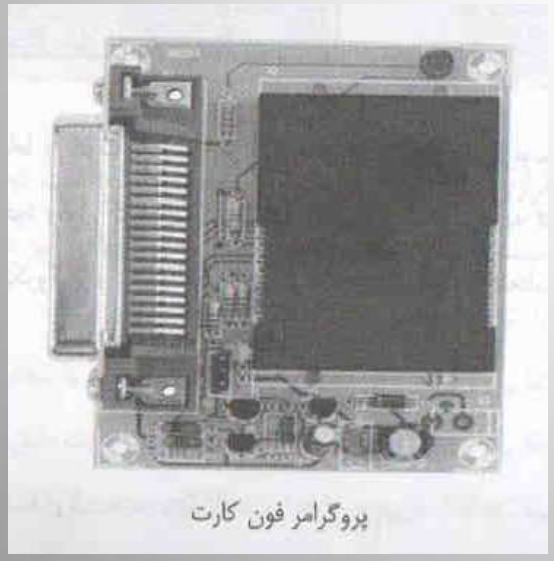
استفاده از این پروتکل باعث افزایش سرعت انتقال تا 480 Mbps میگردد.

ارتباط با کارتهای رمزگذاری تلویزیونی :

Fun Card ها کارتهایی برای رمزگذاری کانالهای تلویزیونی و شبکه های ماهواره ای میباشند. ساختمان داخلی آنها نیز یک میکروکنترلر و یک حافظه EEPROM دارد.

یک پروگرامر ساده ولی مخصوص برای پروگرام کردن آن وجود دارد.

نرم افزار لازم IC Prog میباشد. درایور این سخت افزار به سادگی روی ویندوز XP نصب شده و با IC Prog قابل برنامه ریزی میباشد.

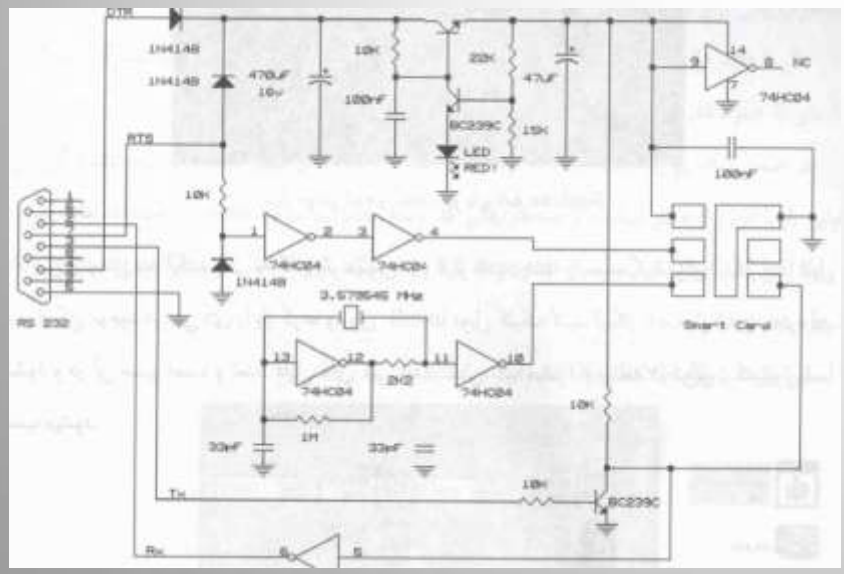


پروگرامر فون کارت

ارتباط با سیم کارتها:

برای ارتباط با محتوای داخلی حافظه سیم کارت نیاز به یک پروگرامر ساده است که بصورت سریال و با استفاده از کابل RS232 به کامپیوتر وصل میشود.

دو نرم افزار Sim-Scan و CARDINAL برای خواندن و نوشتن اطلاعات سیم کارت مورد استفاده هستند.



امنیت در کارتهای هوشمند

امنیت در کارتهای هوشمند

یکی از ملزومات اساسی استفاده از کارتهای هوشمند فراهم آوردن محیطی امن برای داده ها وبرنامه هاست.

علاوه بر بررسی امنیت ، افزایش آن و سایر قابلیتهای اطمینان با ارائه مدلها و روشهای ابتکاری از مقوله های مهم در زمینه کارهای پژوهشی ، شرکت در سمینارها و چاپ مقالات در ژورنالهای معتبر میباشد.

در همین راستا اولین سوالی که مطرح میشود اینست که اساسا " آیا کارت هوشمند امن است ؟ "

امنیت در کارتهای هوشمند:

برای بررسی سطح امنیت کارتهای هوشمند استانداردهای بین المللی نظیر **TCSEC** (آمریکا) و **CCITSE** (برای اروپا) که استاندارد **ISO 15408** را ارائه داده است وجود دارد.

ISO 15408 را با نام معیار **CC** (**Common Criteria**) به معنای معیار مشترک نیز می شناسند.

CC معیاری مشترک برای ارزیابی محصولات **IT** میباشد که شامل استانداردهای بین المللی مرتبط با امنیت کامپیوتر میباشد.

معیار مشترک :

ISO 15408 یا CC بر این مبنا استوار است که کاربران خود احتیاجات امنیتی مورد نظرشان را تعیین کنند و در این صورت تولیدکنندگان ویژگیهای امنیتی محصولات خود را منطبق با درخواست کاربران خواهند ساخت.

به عبارت دیگر:

CC بررسی خصوصیات ،کاربرد وارزیابی محصولات امنیتی کامپیوتر را بر اساس استاندارد انجام میدهد تا وجود سطح امنیتی عنوان شده تضمین گردد.

Evaluation Assurance Level

EAL ها مقادیر عددی هستند که میزان دقت و عمق ارزیابی امنیتی را نشان میدهند. CC دارای ۷ سطح ارزیابی میباشد که از سطوح ۱ به ۷ امنیت افزایش می یابد.

جعبه سیاه:

EAL1 : ارزیابی توسط آزمایش های عملکردی

EAL2: : ارزیابی توسط آزمایش های ساختاری

جعبه خاکستری:

EAL3 : ارزیابی توسط آزمایش های متدلوژی

EAL4 : ارزیابی طراحی آزمایش و بازبینی با روشهای متدلوژی

EAL5: ارزیابی نیمه رسمی طراحی و آزمایش

EAL6 : ارزیابی نیمه رسمی بررسی ها ، طراحی و آزمایش

جعبه سفید:

EAL7 : ارزیابی رسمی بررسی ها ،طراحی و آزمایش

Smart Card Protection Profile

SCPP نیازهای امنیتی IT را برای کارت هوشمند بر مبنای ISO 15408 تشریح میکند و شامل سه بخش ارزیابی معیارهای امنیتی و دو بخش عمومی است که سطح تضمین آن EAL4 میباشد.

ارزیابی معیارهای امنیتی:

۱. مقدمه و مدل عمومی
۲. نیازهای عملیاتی امنیت
۳. نیازمندیهای تضمین امنیت

بخش های عمومی ارزیابی محصولات IT از دید متدولوژی:

۱. **متدلوژی مقدماتی ومدل عمومی**
۲. **متدلوژی ارزیابی**

تهدیدات موجود بر روی کارتهای هوشمند

طبق پروفایل SCPP تهدیدات متعددی بر روی کارتهای هوشمند وجود دارد که برای اجتناب از آنها نیز روش هایی وجود دارد. برخی از آنها عبارتند از :

تهدیدات مهندسی معکوس ، میکروپروبینگ ، تحلیل زمانی ، آنالیز توان و... که در ادامه بحث به ایت تهدیدات و راههای مقابله با آن میپردازیم

طبقه بندی تهدیدات موجود بر روی کارتهای هوشمند

بطور کلی حملات به سیستم کارتهای هوشمند را میتوان از سه بعد بررسی کرد:

- ✓بعد اجتماعی
- ✓بعد فیزیکی
- ✓بعد منطقی

حمله به کارتهای هوشمند از بعد اجتماعی:

این حمله به گونه ای بررسی میشود که افرادی که با کارت هوشمند سر وکار دارند موردهدف قرار میگیرند.

این افراد میتوانند طراحان تراشه های نیمه هادی ، طراحان نرم افزاری ، مالکان کارت و... باشند.

این گونه حملات را تا اندازه ای با قفل بودن کارت میتوان خنثی نمود. در حقیقت بعد اجتماعی روی انگیزه مهاجمین بحث میکند نه روی جنبه های فنی.

حمله به کارتهای هوشمند از بعد فیزیکی:

در این گونه حمله نیاز به دسترسی فیزیکی به اجزاء کارت مخصوصا میکروکنترلرهای روی آن با استفاده از ترفندهای گوناگون دارد و مستلزم وسایل تکنیکی است.

وسایل میتواند شامل میکروسکوپ ، میکرو پروب ،برنده لیزری ، وسایل دستکاری میکرو ، اشعه های یونی متمرکز ، وسایل تیزاب کاری و قلم زنی شیمیایی ، کامپیوترهای پرسرعت جهت تجزیه وتحلیل وثبت کردن ارزیابی جریانات الکتریکی و... میباشد.

حمله به کارتهای هوشمند از بعد فیزیکی:

در این گونه حمله یکی از مهمترین اقدامات جداسازی ماژول از کارت است.

بدین منظور از یک چاقوی نوک تیز میتوان استفاده نمود. سپس باید لایه رزین اپوکسی روی تراشه (لایه ای محافظ) از آن جدا شود. این کار توسط بخار اسیدنیتریک به همراه یک لامپ مادون قرمز به عنوان منبع حرارتی و استون جهت شستشوی تراشه انجام میشود. پس از این کار نیمه هادی تقریبا آزاد و دارای کارکرد میباشد.

حمله به کارتهای هوشمند از بعد فیزیکی:

این حمله معمولا ۲ نوع دارد:

- ✓ **استاتیکی: در حین حمله هیچ نیرو و انرژی به میکرو وارد نمی شود و معمولا خود میکرو هم در حال کار نیست.**
- ✓ **دینامیکی: اعمال نفوذ در حین کار میکرو انجام شده و کاملا وابسته به زمان کار میکرو است.**

حمله به کارتهای هوشمند از بعد منطقی:

بیشتر حملات شناخته شده موفقیت آمیز در سطح منطقی بوده است . منشاء این حملا تفکرات ذهنی و محاسبات است. این مقوله شامل کشف رمز ، بهره برداری ، سوءاستفاده از اشتباهات ، شکافهای اطلاعاتی لورفته موجود در سیستم عامل کارت هوشمند ، بکارگیری اسبهای تروجان و کدهای قابل اجرا در عملیات این گونه کارتهاست.

این حمله معمولا ۲ نوع دارد:

- ✓ **غیرفعال: مهاجم به تجزیه وتحلیل کدهای رمزی بدون اعمال تغییر در آنها میپردازد.**
- ✓ **فعال: مهاجم جریان انتقال اطلاعات را دستکاری میکند.**

حمله به کارتهای هوشمند از دیدگاه دیگری

مطابق ISO 10203-1 میتوان انواع حمله را از نظر چرخه حالات کارت هوشمند تقسیم بندی نمود:

- حمله در مرحله توسعه وترقی(Development)
- حمله در مرحله ارائه وساخت(Production)
- حمله در مرحله کاربرد کارت(Card usage)

چرخه حالات کارتهای هوشمند:

- مرحله توسعه وترقی:

به مرحله طرح سیستم ، مراحل ارتقای تراشه ، توسعه سیستم عامل ، ایجاد برنامه اطلاق میشود .

- مرحله ارائه وساخت:

این مرحله به تمامی جریانات دخیل در ساخت وتولید سخت افزار اشاره دارد. یعنی تمام مراحل از ساخت یک قطعه ریز ویفر (قطعه نازک سیلیکونی که برروی مدارات مجتمع برای ایجادیک تراشه قرار دارند می باشد)

- مرحله کاربرد کارت:

این مرحله ، وارد میدان عمل شدن کارتهای هوشمند است به این معنی که کارت در دسترس استفاده کننده قرار می گیرد.

تاریخچه حملات بر کارتهای هوشمند :

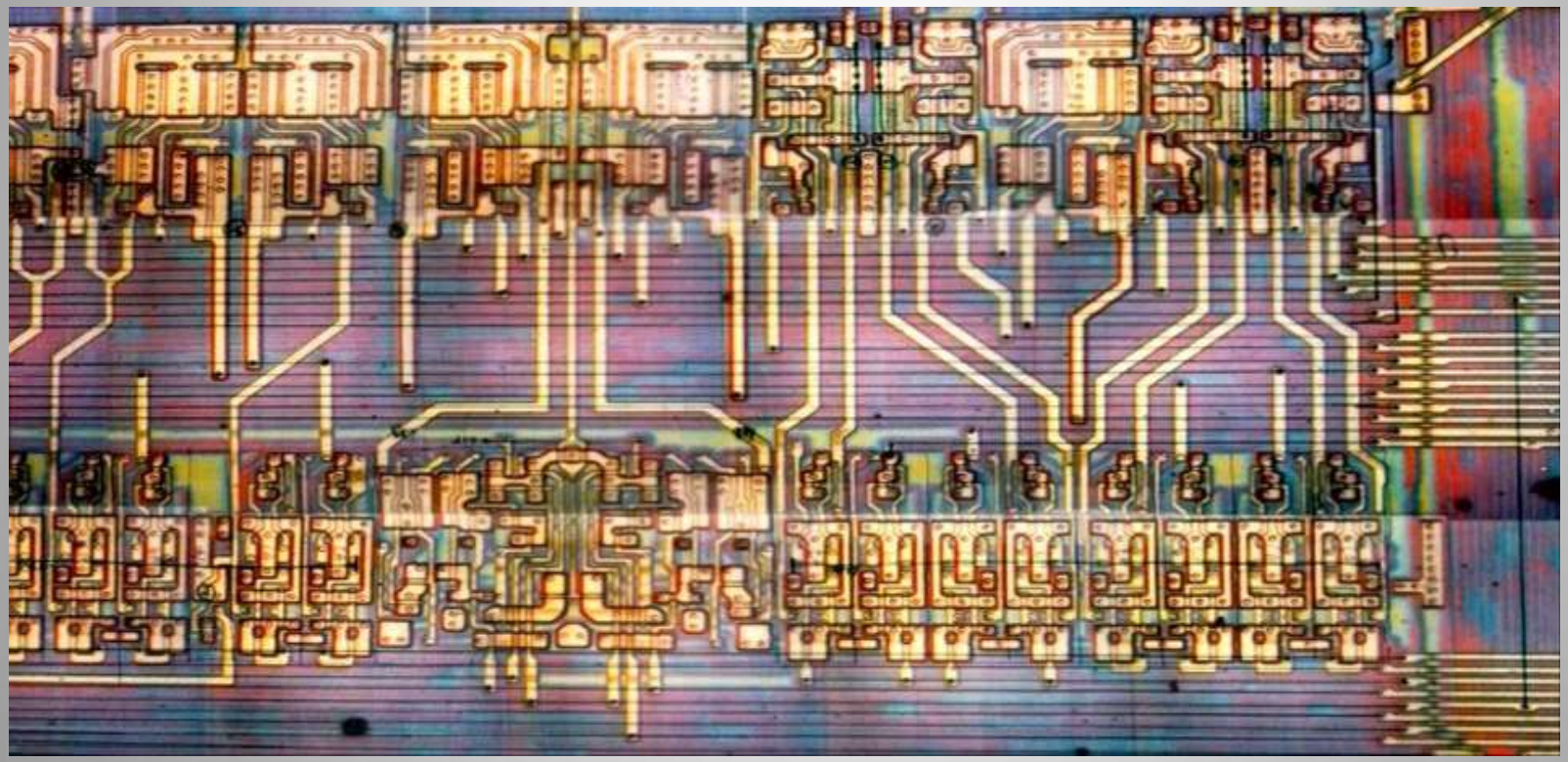
زمان	هدف تهاجم	شرحی کوتاه	مقابله
قبل از ۱۹۹۰	بهره برداری از تبادل اطلاعات	استفاده از سیستمهای متصل شده به ماژول امنیتی که امکان بهره برداری از تبادل اطلاعات بین ترمینال و کارت هوشمند را فراهم میکند	ایجاد پیام متنی
۱۹۹۰	حل کردن لایه اثر ناپذیری	حل کردن لایه اثر ناپذیری که بر روی میکروکنتلر قرار دارد که پیش نیاز دسترسی فیزیکی به اجزای قاب میباشد.	ایجاد جستجوگرهای لایه اثرناپذیری در میکروکنترلر
۱۹۹۱	پاک کردن EEPROM واستفاده از چراغ UV	بوسیله پاک کردن EEPROMو استفاده از چراغ UV ، میتوان به کارهایی مثل برگرداندن شماره گرها به همان مقدار قبای خود دست زد.	ارائه حسگرهای نوری در میکرو
۱۹۹۳	متوقف کردن ساعت	با متوقف کردن ساعت و تجزیه وتحلیل RAM توسط تست کننده های اشعه الکترونی میتوان نتایج محتویات RAM را بدست آورد.	ابداع چک کننده های فرکانس پایین در میکروکنترلر
۱۹۹۳	دستکاری میکروکنترلر با برش لیزری	اجزا موجود در قاب میکروکنترلر قابل دستکاری با برش لیزری میباشند.	ابداع لایه پوشش ایمنی در میکروکنترلر

تاریخچه حملات بر کارتهای هوشمند :

زمان	هدف تهاجم	شرحی کوتاه	مقابله
۱۹۹۵	بهره برداری کردن از گذرگاهها با استفاده از میکروپروب	امکان استفاده از گذرگاهها توسط میکروپروب وجود دارد.	تجمع گذرگاهها در پشت قاب میکروکنترلر
۱۹۹۶	دستکاری میکرو ا استفاده از FIB (Focused Ion Beam) اشعه یونی متمرکز	با استفغاده از FIB میتوان قطعات روی قاب میکروکنترلر را دستکاری کرد.	ایجاد لایه محافظتی بر روی میکروکنترلر
۱۹۹۸	SPA-DPA	اطلاعات درحال پردازش را میتوان از میزان مصرف پردازشگر معین نمود.	ابداع توقف ها و مکث های جابجا و اتفاقی در عملیات
۱۹۹۸	توزیع پردازشگر	با توزیع پردازشگر (مثلا با استفاده از پرتوهای شدید نوری) امکان دخالت در عملیات آن در مراحل حساس انتقال در حین پردازش وجود دارد.	استفاده از جستجوگرهای سودمند درمیکروکنترلر همراه با اقدامات پیشگیرانه نرم افزاری

تشریح انواع حملات موجود بر روی سیستم کارت های هوشمند و راههای مقابله با آنها

۱- حملات مهندسی معکوس
Reverse Engineering



حملات مهندسی معکوس :

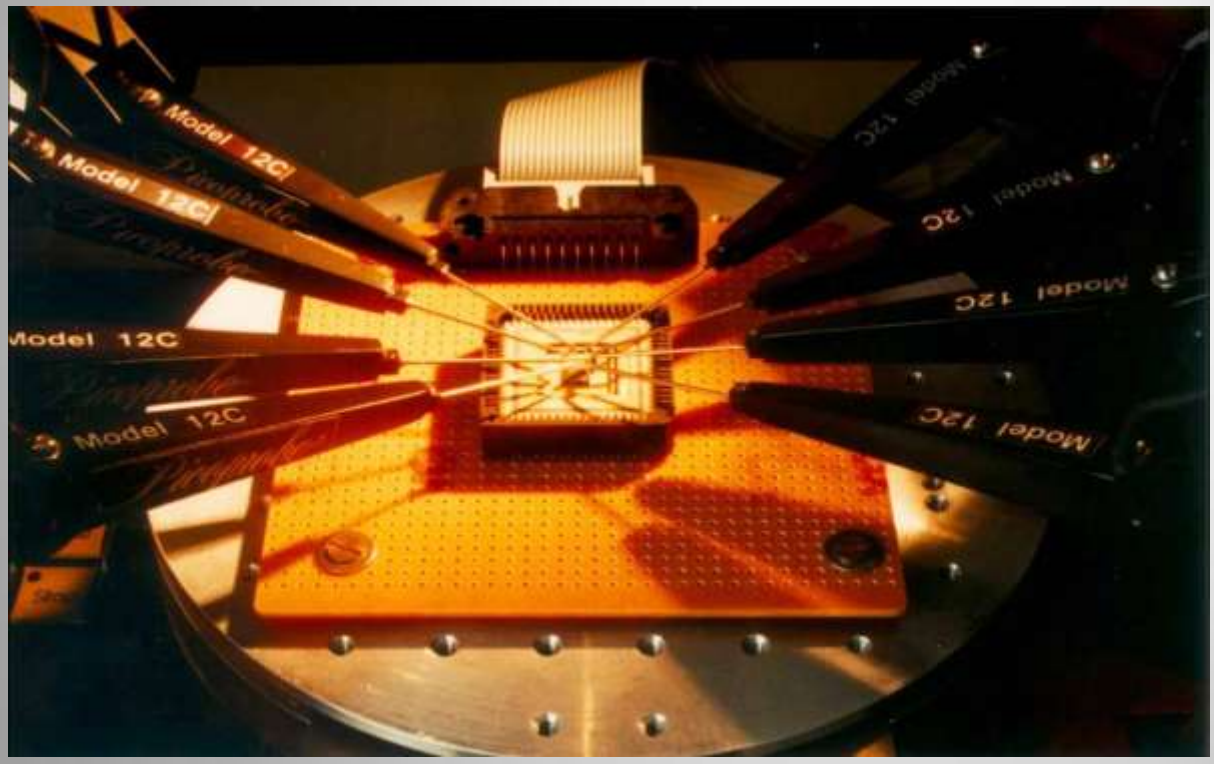
این حمله یک حمله فیزیکی و استاتیکی میباشد. همانطوریکه ذکر شد سطح چیپ با برداشتن صفحه طلایی و بدنه پلاستیکی کارت قابل عریان شدن است و با بکاربردن اسیدنیتریک رزین اپوکسی بکاررفته در آن حل میشود.

- با عریان شدن ریزپردازنده ا می توان زیر میکروسکوپ دید و بلوکها و توابعش را شناخت.
- با مهندسی معکوس طراحی داخلی هدف قرار می گیرد تا چگونگی عملکرد بلوکها کشف و درک شود.این شیوه به ارتقای دانش طراحی چیپ کارت هوشمند و کپی برداری از آن کمک می کند.
- حمله کننده ممکن است به کپی کردن چیپ موفق شود
- نقاط ضعف احتمالی در چیپ را پیدا کند.
- مهندسی معکوس توسط شرکت های رقیب در تولید کارت هوشمند برای ایجاد مزیت رقابتی با یادگیری از رقبا و محصولاتشان به کار می رود.

مقابله با حملات مهندسی معکوس :

- کارتهای هوشمند مدرن با مهندسی معکوس مقابله می کنند.
- از منطق چسباندن استفاده می کنند .
- گزینه های مهم به طور تصادفی روی سطح چیپ پخش می شوند.
- این تکنیک اندازه بلوک را افزایش می دهد و در نتیجه درطراحی بلوکهای بزرگ چون ROM و EEPROM به کار نمی رود.
- راه دیگر مقابله با حمله های مهندسی معکوس پوشش دادن چیپ با یک لایه فلزی دیگر است. که حین حذف آن لایه مدار از بین می رود و خراب می شود.

۲- حملات میکروپروبینگ:
Micro probing



حملات میکروپروبینگ:

همانند حمله مهندسی معکوس در این حمله نیز میتوان پوشش ریز پردازنده را برداشت و با استفاده از دستگاه پروب اطلاعات روی باس های پردازنده را خواند.

حفاظت:

استفاده از لایه های شیشه پوشانی(Passivation) ، استفاده از شبکه های فلزی همانند یک توری بر روی ریز پردازنده ، قرار دادن باس هادر لایه های پایینی نیمه هادی ، استفاده از ایده خود تخریبی (ایده ایست که برای تمامی روشهای تهاجم استفاده میشود ولی توجیه اقتصادی ندارد) و...

۳- حمله بازخوانی حافظه فرار:

حمله بازخوانی حافظه فرار :

همانطوریکه میدانیم محتوای حافظه RAM با قطع برق پاک میشود. با این وجود برای حافظه وقتی به اندازه ۶۰ - درجه سانتیگراد سرد شوند این اتفاق نمی افتد و محتوای RAM مدتی طولانی بدون تغییر باقی میمانند.

بنابراین:

با این شیوه مهاجم میتواند به اطلاعاتی که در حافظه RAM وجود دارد دست یابد. به همین دلیل در کارتهای جدید اطلاعات محرمانه از قبیل کلیدهای مخفی بیش از حد لزوم در RAM نگهداری نمیشوند.

۴- تهاجم با حدس زدن پین:

در این حمله ، مهاجم با خواندن محتوای EEPROM کارت به اطلاعات مخفی نظیر شمارشناسایی یا PIN دسترسی خواهد داشت.

به عنوان دفاع اساس بر این گذاشته میشود که در صورتی که احتمال بازخوانی EEPROM وجود داشته باشد ، باید دست کم مهاجم به اطلاعاتی نظیر PIN بازداشت.

میتوان PIN را به گونه ای رمز نمود و نتیجه را در EEPROM به همراه یک کلید مخفی برای بازکردن آن قرار داد.

البته وقتی مهاجم بتواند کل حافظههوشمند را بخواند قابل به خواندن کلید رمز PIN آن نیز میباشد.

در عمل این روش زمانی موثر است که محتوای حافظه گسترده باشد نه در حد چند بایت.

۵- حمله تحلیل زمانی یا حمله Timing:

زمان اجرای یک برنامه پارامتری است که برنامه نویسان علاقه زیادی به کاهش هر چه بیشتر آن دارند.

در کمال شگفتی ، زمان اجرای یک الگوریتم رمزنگاری میتواند یک کانال اطلاعاتی مفید برای یک هکر باشد.

معمولا زمان پردازش اطلاعات توسط سیستم های رمز نگاری بازای ورودیهای مختلف اندکی متفاوت است.

در حمله تحلیل زمانی ،

اندازه گیری زمان اجرای الگوریتم بازای ورودیهای مختلف به یک مدل آماری خورانده میشود که میتوتند با محاسبه همبستگی بین اندازه گیریهای مختلف یا واریانس اندازه گیری ها بعضی از بیت های کلید را حدس زد.

تعداد نمونه های لازم برای موفقیت حمله بسته به نسبت سیگنال به نویز سیستم دارد. هرچه این نسبت کمتر باشد تعداد نمونه بیشتری نیاز است.

۶ – حمله آنالیز توان:

حمله آنالیز توان:

علاوه بر زمان اجرا توان مصرفی تراشه ممکن است مشخص کند چه عملیاتی در حال اجراست و اطلاعاتی را فاش کند(مخصوصا اطلاعات محرمانه نظیر اطلاعات کلید ها). زیرا همبستگس بین دستور اجرا شده و توان مصرفی وجود دارد.

همانطوریکه در شکل بعدی پیداست توان مصرفی سه دستور نسبت به هم متفاوت است.

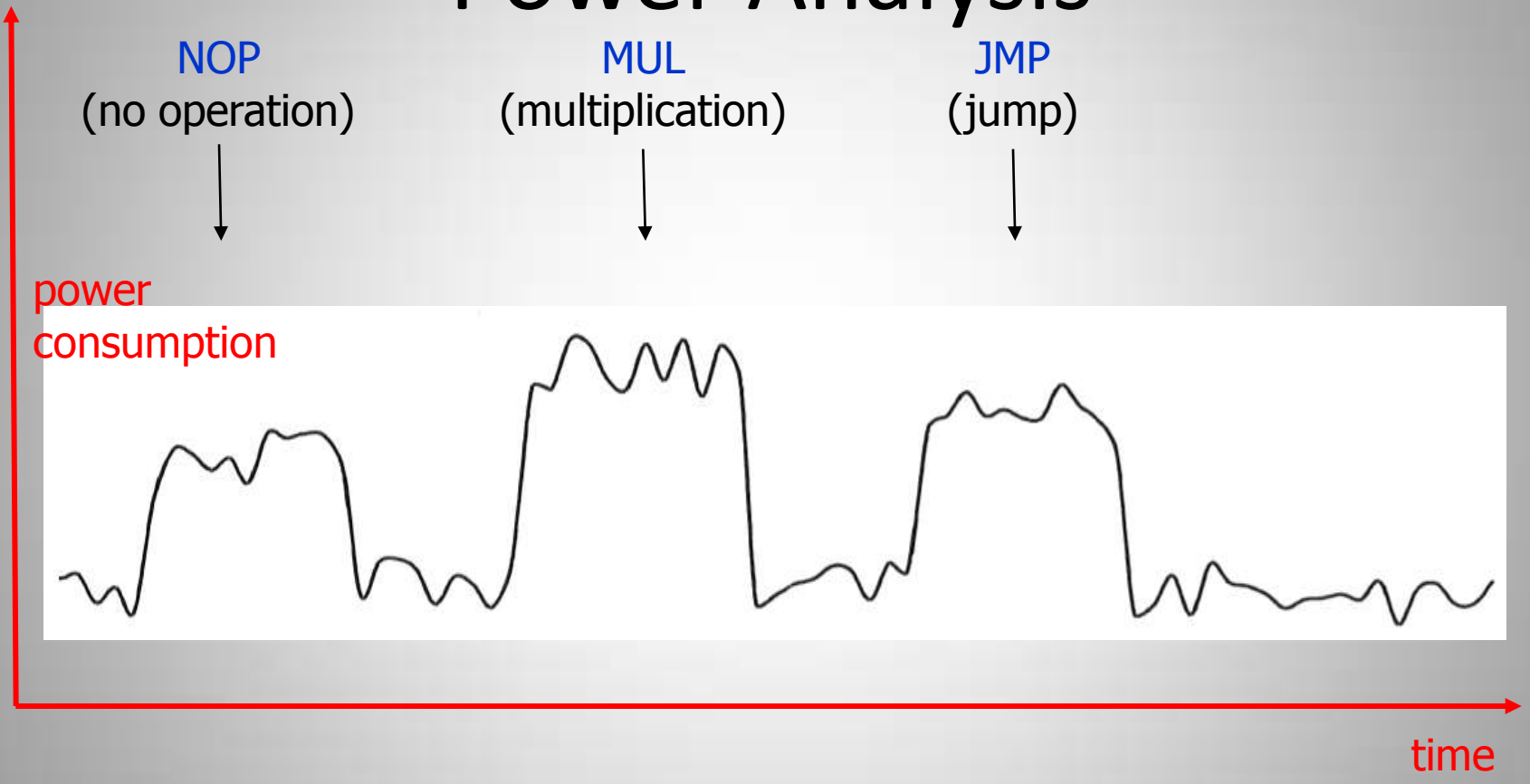
حمله آنالیز توان دو نوع است: حمله آنالیز توان ساده (SPA) و حمله آنالیز تفاضلی توان(DPA)

SPA: Simple Power Attack

DPA: Differential Power Analysis Attack

که در ادامه هر یک را تشریح خواهیم کرد.

Power Analysis

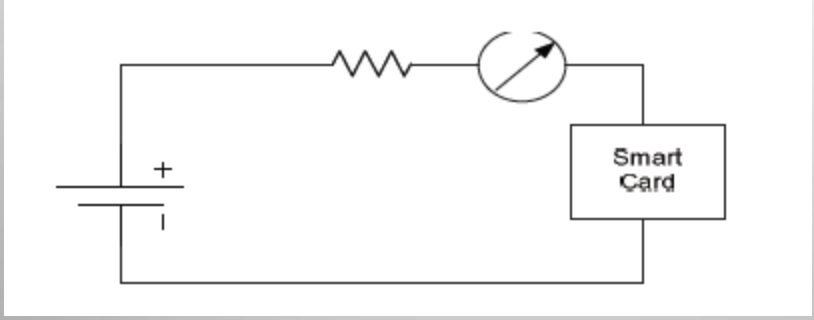


Source: Rankl and Effing, "Handbuch der Chipkarten", 2002

حمله آنالیز توان :

همراه با نوسان کلاک انرژی مصرفی کارت هوشمند در دو ترمینال انتهایی آن به سادگی قابل اندازه گیری است. یک مقاومت کوچک بطور سری با کارت قرار داده میشود و جریان گذرنده از آن اندازه گیری میشود. با نمونه گیری و ارسال نمونه ها به یک PC آنالیز نمونه ها و حمله به سیستم امکان پذیر میباشد.

برای وضوح بیشتر: تصور کنید یک رشته برنامه خاص با یک سری اطلاعات ویژه نمودار یکسان جریانی در زمان را تولید میکند. اگر همان برنامه با استفاده از اطلاعات دیگر اجرا شود نمودار جریان در زمان متفاوت خواهد بود.از این تغییر نمودار میتوان جهت تشخیص اینکه چه نوع داده ای در حال اجرا توسط برنامه میباشد ، استفاده کرد.



حمله آنالیز توان ساده (SPA):

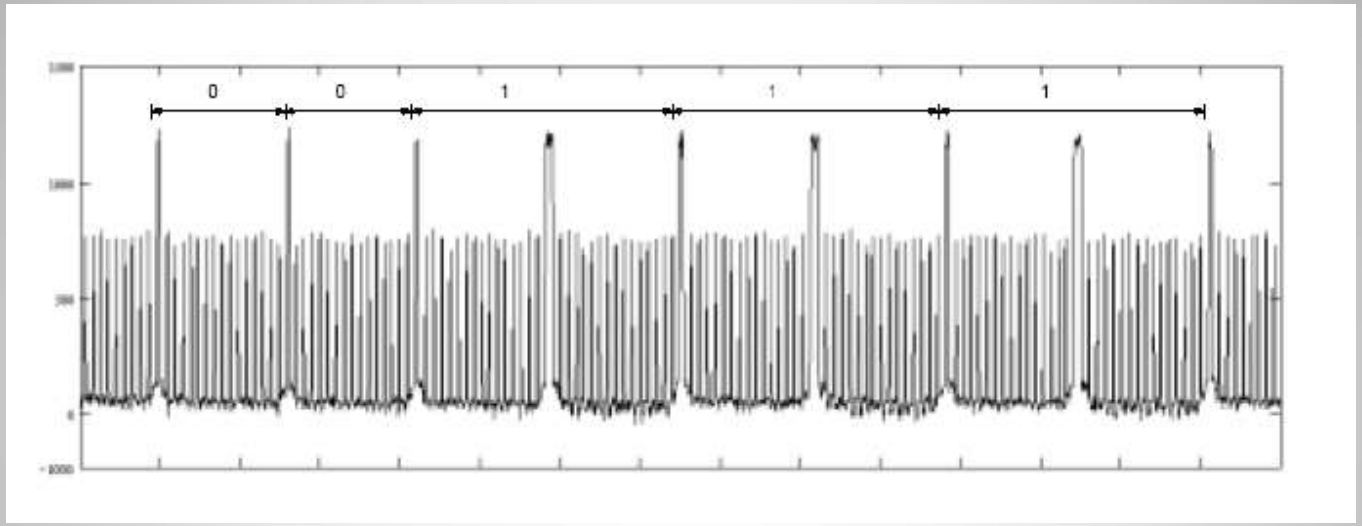
این حمله مستقیما از اندازه گیری های توان مصرفی وسیله حین انجام عملیات استفاده میکند.

الگوی توان یا انرژی مصرفی سخت افزار میتواند اطلاعات مهمی در مورد دستورالعملها ، توالی اجرای آنها و حتی عملوند در اختیار مهاجم قرار دهد.

شکل زیر مصرف توان یک کارت هوشمند که الگوریتم RSA را اجرا میکند هنگام عملیات محاسبه امضای دیجیتال نشان میدهد. ۹ پالس ضربه ای که در شکل نمایش داده شده خبر از آغاز عملیات مربع و ضرب میدهد.

ضرب در مقایسه با مربع نیاز بیشتری به بار کردن رجیسترها دارد و لذا پهنای پالس ضرب بیش از پهنای پالس مربع است. چنانچه در شکل نشان داده شده کلید در این حالت برابر با 00111 بوده که از تجزیه وتحلیل الگوی توان بدست آمده است.

حمله آنالیز توان ساده (SPA):



حمله آنالیز تفاضلی توان (DPA):

یکی از خطرناکترین حملات به کارتهای هوشمند میباشد.و بسیار دقیقتر از تحلیل SPA است.

در تحلیل DPA مقدار مصرف در حین اجرای اطلاعات شناخته شده اندازه گیری میشود وسپس دوباره جریان مصرف در حین اجرای اطلاعات ناشناخته اندازه گیری میشود. این اندازه گیریها چندین بار تکرار میشود. تا با بدست آوردن مقدار میانگین اثرات پارازیت کاهش یابد. وقتی اندازه گیریها کامل شد اختلافات محاسبه شده و نتایج مربوط به اطلاعات ناشناخته از آنها اقتباس میگردد.

راههای سخت افزاری مقابله با حمله آنالیز توان:

- ✓ **جاسازی یک رگولاتور ولتاژ پر سرعت در تراشه ای که از یک سنسور مقاومت برای نظارت بر جریان میکرو استفاده میکند.**
- ✓ **استفاده از تولیدکننده های پارازیت ساختگی جریان روی تراشه**
- ✓ **طراحی پردازشگری اصلاح شده جهت پشتیبانی جریانی ثابت و بدون تغییر**

راههای سخت افزاری مقابله با حمله آنالیز توان:

هر سه روش قبل تا حد زیادی مصرف انرژی در میکرو را بالا میبرد که در برخی از مواقع کاربردی ارتباطات راه دور نامطلوب بنظر میرسد.

یک اقدام جایگزین و موثر فعال نمودن قسمت هایی از میکرو که به کارکرد آنها در زمان اجرای تحلیل توان احتیاجی نیست ، میباشد. برای این منظور می توان از مبدل کد CRC و کمک پردازشگر با استفاده از داده های تصادفی جهت ایجاد پارازیت ساختگی در جریان مصرف استفاده کرد.

همچنین در میکروهایی که مولد ساعت روی خود دارند ، با استفاده از تغییر دادن مدام یا تصادفی فرکانس ساعت در مقاطع معینی بکار برد.

راههای نرم افزاری مقابله با حمله آنالیز توان:

- ✓ ساده ترین روش استفاده از آن دسته دستورات ماشین است که میزان مصرف مشابهی دارند.
- ✓ داشتن چندین پردازه تصادفی مختلف برای اجرای محاسبات یکسان بصورت الگوریتم مخفی
- ✓ اجرا کردن تصادفی دستور NO-OP در نقاط مختلف برنامه یکی دیگر از راههای به هم ریختن الگوی مصرف توان پردازنده میباشد.

۷- حملات تحلیل الکترومغناطیسی:

- از نظر تئوری این امکان وجود دارد که با اندازه گیری اشعه تابشی الکترومغناطیسی ، بتوان درباره پروسه داخلی میکروکنترلر کارت هوشمند به نتایجی دست یافت

حملات تحلیل الکترومغناطیسی:

میدان های مغناطیسی با ابعاد و قدرت کم را میتوان با استفاده از دستگاه فوق رسانای ذرات تداخلی یا SQID

(Super Conducting Quantum Interface Device) اندازه گیری نمود. با این وجود این عمل از نظر تکنیکی خیلی مشکل است و دانش ساختار داخلی دستگاه نیمه رسانایی که برای این روش ضروری است معمولا در دسترس نیست.

به علاوه :

IC ها را میتوان با قرار دادن چندین مسیر بر روی یکدیگر در مقابل این حملات محافظت کرد.

حتی اگر:

۸- حمله القاء خطا:

یک روش قدرتمند رمز شکنی ایجاد مشکل یا القای خطاهای تعمدی در سیستم است با این امید که محاسبات با وجود خطا باعث نشت اطلاعات کلید یا دیگر اطلاعات مهم بشود.

انواع القاهای خطا در کارت های هوشمند:

۱. ولتاژ: طبق استاندارد ایزو ولتاژ تغذیه یک کارت هوشمند ۵ ولت میباشد در حالیکه نوسانات تا حد ۰/۵ ولت نیز قابل قبول است. هر نوع ضربه ولتاژ با ارتفاع بیش از ۱۰% سبب ایجاد خطای مطلوب برای مهاجم میگردد.

۲. کلاک:ایزو برای کلاک مرجع کارت هوشمند مقدار تعیین کرده است. کاهش یا افزایش فرکانس سبب خواهد شد تا در پردازش CPU اختلال ایجادشود. برخی glitch های روی کلاک میتواند سبب تغییر رفتار اجرایی CPU و حتی Bypass شدن بعضی دستورالعملها شود.

۳. دما: بالابردن دما میتواند سبب برهم خوردن نظم کار کارت هوشمند گردد.

۴. تشعشع: تشعشعاتی که بصورت متمرکز و به نقاط صحیح تابانده میشود میتواند سبب ایجاد خطاهای مطلوب برای مهاجمین در کارت هوشمند شود.

یک راه ساده پیشگیرانه :

ساده ترین راه مقابله با این خطاها اینست که عملیات رمزنگاری دوبار انجام شود و چنانچه نتیجه هر دو بار یکی بود آنگاه نتیجه به خروجی ارسال میشود و بالطبع زمان بیشتری نیاز دارد.البته احتمال آنکه نتیجه هردو بار عملیات توام با خطا باشد و یکسان باشد نیز وجود دارد.

دوطرح برای آینده:

۱- نمایش عملکرد داخلی در محیط آزمایشگاهی

۲- ارسال ودریافت دوطرفه همزمان