Departamento de Engenharia Informática
Faculdade de Ciências e Tecnologia
Universidade de Coimbra

Arquitectura de Computadores 2

"DESCRIÇÃO DA ARQUITECTURA INTERNA DE UM SMART CARD"

Crispim Alberto Caldeira Tribuna 501000897
Pedro Miguel Pereira Verissimo 501011276

ÍNDICE

"DESCRIÇÃO DA ARQUITECTURA INTERNA DE UM SMART CARD"

por

Crispim Alberto Caldeira Tribuna / Pedro Miguel Pereira Veríssimo
Departamento de Engenharia Informática
Universidade de Coimbra
ctribuna@student.dei.uc.pt / pmver@student.dei.uc.pt

RESUMO

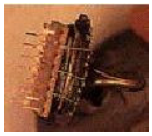
Smart Cards cartões com microprocessador permitem guardar mais informação que os cartões magnéticos, e são mais seguros. Os chips nos cartões podem processar os dados na memória do cartão. A geração corrente de cartões tem um processador de 8 bits , 16 KB de memória ROM e 512 bytes de RAM.
Estes cartões são utilizados para uma variedade de aplicações, especialmente as que incluem criptografia, que envolve a manipulação de muitos dados numéricos.

PALAVRAS CHAVE

Smart Card, criptografia, microprocessador, memória.

1. INTRODUÇÃO

Avanço tecnológico é uma exigência do mundo actual, onde informações e dados são transferidos em questão de segundos. Dentro dessa realidade, os Smart Cards constituem-se uma forma segura e eficaz de armazenar e transferir informações.
Desde há uns anos para cá, que o sistemas baseados em Smart Cards vêm aumentado (sendo estimado vários biliões de utilizadores), nos mais variados tipos de aplicações, no campo da saúde, bancário, entretenimento, comunicações, transportes entre outros. A maioria das aplicações suportadas, beneficiam de características adicionais e segurança que os Smart Cards fornecem.



Uma breve contextualização histórica, conceito Smart Card não é algo recente, em 1947 um jornalista Francês Roland Moreno inventou um revolucionário sistema de pagamento, o Smart Ring – um sistema electrónico da época baseado numa aplicação de armazenamento de valores, sobre um anel. Anos mais tarde, voltou-se à ideia do Smart Ring, e por volta de 1975, o primeiro formato de cartão de crédito com chip e com contactos de um lado foi feito, por uma companhia francesa CII-Honeywell-Bull.

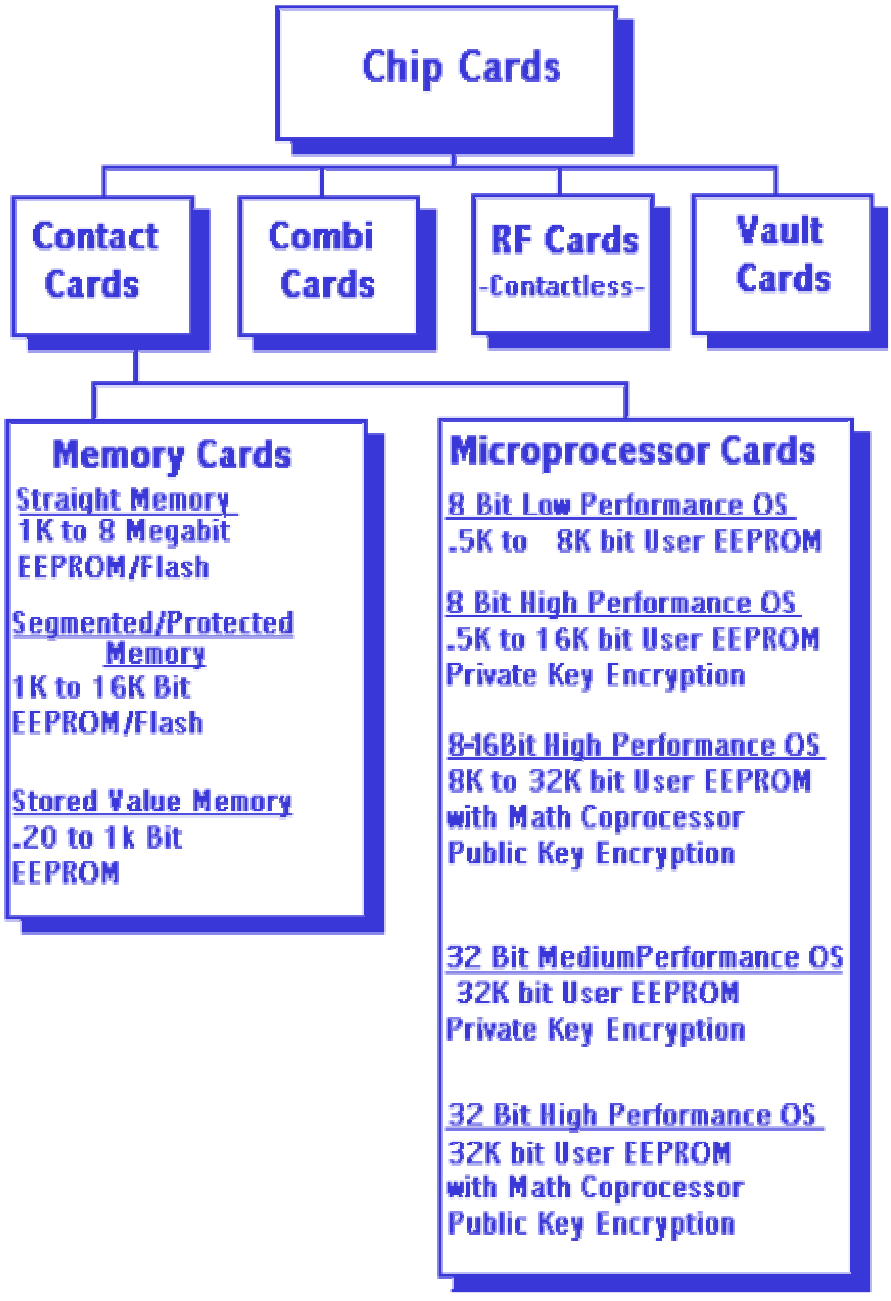
O Smart Card surge normalmente na forma, de um cartão de plástico no qual se encontra um chip de computador, que armazena e onde se efectuam

transacções de dados entre utilizadores. Estes dados são associados com qualquer valor ou informação ou ambos, e são armazenados e processados dentro do chip presente nos cartões, seja na memória ou no microprocessador. Os dados do cartão são transaccionados por um leitor constituinte de um sistema de computação.

Tenciona-se com este documento, uma descrição da arquitectura interna de um Smart Card.

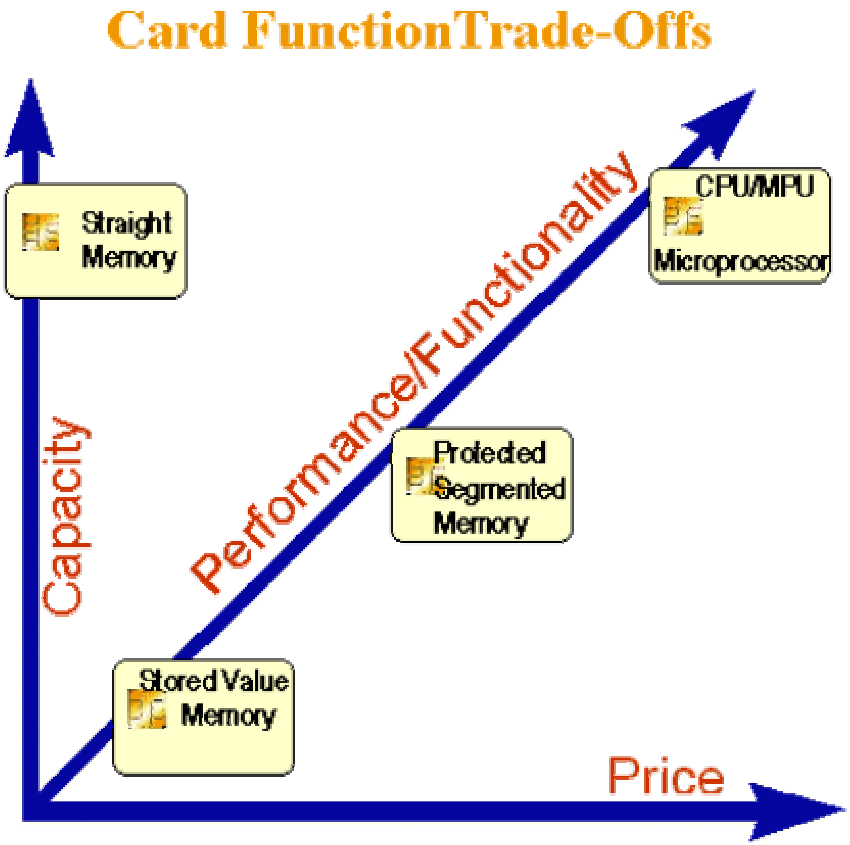
2. TIPOS DE SMART CARDS

Os Smart cards são definidos de acordo com o tipo de chip que é implantado no cartão e as suas capacidades. São muitas as opções, escolher para o desenho de um sistema smart cards.



Neste capítulo serão explicados os diferentes tipos de cartões de contacto (existem quatro tipos de smart cards: Contact Cards, Combi-Cards, RF Cards, VaultCards)
Existem no mercado quatro tipos de cartões de contacto nomeadamente Straight Memory Cards, Protected / Segmented Memory Cards, Stored Value Memory Cards e CPU/MPU Microprocessor Multifunction Cards.

Aumentando o nível de poder de processamento, flexibilidade e memória aumentam também o custo. A escolha do tipo certo de smart card para a nossa aplicação, pela avaliação do custo *versus* funcionalidade e determinando o nível que queremos de segurança. O gráfico que se segue demonstra, de um modo geral a "regra do Polegar".



MEMORY CARDS

Cartões de memória não têm qualquer tipo de poder de processamento sofisticado e não fazem qualquer gestão de ficheiros dinâmica. Todas as memórias comunicam com os leitores, se bem que por protocolos síncronos.

STRAIGHT MEMORY CARDS

Estes cartões apenas armazenam dados e não têm capacidade para o processamento de dados (não tendo qualquer tipo de processador). Estes cartões são de custo baixo por bit para o utilizador de memória. Eles não

conseguem identificar a eles próprios relativamente ao leitor, por isso o sistema têm de saber, que tipo de cartão está inserido no leitor.

PROTECTED / SEGMENTED MEMORY CARDS

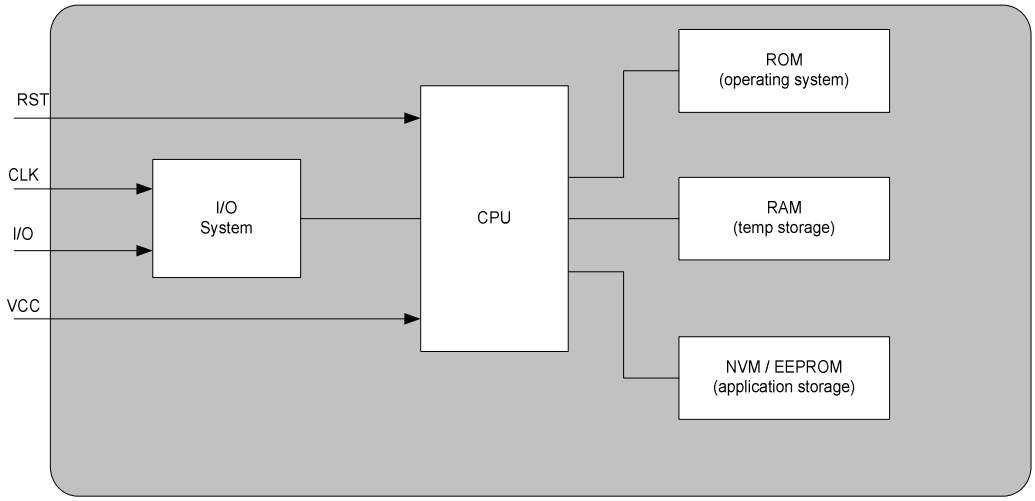
Estes cartões têm uma lógica interna para controlar o acesso à memória do cartão. Considerados as vezes como cartões memória inteligentes, estes dispositivos podem ser configurados relativamente à protecção contra escrita de alguns ou de todo *array* de memória. Alguns destes cartões podem ser configurados para restringir o acesso à leitura e à escrita. Isto é realizado com o uso de *password ou system key.* Este tipo de cartões pode ser dividido em secções lógicas, para planeamento de multi-funcionalidades.

STORED VALUE MEMORY CARDS

Estes cartões foram desenvolvidos, para uma funcionalidade específica, ou seja armazenar um valor ou um símbolo. Os cartões são descartáveis ou carregáveis. Muitos cartões deste tipo, possuem medidas de segurança permanentes no ponto da manufactura. Estas medidas podem incluir *passwords* entre outros mecanismos, que são *hard-coded* no chip pelo fabricante. Os array de memória destes dispositivos são configurados como decréscimos ou contadores. É pouca ou nenhuma a memória deixada, para qualquer outra função. Para aplicações simples tais como um cartão de telefone, o chip tem 60 ou 120 células de memória, uma para cada unidade de telefone. A célula de memória é limpa cada vez que uma unidade do telefone é usada. Uma vez que todas as unidades de memória são usadas, o cartão pode tornar-se inútil. Este processo pode ser invertido na caixa de cartões recarregáveis.

3. ARQUITECTURA

Neste tópico iremos analisar a arquitectura típica de um smart card. Na figura abaixo encontra-se um esquema dessa arquitectura. Neste tópico iremos analisar cada componente da arquitectura e que se encontram representados na figura.



CPU

Normalmente são usados nos smart card processadores de 8 bits. No entanto, e em casos que o justifiquem, são usados também processadores de 16 ou 32 bits. Estes processadores são processadores extremamente simples não usando tecnologias tais como multi-threading. Normalmente a velocidade destes processadores é de 1 MIPS. Também é incorporado um processador que tem como função a encriptação.

Memória

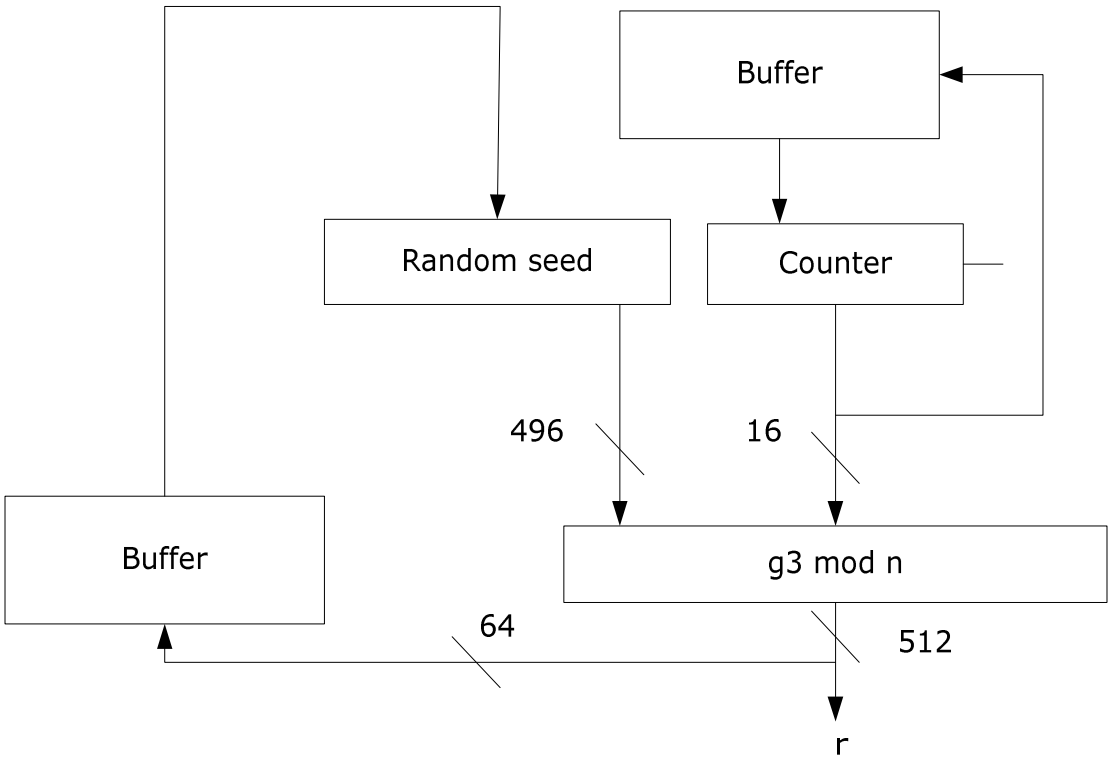
Existem tês tipos de memória nestes cartões. Existe uma RAM de 1kb, que tem as mesmas funções que num processador doméstico, ou seja, tem como função minimizar o tempo de acesso à memória. Existe também uma memória chamada EEPROM (Electrically Erasable PROM). Esta memória tem maior capacidade de armazenamento (entre 1 kb 24 kb), mas tem tempos de acesso muito maiores do que a RAM. Esta memória só pode ser acedida para leituras/escritas 100 000 vezes, sendo por isso considerada uma memória com acessos finitos. O último tipo de memória é uma memória ROM (read only memory) e contém os algoritmos de encriptação e o sistema operativo. A sua capacidade situa-se entre os 8 e os 4 Kb.

Input/Output

Existe uma única porta em série de I/O controlada pelo processador. Esta porta tem normalmente taxas de débito na ordem dos 9600 bits/segundo. No entanto estas taxas podem atingir 115200 bits/segundo. As comunicações entre esta porta e o processador estão normalizadas de acordo com a norma ISO 7816

Gerador de números aleatórios

De seguida segue um esquema de uma implementação de um gerador de números aleatórios. A sua importância será vista mais adiante, aquando da explanação de alguns algoritmos



Interfaces (IFDs)

Como todos os computadores, o smart card precisa de energia e de um relógio para funcionar. Estas necessidades são suprimidas por uma interface, normalmente um leitor de smart cards, que está em contacto com o cartão. O leitor também é responsável pelo canal de comunicação entre a aplicação de software do computador e o sistema operativo do smart card. Este canal é half-duplex, o que significa que podem ocorrer escritas e leituras, mas não ambas ao mesmo tempo. A informação que é enviada/recebida é guardada num buffer na RAM do smart card. Como esta memória não é muito grande (cerca de 1Kb) há necessidade da informação ser enviada em pequenos pacotes (10-100 bytes).

Em seguida apresenta-se uma tabela com as principais características de alguns smart cards

Smart Card	Word Size	ROM	EEPROM	RAM	Voltage	Clock	Write/erase cycles	Transmission rate
Infineon SLE 44C10S	8 bit	9K	1K	256b	2.7 – 5.5V	5MHz	500 000	9600 baud
Orga ICC4	8 bit	6K	3K	128b	4.7 – 5.3V		10 000	
GemCombi	8 bit		5K		4.5 – 5.5V	13.6MHz	100 000	106 kbaud
DNP Risona	8 bit		1K		5V	3.5MHz		9600 baud
AmaTech Contactless	8 bit		1K		5V	13.6MHz	100 000	
Schlumberger	8/16 bit	8K	16K	256b	5V	1-5MHz	100 000	9600 baud

Comunicações e formatos dos comandos

As comunicações com os smart cards estão bem descritas na norma 7816-3 da ISO. Basicamente pode-se definir dois protocolos: um orientado ao bit e outro orientado ao bloco.

A arquitectura aberta dos smart cards

A arquitectura aberta dos smart cards toma em conta o ciclo de vida dos smart cards. Esta está normalizada pela norma ISO 7816, e o princípio da arquitectura está baseada em três princípios:

- COMPILADOR DE SMART CARD: Para a criação dos smart cards, este cria desde um alto nível de descrição todos os dados requeridos para a inicialização e personalização do cartão
- O AGENTE DO SMART CARD: Controla o sistema operativo do cartão, e cobre a parte da interface de aplicação para um smart card
- A AGENCIA DE SAMART CARD: Esta controla o uso de diferentes agentes de smart cards e oferece à aplicação um tipo de smart cards independentes da interface.

Sistemas operativos

Normalmente encontra-se nos smart card um pequeno sistema operativo com cerca de 20 a 30 comandos. Existem normas (ISO 7816 e CEN 726) que especificam os comandos que um smart card pode suportar. A relação existente entre um smart card e leitor é uma relação “master/slave”. O leitor manda uma execução para o cartão, este executa-a e depois manda o resultado ao leitor.

Ficheiros de Sistema

A maior parte dos sistemas operativos suportam um ficheiro de sistema também baseado na norma ISO 7816. Actualmente um ficheiro smart card é simplesmente um bloco contínuo. Os ficheiros estão organizados em árvore. Os ficheiros smart card não têm a possibilidade de se alterar o seu tamanho, e como tal têm de ser criados com o tamanho esperado para o ficheiro. Existem diferentes tipos de ficheiros, como por exemplo cíclicos, lineares, SIM, etc. Todos eles possuem operações de leitura, escrita, criar, apagar e modificar. Alguns tipos de ficheiros possuem tipos especiais de operações, tal como se ilustra na tabela abaixo.

Tipo	Operações especiais	Exemplo
Linear	Procurar	Cartão de credito – tabela de conta
Cíclico	Ler próximo, ler anterior	Log das Transacções
Transparente	Ler e escrever binário	Imagem
Ficheiro SIM	Encripta, desencripta	Telemóvel

Software

Devido ao facto de a memória EEPROM apenas pode ser escrita um número finito de vezes. É típico na programação destes cartões, pôr primeiro o programa a correr num simulador para fazer o debug.

Performance

Philips, Siemens, Thomson e Motorola tem dominado o mercado de smart cards nos últimos anos. A existência de várias aplicações e protótipos confirmam esta realidade.

Linguagem de programação

A maior parte dos smart cards são programados em linguagens de baixo nível especificamente criadas para o efeito. Algumas dessas linguagens foram feitas com base em instruções nativas de alguns chips, como por exemplo o Motorola 6805, o Intel 8051, ou o Hitachi H8.
No entanto, em 2000 foi criado um novo tipo de cartões, chamados de cartões reconfiguráveis. Estes possuem um sistema operativo mais potente que permite que se adicione ou apague aplicações de código depois destes terem sido criados. Estes cartões são normalmente programados em Java, e daí a sua designação “Java cards”.

4. CRIPTOGRAFIA

Coprocessadores aritméticos

Uma das operações que com mais frequência e usada pelos smart cards é a multiplicação modular (d = t mod n onde t = a.b). Esta operação é normalmente utilizada na criptografia. A eficiência, medida em velocidade e complexidade do hardware, para realizar este tipo de operações, é um dos pontos chaves deste tipo de aplicações. Normalmente, ma maioria dos sistemas criptográficos a e b combinam muito mais frequentemente do que n, e portanto a maioria dos aceleradores criptográficos são optimizados para realizar aritmética modular trabalhando na base de um uso pouco frequente de n.
Um coprocessador aritmético (ACP) é um hardware dedicado para obter o valor de d, Normalmente os micro controladores dos cartões tratam o ACP como um conjunto de direcções RAM especiais, onde os dados são escritos na forma (a, b, n) e lidos na forma (d).
Normalmente os ACP's executam os seguintes passos (possivelmente integrados como um comando macro em uma liberaria):

1. Rasteio do hardware e inicialização
2. Carga dos operadores a, b e opcionalmente n
3. Multiplicação (possivelmente repetida)
4. Apresentação do resultado

Alguns dos algoritmos mais utilizados para obter o valor d são: Montgomery (utilizado pelos chips da Motorola), de Waleffe and Quisquater utilizado pela Philips), Levy-dit-Vehel and Naccache (utilizado pela Gemplus), Bucci and other variants of Barrett (utilizado pela Amtec), Sedlak (utilizado pela Siemens).

O SC49: Um micro controlador de chave publica

A Motorola teve uma participação muito activa na criação dos smart cards. Esta desenvolveu, em pareceria com a Groupe Bull, nos finais dos anos 70, um microprocessador que tem evoluído até aos dias de hoje.
A Motorola introduziu o MC68HC05SC49 (SC49 para abreviar) especialmente direccionado par a performance dos requisitos competacionais das aplicações de criptografia de chave publica e privada.
O SC49 trabalha com um coprocessador chamado MAP (modular arithmetic processor) que faz os cálculos do algoritmo de Montgomery. Este processador tem uma capacidade de multiplicação modular de 512*512 bits, mas que em conjunto com um software especial pode realizar uma multiplicação modular de 768 por 1024 bits.
A velocidade típica dos bus do SC45 pode variar entre 1MHZ e os 5 MHZ. Um PLL eleva a frequência de o relógio interno. Um gerador de números aleatório gera as chaves. A habilidade do coprocessador para gerar chaves significa que este nunca revela a chave secreta de um micro controlador de um smart card, e isto é um elemento crucial de segurança do sistema.
O SC49 corre o código com uma ROM de 13.3 Kbytes e uma RAM de 512 bytes. A disponibilidade para o utilizador são 4 kbytes de EEPROM com um

tempo de escrita de 2 ms. Esta assegura a retenção dos dados durante um período de 10 anos.

Montgomery

Os chips da Motorola, da Thomson e da Universidade Católica de Louvain usam este algoritmo. Em 1987 Montgomery publicou um algoritmo elegante para calcular d' = ab2^-N mod n. Este algoritmo cancela os 1's menos significativos de t somadores a t adequados múltiplos de n e desprezando o t à direita. Com as saídas dos d's os programadores devem corrigir o resultado aplicando o algoritmo a d' e uma constante 4^N mod n. O algoritmo é bastante simples (com d' inicialmente a 0):
for i = 0 to N - 1
d' = d' + b a[i]
d' = d' + n d'[0]
d' >> 1
if d' < n then return (d')
else return (d' - n)

Exemplos:

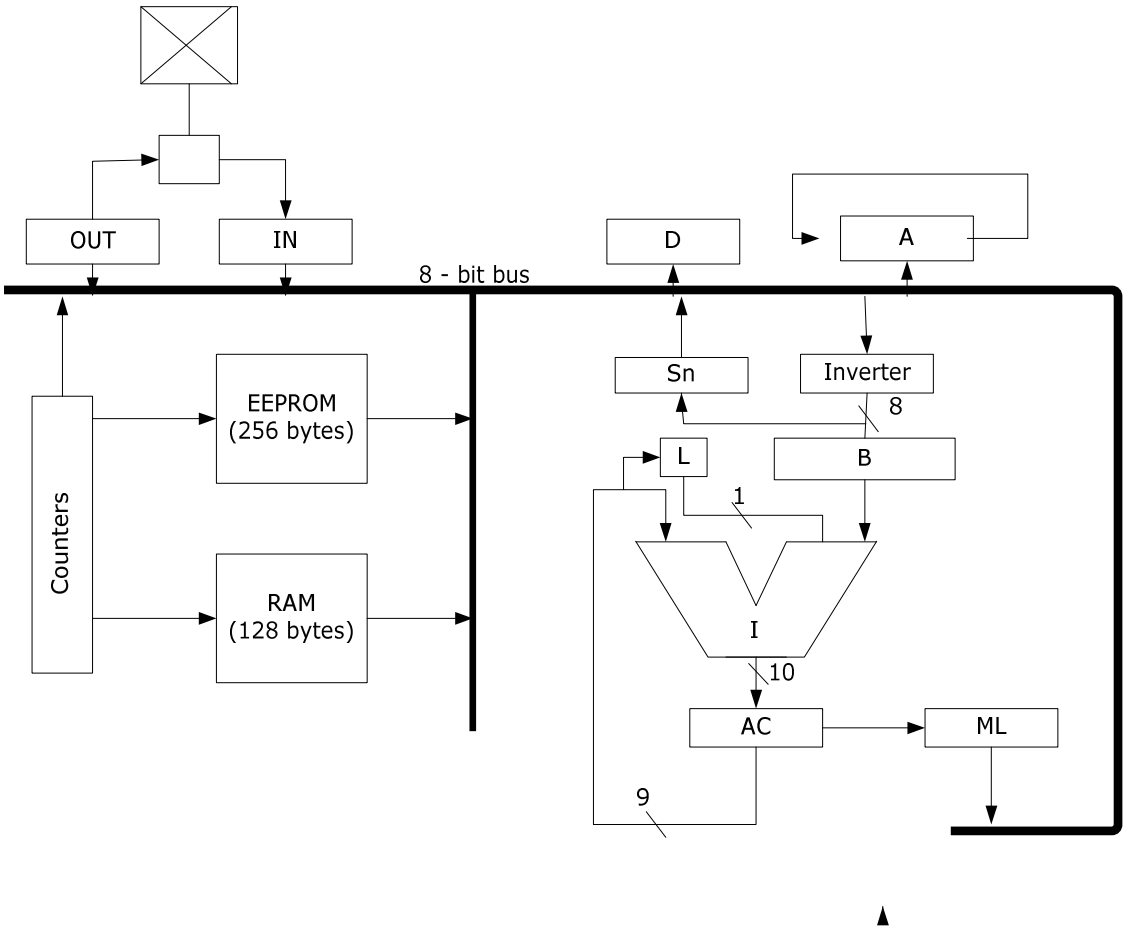
N=4 a=5 b=7 n=11

i	0	1	2	3
d' = + b a(i)	7	9	17	14
d' = + n d'(0)	18	20	28	14
d' >> 1	9	10	14	7

N = 8 a = 37 b = 19 n = 101

i	0	1	2	3	4	5	6	7
d' = + b a(i)	19	60	49	75	88	63	82	41
d' = + n d'(0)	120	60	150	176	88	164	82	142
d' >> 1	60	30	75	88	44	82	41	71

A imagem seguinte representa a implementação de um chip usando o algoritmo de Montgomery



De Waleffe e Quisquater

Os chips da Philipps usam este algoritmo. Os autores observaram que poderiam utilizar a função f(y,x,c) = yx + c, onde x é um inteiro de N bits, e y é um registo de v bits (geralmente 24) e c é um acumulador de N+v bits, para:

- Calcular o produto t (c é um acumulador da multiplicação, x é o a, e y é a i-ésima parte de b de v bits)
- Reduzir e obter t mod n somando a c=t um múltiplo y=k de x = n = complemento a 2 de n apropriado

É fácil estimar K usando os n bits mais significativos de v

Levy-dit-Vehel e Naccache

Chips da Gemplus usam este algoritmo, que calcula t com uma tripla multiplicação série – paralelo; este é um bloco de software que multiplica ax, ay e az simultaneamente, sempre que x ^ y = x ^ z = y ^ z = 0.
Este algoritmo executa os seguintes passos:

- Separar a b em dois blocos de N/2 bits b = b" | b', e faz x = b' ^ b"
- Calcular {u = ax, v = a(b' + x), w = a(b" + x)}
- Calcular t = delay [u + w] + u + v

Bucci e outras variantes de Barrett

Os chips da Amtec usam estes algoritmos. Barrett faz uma aproximação de d com d'=d, em que d'>d+2n. Este algoritmo usa um parâmetro L que delimita o tamanho máximo de t (L=2N) e uma constante K=2^L/n precálculada. O algoritmo segue os seguintes passos:

1. d = t - n((k(t >> (N - 1))) >> (L - N +1))
2. while d >= n do d = d – n (tem que se fazer pelo menos duas vezes)
3. return(d)

Sedlak

A Siemens usa este algoritmo de redução para os seus cálculos. Por ser idêntico aos algoritmos atrás descritos, não será aqui explicado

Implementação de alto nível

Normalmente é recomendado separar os sistemas de criptografia (RSA, DSA e outros) das operações de criptografia (verificação, encriptação, verificação de chaves, entre outros). Os desenhadores implementam isto criando um buffer I/O no cartão e no terminal. Neste modelo, os seguintes passos são realizados para que o cartão execute uma operação de criptografia:

1. Um comando de escrita selecciona um arquivo chave específico de um sistema
2. Um comando de escrita escreve os dados do processo (mensagens, texto cifrado entre outros)
3. Um comando de leitura (especifico a uma operação) devolve o resultado do cartão

Semelhante aproximação resulta em um conjunto reduzido de comandos e permite um upgrade do cartão sem adicionar novos comandos de comandos. O seguinte exemplo ilustra:

- A encriptação de uma mensagem "process me that" com chave RSA contida em um arquivo 2401
- A assinatura da mensagem "123" com o arquivo DSA 334A y
- Intercambio das chaves Diffie-Hellman com o arquivo E1F3

select file 2401
{RSA, 768, s/e/i}
put data
{"process me that"} /* dados a processar */
get data:
encrypt 0000
{"E32A371B908AB37"} /* = ENCRYPY.EXE */

select file 334A
{DSA, 512, s} /* = TYPE em DOS */
put data
{"123"} /* dados a processar */
get data:
sign 0000

{"ADE603B826FDE04"} /* = SIGN.EXE */
select file E1F3
{D-H, 512, k} /* = TYPE em DOS */
put data
{"process me that"} /* a ^ x mod p */
get data:
key exchange
{"AE589EB6A564CDD"} /* = KEY_EXCHANGE.EXE devolve a ^ y mod p */

Durante um intercâmbio de chaves, o utilizador deve especificar um ID de um arquivo de destino (neste caso 2010) para a chave comum. O mundo externo nunca pode aceder a este valor.

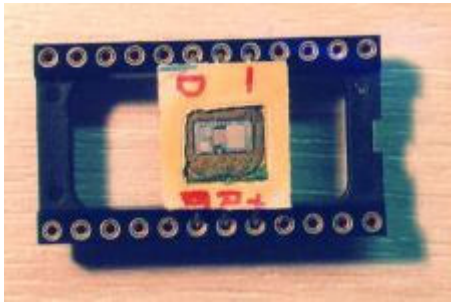
5. TECNOLOGIA E SEGURANÇA

Os Smart Cards são muitas vezes usados em aplicações, que requerem uma forte segurança, protecção e autenticação. A tecnologia e a segurança, estão muito relacionadas. *Crackers* encontram sempre maneiras, pelas quais descobrem os supostos dados seguros nos cartões, o que leva aos fabricantes surgirem com mais sofisticadas protecções e chaves nos cartões, sendo um ciclo sem fim, com ambos os lados a utilizarem e a inventarem tecnologia melhor.

- Segurança ao nível do Hardware

Problemas

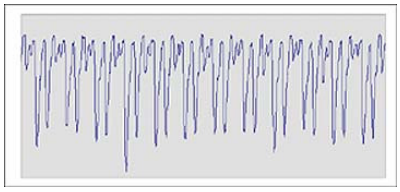
Todos os dados e *passwords* são armazenados na EEPROM e podem ser apagados ou modificados por uma fonte de voltagem fora do normal. Por isso alguns processadores, possuem sensores implementados para detectarem mudanças do ambiente. Embora, seja difícil encontrar o nível certo de sensibilidade, o que leva a que este sistema não seja usado largamente. Outro método de ataque, inclui aquecimento do controlador a altas temperaturas ou focalizando luz ultravioleta na EEPROM, para remover o bloqueio de segurança. Os ataques invasivos são mais destrutivos, quando o cartão é cortado e o processador removido. Sendo ai possível o *reverse-engineered*do do cartão.



Smart Card depois do ataque

Ácido Nítrico (>98º NHO3) dissolve a embalagem sem afectar o chip

Análise de energia diferencial (DPA), é um ataque estatístico num algoritmo cryptográfico, que compara uma hipótese com o resultado medido, que frequentemente consegue obter uma chave de encriptação de um Smart Card ou de outro dispositivo. A análises simples de energia (SPA), análise directa dos dados gravados da energia para determinar acções e dados, é também utilizada.



Análise de energia

Soluções

Diversas tecnologias foram e estão a ser desenvolvidas para proteger os Smart Cards :

Barreira Tecnológica – A tecnologia avançada de 0.6 mícron (hoje em dia existem processadores com tecnologia de 0.16 mícron) reduz extremamente o tamanho e o consumo de energia dos cartões, bem como as variações relativas nos suas operações. Isto torna difícil que métodos externos do SPA/DPA distingam entre flutuações normais do cartão e as flutuações dos dados relacionados.

Flutuação do Relógio – Uma funcionalidade especial na gestão do software do relógio, quando usada concretamente, resulta no sincronismo altamente variável do software quando é executado a aplicação.

Comportamento Imprevisível – Um temporizador interno tem com potencialidade de interrupção, e um gerador aleatório do número são usados para introduzir variações imprevisíveis na maneira como é executado o software, com mudanças consequentes no teste padrão do consumo de potência.

Projecto Robusto – Um projecto modular permite que as novas variações do hardware, incluindo as alterações habituais, sejam produzidas rapidamente e eficientemente, desse modo permite uma resposta rápida aos novos cenários de ataque.

Controle de Memória para multi-aplicações – Um sistema de controle aumenta o acesso à memória, fornecendo um suporte seguro ao sistema operativo para cartão multi-aplicações.

Mecanismo de segurança e funções de *firmware* – Um aumento dos mecanismos de segurança e das funções de *firmware*, permitem que a aplicação detecte e responda apropriadamente à ocorrência das circunstâncias que puderam indicar um ataque. Estas circunstâncias incluem condições funcionamento/operação inválidas, endereços incorrectos, e violações da integridade do *chip*; as respostas possíveis incluem interrupções, restauração do programa, apagamento imediato de toda a RAM e a programação flash de toda a EEPROM.

6. JAVA CARDS

Um smart card "Java Card" é basicamente um cartão que pode ser programado numa linguagem de alto nivel, em vez de ser programado em assembly. No entanto, este tipo de cartões ainda tem outras vantagens, nomeadamente a portatibilidade e o seu design baseado em applets. A prova do seu sucesso é dada pela percentagem de Java cards feitos face ao total de smart cards, que em 2001 era de cerca de 24% (note-se que este tipo de cartões foi criado em Setembro de 1996).
No entanto é praticamente impossível implementar num smart card um sistema de Java, dado o tamanho que um sistema de Java normalmente ocupa. Para que seja possível a implementação num smart card divide-se o sistema em duas partes mais pequenas (Java card virtual machine e Java Card Runtime Environment) e que serão descritas nas duas seguintes secções.

JAVA CARD VIRTUAL MACHINE

Esta parte define uma máquina virtual que facilita bastante o trabalho dos programadores.

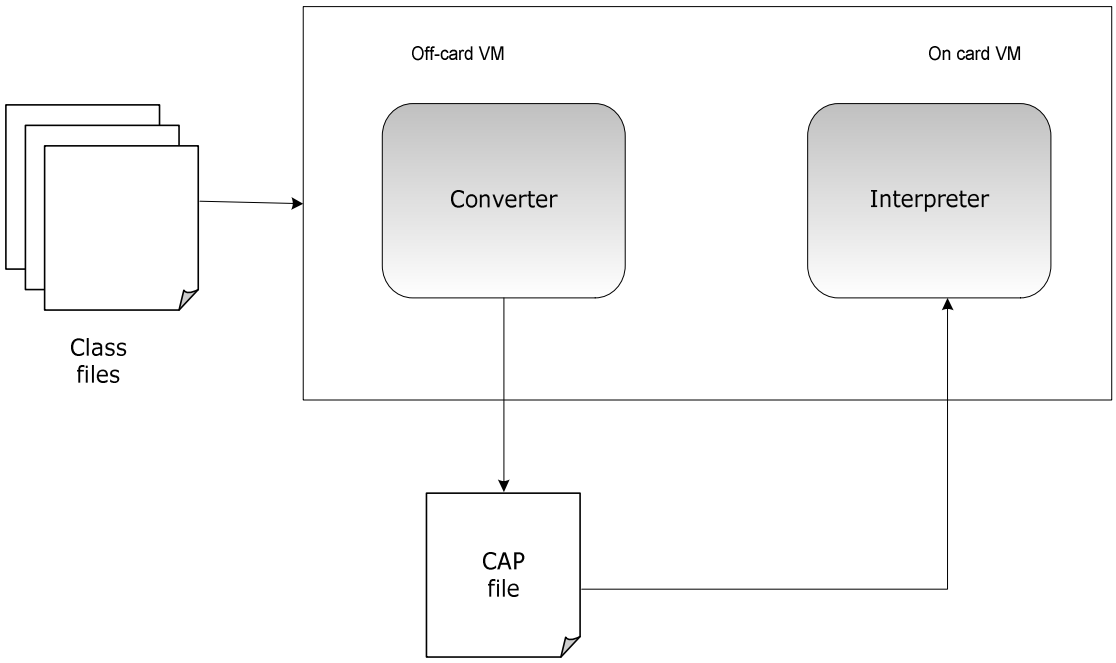
Linguagem de programação

Por razões de eficiência, a Java card virtual machine (JCVM) apenas permite a utilização de uma parte da linguagem Java a ser usada na programação de applets. Segue-se uma breve descrição desta situação:

Tipos aceites	Tipos não aceites
boolean, byte, short, int	double, float, long, character, string
Arrays de 1 dimensão	Arrays multi-dimensionais
Java classes, packages, interfaces, exceptions	Dynamic Class Loading
Java object-oriented features: inheritance, virtual methods, overloading and dynamic object creation, access scope, and binding rules	Security Manager
	Garbage Collection
	Threads

Estrutura divisível

A JCVM é dividida em duas partes (conversor e interpretador) conforme ilustrado na figura abaixo

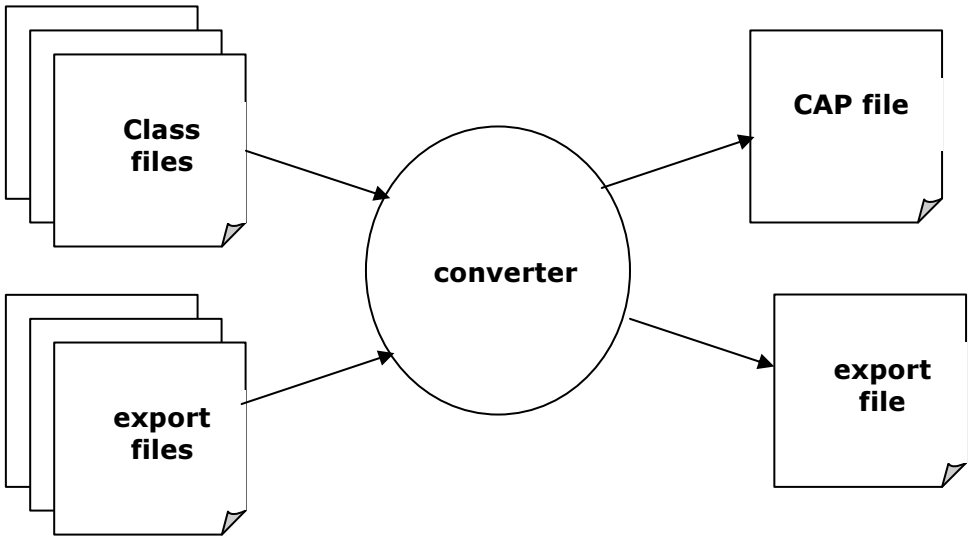


No início são dados todos ficheiros necessários para a execução.
O compilador de Java tem as seguintes tarefas:

- Verificar violações da linguagem
- Resolver as referências simbólicas de modo a ficarem mais compactas e assim permitir um melhor desempenho do cartão
- Optimizar o código binário
- Criar a máquina virtual das estruturas de dados para representar as classes
- Produzir um ficheiro binário executável CAP, que possa correr no interpretador

NOTA: Um ficheiro CAP é um tipo especial de ficheiros criados exclusivamente para estes tipos de cartões.

A figura abaixo representa esquematicamente um compilador



7. CONCLUSÃO

Como pode ser visto ao longo do trabalho, um smart card pode ter vários tipos, como por exemplo cartões de memória ou cartões com capacidade de processamento. Estes últimos têm uma arquitectura em tudo idêntica à de um computador pessoal (naturalmente com capacidades em termos de memória e processamento mais reduzidas).
A característica em que as empresas deste tipo de cartões mais têm investido é a segurança, pois esta é a principal razão do sucesso que estes cartões têm apresentado, nomeadamente em relação aos cartões de banda magnética.

8. PERGUNTAS & RESPOSTAS

Explica as variantes, memória e microprocessador nos smart cards e também cartões de contacto e *contactless*?

O smart cards tem um micro processador e/ou uma memória embutida nele, na presença de um leitor, o seu poder de processamento serve para várias aplicações. Disponibilizando dados pessoais e financeiros, apenas aos utilizadores apropriados.

Smart cards surgem em duas variedades memória e microprocessador. Os cartões de memória apenas armazenam dados e podem ser visualizados, tal como uma pequena disquete com um regime de segurança opcional. O cartão com microprocessador, este cartão tal como um computador tem *input/output*, sistema operativo e um disco rígido com alguns mecanismos de segurança.

Cartões contacto e *contactless*, são dois tipos de interfaces diferentes para smart cards. Os cartões de contacto são inseridos num leitor de smart cards, têm contacto físico com o leitor. Enquanto que os *contactless* smart cards, possuem uma antena no inerente ao cartão que permite a comunicação com o leitor, sem contacto físico. Existem uns híbridos que combinas as capacidades dos dois com alto nível de segurança.

Descreva de forma resumida a arquitectura de um smart card, que não seja apenas um cartão de memória?

Um smart card é constituído por um processador de 8 bits e por um co-processador que tem como finalidade o processamento dos algoritmos de criptografia. Um smart card tem três tipos de memórias: uma RAM, uma ROM e uma EEPROM que se pode comparar (em termos de finalidades) a um disco rígido num computador de secretária.
O smart card comunica com o mundo exterior (normalmente um leitor) através de um sistema de I/O.

9. AGRADECIMENTOS

Os autores agradecem a todos os colegas que o incentivaram e ajudaram na pesquisa e elaboração do artigo. Não podíamos, igualmente, deixar de agradecer aos docentes da disciplina de “Arquitectura de Computadores 2”, da Licenciatura em Engenharia Informática, por toda a ajuda e motivação.

10. REFERÊNCIAS

- Java CardTM Technology for Smart Cards: Architecture and Programmer's Guide, by Zhiqun

- Grupo Smart Card http://www.smartcard.co.uk/

- SUN - Java Card Platform http://java.sun.com/products/javacard/

- Desing Smart Cards http://people.cs.uchicago.edu/~dinoj/smartcard/

- CardLogix http://www.cardlogix.com