República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0612024-5 A2**

BRPI0612024A2

(22) Data de Depósito: 11/05/2006
(43) Data da Publicação: 13/10/2010
(RPI 2075)

(51) Int.Cl.:
G07F 7/10
G06F 21/00
H04L 9/00
G06K 19/07

(54) Título: **DISPOSITIVO, MÉTODO PARA INICIALIZAR UMA CHAVE SEGURA A SER COMPARTILHADA ENTRE O PRIMEIRO CIRCUITO INTEGRADO E O SEGUNDO CIRCUITO INTEGRADO, CIRCUITO INTEGRADO, PROGRAMA DE COMPUTADOR EXECUTADO EM UM CIRCUITO INTEGRADO, E, CHIP DE GERENCIAMENTO DE ENERGIA ADAPTADO PARA EXECUTAR O GERENCIAMENTO DE ENERGIA DO DISPOSITIVO**

(30) Prioridade Unionista: 13/05/2005 US 11/128,676

(73) Titular(es): NOKIA CORPORATION

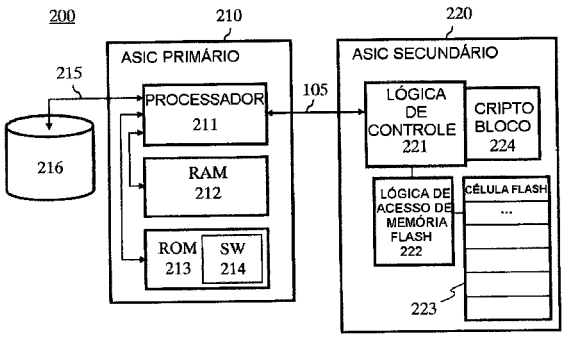
(72) Inventor(es): JAN-ERIK EKBERG, LAURI PAATERO, NADARAJAH ASOKAN

(74) Procurador(es): Araripe & Associados

(86) Pedido Internacional: PCT FI2006050186 de 11/05/2006

(87) Publicação Internacional: WO 2006/120302de 16/11/2006

(57) Resumo: DISPOSITIVO, MÉTODO PARA INICIALIZAR UMA CHAVE SEGURA A SER COMPARTILHADA ENTRE O PRIMEIRO CIRCUITO INTEGRADO E O SEGUNDO CIRCUITO INTEGRADO, CIRCUITO INTEGRADO, PROGRAMA DE COMPUTADOR EXECUTADO EM UM CIRCUITO INTEGRADO, E, CHIP DE GERENCIAMENTO DE ENERGIA ADAPTADO PARA EXECUTAR O GERENCIAMENTO DE ENERGIA DO DISPOSITIVO. Um símbolo de segurança interno mas não integrado é fornecido para o dispositivo, que compreende um primeiro circuito integrado compreendendo um processador seguro. O símbolo de segurança é fornecido pelo segundo circuito integrado separado do primeiro circuito integrado, O segundo circuito integrado compreende um dispositivo de armazenagem não-volátil seguro. O processador seguro comunica a informação para o segundo circuito de maneira segura para a informação segura ser armazenada seguramente em um dispositivo de armazenagem não-volátil seguro, e o segundo circuito integrado comunica a informação armazenada em um dispositivo de armazenagem não-volátil seguro para o processador seguro de maneira segura. As comunicações são asseguradas por meio de criptografia. O primeiro circuito integrado e o segundo circuitointegrado são partes internas do dispositivo. Um método de utilização para distribuir a chave segura a ser compartilhada entre os circuitos e a ser usado na criptografia é também descrito.



PI 0612024-5

"DISPOSITIVO, MÉTODO PARA INICIALIZAR UMA CHAVE SEGURA A SER COMPARTILHADA ENTRE O PRIMEIRO CIRCUITO INTEGRADO E O SEGUNDO CIRCUITO INTEGRADO, CIRCUITO INTEGRADO, PROGRAMA DE COMPUTADOR EXECUTADO EM UM CIRCUITO INTEGRADO, E, CHIP DE GERENCIAMENTO DE ENERGIA ADAPTADO PARA EXECUTAR O GERENCIAMENTO DE ENERGIA DO DISPOSITIVO".

CAMPO DA INVENÇÃO

A presente invenção refere-se à provisão de um dispositivo de armazenagem seguro, de integridade protegida para um dispositivo. Particularmente, mas sem exclusividade, ela se refere à manutenção de estado em um dispositivo portátil, tal como um telefone móvel.

ANTECEDENTES DA INVENÇÃO

O uso de dispositivos de comunicação pessoal em vários aspectos de nossas atividades cotidianas aumentou drasticamente nos últimos anos. Telefones móveis modernos tornam-se dispositivos de multiuso capazes de diversas novas aplicações de segurança, tal como clientes de gerenciamento de direitos digitais (DRM) e transações bancárias. Com a proliferação dos dispositivos de comunicação pessoal, se tornou cada vez mais importante proteger os dados cruciais armazenados dentro do dispositivo. Por exemplo, o uso de um PIN tem sido implementado com os dispositivos de comunicação pessoal para controlar acesso ao dispositivo. Contudo, é possível que se possa adivinhar o PIN se for concedido um número ilimitado de tempo e de tentativas para se introduzir um PIN. Desse modo, além do uso de um PIN, é útil limitar o número de tentativas para se introduzir um PIN.

Para limitar o número de tentativas de acesso ao dispositivo, é possível utilizar algum tipo de contador no dispositivo de comunicação pessoal. O contador é limitado criptograficamente à informação de estado relacionada aos dados cruciais usados pelo dispositivo e pode ser usado como um mecanismo de proteção contra furto. Nesse contexto, a informação de estado pode significar informação indicando o número de tentativas de acesso ao PIN, incorretas, sucessivas. Após

certo número (digamos três) de tentativas incorretas para entrada do PIN, o dispositivo é bloqueado até que uma chave de desbloqueio de PIN especial (isto é, código PUK) seja introduzida.

Se o dispositivo de armazenagem de informação de estado no dispositivo não tiver proteção de integridade, pode ser possível para uma pessoa mal-intencionada registrar a informação de estado atual, tentar três PINs sucessivos (durante o qual o dispositivo atualizará a informação de estado), e sobregravar a informação de estado recentemente atualizada com os dados gravados antigos. Desse modo, a pessoa mal-intencionada conseguiria mais três tentativas para descobrir o PIN correto.

Além de manter a monitoração das tentativas de acesso PIN/senha, incorretas, sucessivas, existem vários outros usos na área de DRM, nos quais a capacidade de armazenar seguramente informação de estado, em um dispositivo pessoal seguro, pode ser necessária.

Monitorar um valor de contador pode também ser útil quando for necessário controlar o consumo de conteúdo de dados. Por exemplo, uma terceira parte poderia pretender impedir que um usuário de um dispositivo de comunicação pessoal reproduzisse uma música mais do que dez vezes. O direito de reproduzir a música dez vezes é distribuído como um certificado eletrônico que especifica uma limitação de 10 usos mediante implementação de um contador. Contudo, se um usuário pode reiniciar o contador após cada uso, a música pode ser reproduzida indefinidamente sem se ter que pagar ao proprietário dos dados, por cada uso.

Em dispositivos móveis, também existem estados de segurança dependentes do dispositivo que deveriam ser acessíveis de forma segura por toda a vida útil do dispositivo. Por exemplo, um telefone móvel pode ter um recurso de bloqueio de telefone que efetivamente deve impedir o uso de telefones roubados. Quando o bloqueio é engatado, um identificador do presente módulo de identidade de assinante (SIM) é armazenado em uma memória persistente regravável do telefone com uma representação adequada (por exemplo, um código hash de sentido único) de um código de números de combinação. Sempre que o SIM é

substituído, se a proteção do telefone estiver habilitada, o telefone primeiramente solicita ao usuário o código de números correspondente e somente se esse for introduzido de forma bem-sucedida, é que o telefone armazena o ID do novo SIM e permite seu uso. Contudo, para impedir ataque de força bruta, o telefone também deve manter um contador de códigos de números que falharam de modo que após três tentativas mal-sucedidas, o telefone se torna mais completamente bloqueado.

Na área de DRM, onde manutenção não-volátil de informação de estado crucial tem sido necessária, vários métodos de criptografia têm sido usados para proteger a informação de estado crucial, tal como valores cruciais de contador, etc.

Um aspecto da criptografia envolve a codificação ou criptografia de dados digitais para tornar os mesmos incompreensíveis por todos exceto os recebedores pretendidos. Em outras palavras, quando a criptografia é empregada no contexto de DRM, os dados são criptografados e uma chave de descriptografia é entregue àqueles terminais ou usuários que pagaram para consumir o conteúdo de dados. Com essa finalidade, os sistemas criptográficos podem ser usados para preservar a privacidade e integridade dos dados mediante prevenção do uso e alteração dos dados por partes não-autorizadas. Além da criptografia, também a autenticação da origem dos dados é usada para se ter certeza de que, por exemplo, apenas uma parte que tem a chave certa pode gerar a assinatura certa ou o código de autenticação de mensagem (MAC).

Por exemplo, uma mensagem de texto simples consistindo em sons digitalizados, letras e/ou números pode ser codificada numericamente e, então, criptografada utilizando-se um algoritmo matemático complexo que transforma a mensagem codificada com base em um determinado conjunto de números ou dígitos, também conhecido como chave de cifrar. A chave de cifrar é uma seqüência de bits de dados que pode ser aleatoriamente escolhida ou ter propriedades matemáticas especiais, dependendo do algoritmo ou criptossistema utilizado. Algoritmos criptográficos sofisticados implementados em computadores podem transformar e manipular os números que têm centenas ou milhares de bits de comprimento e

podem resistir a qualquer método conhecido de descriptografia não-autorizada. Existem duas classes básicas de algoritmos criptográficos: algoritmos de chave simétrica e algoritmos de chave assimétrica.

Algoritmos de chave simétrica utilizam uma chave de cifrar idêntica tanto para criptografar, pelo remetente da comunicação, como para descriptografar, pelo recebedor da comunicação. Criptossistemas de chave simétrica são elaborados com base na confiança mútua das duas partes compartilhando a chave de cifrar para usar o criptossistema para proteção contra terceiras partes que não são confiáveis. Um algoritmo de chave simétrica conhecido é o algoritmo National Data Encryption Standard (DES) publicado primeiramente pelo National Institute of Standards and Technology. Vide *Federal Register, Mar. 17, 1975, Vol. 40, N° 52 e Aug. 1, 1975, Vol. 40, N° 149.* O dispositivo criptográfico remetente utiliza o algoritmo DES para criptografar a mensagem quando carregada com a chave de cifrar (uma chave de cifrar DES tem 56 bits de comprimento) para aquela sessão de comunicação (a chave de sessão). O dispositivo criptográfico recebedor utiliza um inverso do algoritmo DES para descriptografar a mensagem criptografada quando carregada com a mesma chave de cifrar conforme usada para criptografia.

Algoritmos de chave assimétrica utilizam diferentes chaves de cifrar para criptografar e descriptografar. Em um criptossistema utilizando um algoritmo de chave assimétrica, o usuário torna pública a chave de criptografia e mantém a chave de descriptografia privada, e não é exeqüível derivar a chave de descriptografia privada a partir da chave de criptografia pública. Desse modo, qualquer um que conheça a chave pública de um usuário específico poderia criptografar uma mensagem para aquele usuário, ao passo que apenas o usuário, que é o proprietário da chave privada correspondendo àquela chave pública, poderia descriptografar a mensagem. Esse sistema de chave pública/privada foi proposto primeiramente em Diffie e Hellman, *"New Directions in Cryptography"*, IEEE Transactions on Information Theory, November 1976, e na Patente US 4.200.770 (Hellman et al.).

Os sistemas criptográficos assinalados acima têm sido usados para proteger

informação de estado em um dispositivo de comunicação pessoal mediante armazenagem segura da informação de estado em umas duas formas. Em primeiro lugar, mediante gravação de um instantâneo para a informação de estado e computando a sua "soma de verificação", por exemplo, através do uso de uma função hash de sentido único. O resultado é armazenado dentro de um local de memória resistente à violação do dispositivo. Portanto, se alguém tentar mudar a informação de estado, a soma de verificação do resultado não combinará com o valor de soma de verificação armazenado no dispositivo pessoal. Em segundo lugar, mediante uso de um contador monotônico, persistente dentro do dispositivo. Cada vez que houver uma mudança de estado, a informação de estado é armazenada junto com o valor atual do contador criptografado utilizando uma chave de dispositivo. Desse modo, ninguém pode mudar a informação de estado criptografada sem a chave.

Contudo, esses dois métodos da técnica anterior exigem uma pequena quantidade de armazenagem de ler-gravar dentro da mesma zona resistente à violação que contém o próprio processador seguro.

No campo de DRM, as aplicações envolvidas são providas tipicamente pelo circuito digital integrado. Se um processador seguro executando tal aplicação tiver espaço atualizável suficiente dentro de seu dispositivo de armazenagem persistente, resistente à violação, é mais propriamente fácil implementar a proteção de integridade para informação de estado. Maheshwari et al. revelou tal arranjo em *"How to Build a Trusted Database System on Untrusted Storage"*, OSDI 2000. Infelizmente, as razões econômicas estão erradicando as memórias regraváveis, não-voláteis nos circuitos digitais integrados. Ter uma memória atualizável, ou um dispositivo de armazenagem de ler-gravar, integrado dentro do perímetro resistente à violação do processador seguro, é dispendioso, especialmente em dispositivos particularmente limitados em termos de recursos como os telefones móveis. Em outras palavras, a armazenagem de informação de estado e processamento seguro das aplicações nem sempre são econômicos (ou nem mesmo práticos) dentro da mesma zona resistente à violação, que o

processador seguro, por exemplo, dentro do circuito integrado do processador seguro.

Além disso, como sabido na técnica, os blocos IC digitais tendem a ser otimizados em termos de custo de modo que alguns deles nem mesmo podem acomodar uma memória persistente regravável (por exemplo, memória flash), uma vez que a inclusão da mesma obrigaria a fabricação de seis camadas de silício em vez das quatro camadas comuns para a área do bloco IC. Portanto, outra vez, prover simplesmente um processador seguro com uma memória não-volátil parece não ser adequado economicamente, e tecnicamente, para todos os usos.

Conseqüentemente, existe um problema em como implementar uma armazenagem segura de integridade protegida para um processador seguro de um dispositivo geralmente limitado em termos de recursos.

Como uma solução prática para esse problema, um Pedido de Patente co-pendente dos requerentes do presente pedido, número de publicação *US 2003/0079122 A1*, apresenta a idéia de utilizar um dispositivo de armazenagem resistente à violação, externo, para armazenar informação de estado importante. A idéia de contadores autenticados (ou "confiáveis") é introduzida. O pedido de patente US *2003/0079122 A1*, revela que um contador autenticado pode ser implementado em um símbolo de segurança resistente à violação, externo, tal como um cartão inteligente, o qual pode ser usado pelo processador seguro para proteção de integridade de sua armazenagem de estado. Para fazer com que isso funcione, o processador seguro precisa ser capaz de autenticar o símbolo de segurança externo. Com essa finalidade, o pedido de patente *2003/0079122 A1* revela o uso de uma infra-estrutura de chave pública (PKI).

Contudo, uma infra-estrutura de chave pública é mais propriamente complexa em termos de configuração porque envolve a coordenação e acordos entre fabricantes de dispositivo e fabricantes de símbolos de segurança, externos. Ela também impõe uma quantidade de carga de processamento aos símbolos de segurança, externos, ou memórias.

SUMÁRIO DA INVENÇÃO

É um objetivo da invenção, evitar ou pelo menos aliviar, os problemas encontrados na técnica anterior.

De acordo com um primeiro aspecto da invenção é provido um dispositivo que compreende:

um primeiro circuito integrado mediante formação de uma primeira zona confiável, o primeiro circuito integrado compreendendo um processador seguro; e

um segundo circuito integrado separado do primeiro circuito para formar uma segunda zona confiável, o segundo circuito integrado compreendendo um dispositivo de armazenagem, não-volátil, seguro, dentro da segunda zona confiável, em que

o processador seguro é configurado para comunicar informação a partir da primeira zona confiável para a segunda zona confiável de uma maneira segura para a informação segura ser armazenada seguramente no dispositivo de armazenagem, não-volátil, seguro;

o segundo circuito integrado é configurado para comunicar informação armazenada em seu dispositivo de armazenagem, não-volátil, seguro, a partir da segunda zona confiável para o processador seguro dentro da primeira zona confiável de uma maneira segura; e em que

o primeiro circuito integrado e o segundo circuito integrado são partes internas do dispositivo.

Em uma modalidade, um símbolo de segurança, interno, ou dispositivo de armazenagem é provido para armazenar seguramente a informação segura, tal como informação indicativa de diferentes contadores. Um símbolo de segurança interno é aquele que é parte do dispositivo, e pode ser inicializado durante montagem do dispositivo. Entretanto, o símbolo de segurança não está dentro do perímetro resistente à violação do processador seguro. Vantajosamente, o símbolo de segurança interno é provido pelo segundo circuito integrado, o qual contém a memória não-volátil capaz de manter a informação de estado de segurança relacionada por um período de tempo sem fornecimento contínuo de energia.

Vantajosamente, o dispositivo compreende um circuito de armazenagem e

processamento de informação de segurança em um módulo de montagem comum de modo que a comunicação entre o primeiro e o segundo circuito pode não ser detectável a partir de conectores interconectando os dois módulos de montagem.

Além disso, pode ser econômico prover o primeiro circuito apenas com uma memória volátil regravável e desse modo possivelmente reduzir a complexidade do primeiro circuito enquanto fazendo uso do segundo circuito que pode ser mais bem adequado para prover uma memória regravável persistente. Por exemplo, blocos de circuito integrado (IC) digital, atuais, podem não ser adaptados economicamente para prover uma memória flash enquanto que os circuitos analógicos, tal como um chip de gerenciamento de energia, pode ser adaptado de forma relativamente simples para prover uma armazenagem persistente com pequeno custo. Isso é particularmente conveniente no caso de produtos fabricados em dezenas ou centenas de milhões tais como os telefones móveis.

Vantajosamente, o primeiro e segundo circuitos são adaptados para estabelecer um protocolo de comunicação, seguro a ser usado entre a primeira e a segunda zona confiável. O protocolo contém pelo menos comandos LER e GRAVAR e operações de mudança de chave, por exemplo, um comando GRAVAR CHAVE. Conseqüentemente, em uma modalidade o dispositivo é provido com gerenciamento de estado de chave permitindo que mais do que uma chave seja compartilhada entre a primeira e a segunda zona confiável. A armazenagem não-volátil da segunda zona confiável pode compreender pelo menos uma variável de estado de chave indicando a chave compartilhada a ser usada na comunicação. A variável de estado é mantida e atualizada quando uma chave compartilhada entre a primeira e a segunda zona confiável é mudada.

Uma modalidade da invenção provê uma verificação da condição de recente para as operações de LER e GRAVAR. Para as operações de LER: o processador seguro pode incluir um valor aleatório como um parâmetro em um comando LER de modo que ele pode verificar se um resultado subseqüente recebido a partir do segundo circuito integrado é recente, isto é, não reproduzido. Para operações de GRAVAR: a propriedade de recente pode ser realizada mediante inclusão do valor

antigo em uma célula alvo como um parâmetro no comando GRAVAR, e mediante verificação no segundo circuito integrado, se esse parâmetro no comando GRAVAR for idêntico ao valor antigo na célula alvo. Se não for, o comando GRAVAR não será permitido.

Em ainda outra modalidade, o segundo circuito integrado é adaptado para usar apenas uma única primitiva criptográfica para toda a sua operação criptográfica.

De acordo com um segundo aspecto da invenção é provido um método para inicializar uma chave segura a ser compartilhada entre um primeiro circuito integrado e um segundo circuito integrado, o método compreendendo:

distribuir a chave segura a ser compartilhada entre o primeiro circuito integrado e o segundo circuito integrado a partir de um servidor de distribuição de chave segura para o primeiro e segundo circuitos integrados, em que o método compreende:

proteger a distribuição da chave segura a partir do servidor de distribuição de chave segura para o primeiro circuito integrado utilizando uma primeira chave, a primeira chave sendo uma chave compartilhada antecipadamente entre o primeiro circuito integrado e o servidor de distribuição de chave segura; e

proteger a distribuição da chave segura a partir do servidor de distribuição de chave segura para o segundo circuito integrado utilizando uma segunda chave, a segunda chave sendo uma chave compartilhada antecipadamente entre o segundo circuito integrado e o servidor de distribuição de chave segura.

De acordo com um terceiro aspecto da invenção é provido um circuito integrado, o qual compreende:

um processador seguro para emitir e criptografar comandos a serem transferidos para outro circuito integrado de acordo com um protocolo seguro, em que

o protocolo seguro compreende uma operação de mudança de chave através da qual uma chave segura compartilhada entre o circuito integrado e o outro circuito integrado pode ser mudada.

De acordo com um quarto aspecto da invenção é provido um programa de computador executável por um processador seguro de um circuito integrado, compreendendo:

código de programa para emitir comandos para serem transferidos para outro circuito integrado de acordo com um protocolo seguro; e

código de programa para fazer com que o processador seguro inicie uma operação de mudança de chave por intermédio da qual uma chave segura compartilhada entre o circuito integrado e outro circuito integrado é mudada.

De acordo com um quinto aspecto da invenção é provido um circuito integrado, o qual compreende:

uma memória não-volátil para armazenar dados seguros recebidos a partir de outro circuito integrado; e

lógica para acessar a memória não-volátil, em que o circuito é adaptado para comunicar os dados seguros armazenados na memória não-volátil e protegidos por intermédio de criptografia para outro circuito integrado, e em que

o circuito integrado é configurado para usar uma única primitiva criptográfica.

De acordo com um sexto aspecto da invenção é provido um programa de computador executável em um circuito integrado, compreendendo:

código de programa para proteger as comunicações com outro circuito integrado mediante uso de uma chave compartilhada entre o circuito integrado e o outro circuito integrado; e

código de programa para mudar entre diferentes estados de chave de diferentes níveis de segurança.

De acordo com um sétimo aspecto da invenção é provido um chip de gerenciamento de energia para realizar gerenciamento de energia de um dispositivo, o chip de gerenciamento de energia compreendendo uma memória não-volátil, segura, e lógicas, de modo a prover um símbolo de segurança para um processador seguro.

O programa de computador de acordo com o quarto e/ou sexto aspecto da presente invenção pode ser armazenado em meios legíveis por computador. O programa de comutador de acordo com o quarto e/ou sexto aspecto da presente invenção pode ser transportado por um sinal de informação.

Vantajosamente, a operação do processador e/ou lógica do segundo circuito

integrado pode ser programada por intermédio de programa de computador gravado em uma memória a partir da qual o programa é subseqüentemente executado para controlar a operação de um dispositivo respectivo. Vantajosamente, o programa pode ser gravado apenas durante o processo de produção de um dispositivo compreendendo o processador e a lógica. Alternativamente, o programa pode ser armazenado na configuração de um dispositivo compreendendo o processador e a lógica para seu uso normal. A armazenagem na configuração pode ser realizada em conexão de serviço ou uso final.

De acordo ainda com outro aspecto da invenção é provido um primeiro circuito integrado em linha com o primeiro aspecto da invenção. O primeiro circuito integrado é configurado para operar com um segundo circuito integrado como uma parte interna de um dispositivo. De acordo ainda com outro aspecto da invenção é provido um segundo circuito integrado em linha com o primeiro aspecto da invenção. O segundo circuito integrado é configurado para operar com um primeiro circuito integrado como uma parte interna de um dispositivo.

As reivindicações dependentes se referem às modalidades da invenção. A matéria contida nas reivindicações dependentes relacionadas a um aspecto específico da invenção também é aplicável aos outros aspectos da invenção.

BREVE DESCRIÇÃO DOS DESENHOS

As modalidades da invenção serão descritas agora a título de exemplo com referência aos desenhos anexos nos quais:

A Figura 1 mostra a idéia de se ter duas zonas confiáveis separadas dentro de um dispositivo de acordo com uma modalidade da invenção;

A Figura 2 mostra um diagrama de blocos simplificado de um módulo de conjunto de telefone móvel de acordo com uma modalidade da invenção;

A Figura 3 mostra um procedimento de inicialização de acordo com uma modalidade da invenção; e

A Figura 4 mostra uma estação móvel de uma rede de comunicação celular de acordo com uma modalidade da invenção.

DESCRIÇÃO DETALHADA

Uma modalidade da invenção é projetada para permitir que um processador seguro armazene seguramente informação de estado em um símbolo de segurança interno. O termo símbolo de segurança interno significa aqui um símbolo de segurança interno significa um símbolo de segurança interno a um dispositivo ao contrário dos símbolos de segurança externos ao dispositivo (tal como cartões inteligentes removíveis) conhecidos a partir da técnica anterior. Contudo, embora o símbolo de segurança interno forme parte do dispositivo, isto é, ele é substancialmente insubstituível, o símbolo de segurança interno não é integrado ao processador seguro. Em outras palavras, essa modalidade da invenção apresenta um símbolo de segurança ou dispositivo de armazenagem que é interno (ao dispositivo), mas não integrado (ao processador seguro).

A Figura 1 mostra uma primeira zona confiável 101 limitada por um primeiro perímetro confiável 110. O processador seguro está situado dentro do primeiro perímetro confiável. A zona dentro do primeiro perímetro confiável é resistente à violação. O símbolo de segurança interno não está dentro do primeiro perímetro confiável, porém, uma segunda zona confiável 102, limitada por um segundo perímetro confiável 120, está disposta dentro do dispositivo e o símbolo de segurança interno é implementado nesse lugar. Além disso, a segunda zona confiável é resistente à violação.

A segunda zona confiável 102 é separada da primeira zona confiável 101. O processador seguro da primeira zona confiável se comunica com o símbolo de segurança interno por intermédio de um canal de comunicação 105 implementado entre a primeira zona confiável e a segunda zona confiável. Conseqüentemente, duas zonas confiáveis resistentes à violação, permanentes e separadas, unidas por um canal de comunicação, são implementadas no dispositivo.

Um exemplo de um processador seguro é um chip ASIC de banda base seguro em uma estação móvel, tal como um telefone móvel de uma rede celular. Um exemplo correspondente de um símbolo de segurança interno é um chip de circuito integrado (IC) separado, por exemplo, um chip de gerenciamento de energia. Um

exemplo do canal de comunicação é um barramento I^2C.

Dispositivos portáteis, de mão, tais como os telefones móveis são fabricados, tipicamente, mediante união de um conjunto de módulos de montagem. De acordo com uma implementação vantajosa, o chip (ou circuito) compreendendo o processador seguro, o canal de comunicação de interconexão e o chip separado (ou circuito) compreendendo o símbolo de segurança interno pertencem a um módulo de montagem comum. Eles podem ser implementados em uma placa de circuito comum. Alternativamente, eles podem pertencer a diferentes módulos de montagem, conectados juntos por intermédio do canal de comunicação.

A Figura 2 apresenta um diagrama simplificado de blocos de um módulo de montagem de telefone móvel 200 de acordo com uma modalidade da invenção. O módulo de montagem 200 é uma placa de circuito ou outra entidade integral compreendendo dois ou mais blocos IC. Os blocos IC são referidos aqui como chips IC integrados independente de se eles efetivamente contêm quaisquer chips de silício.

O módulo de montagem 200 compreende dois chips IC específicos: um ASIC primário 210 e um ASIC secundário 220, em que o ASIC secundário 220 provê o ASIC primário 210 com um símbolo de segurança. O ASIC primário 210 pode ser o ASIC de banda base seguro, um chip IC digital capaz de operação de freqüência de banda base, e o ASIC secundário pode ser o chip de gerenciamento de energia (também conhecido como EMC), um chip IC analógico capaz de gerenciamento de energia.

O ASIC primário 210 compreende um processador seguro 211, uma Memória de Acesso Aleatório, segura 212 tal como um cache de Camada 1 e uma memória de leitura não-volátil 213 (ROM). A ROM 213 contém parte do código de programa de computador 214 para controlar a operação do processador seguro 211 quando carregado após a inicialização do dispositivo. O ASIC primário 210 é conectado à outra memória não-volátil 216 por intermédio de um barramento de memória 215. A memória não-volátil 216 forma uma armazenagem protegida em uma zona não-segura (não resistente à violação) fora da primeira zona confiável.

Conseqüentemente, o processador seguro tem memória regravável, não-volátil apenas no lado externo da primeira zona confiável. O dispositivo de armazenagem protegido 216 é secreto porque sua informação é criptografada utilizando uma chave interna conhecida dentro do primeiro perímetro confiável. Contudo, o dispositivo de armazenagem, protegido, não tem proteção de integridade, uma vez que a informação contida na mesma pode ser substituída, pelo menos em princípio, por uma pessoa mal-intencionada, sofisticada.

O ASIC secundário 220 contém uma memória não-volátil regravável tal como uma memória flash. O ASIC secundário 220 compreende ainda lógica de acesso de memória flash 222 para acessar a memória flash, lógica de controle 221 para realizar comunicação com o ASIC primário 210, e um cripto bloco 224 acoplado à lógica de controle 221 para realizar primitivas criptográficas. Se o ASIC secundário 220 é o chip de gerenciamento de energia de um telefone celular, o ASIC secundário 220 compreende adicionalmente outros blocos apropriados para realizar funções normais de gerenciamento de energia. Essas funções envolvem controlar o fornecimento de energia para os componentes com uma voltagem superior àquela que pode ser controlada pelo circuito digital de um telefone celular típico. Os blocos lógicos 221 e 222 e o cripto bloco 224 podem ser implementados por hardware, software, ou uma combinação de hardware e software.

Deve ser considerado que não é necessário implementar o ASIC secundário 220 em um chip analógico. Ao contrário, um IC digital integrado no conjunto 200 com uma memória persistente regravável seria igualmente utilizável. Além disso, as modalidades da invenção são igualmente aplicáveis com blocos IC de outro tipo.

O ASIC primário 210 pode ser qualquer IC adequado capaz de executar código de programa de computador de modo que é difícil interferir em sua execução quando ele executa aplicações dentro do primeiro perímetro confiável 110, isto é, na primeira zona confiável resistente à violação 101. A zona confiável 101 contém os registradores necessários e áreas de memória que geralmente contêm dados seguros. O ASIC secundário 220 tem a segunda zona confiável 102 contendo os circuitos lógicos 221 e 222, o cripto bloco 224 e porções relevantes, senão todas,

da memória regravável, não-volátil ou persistente 223. O circuito lógico 222 provê vantajosamente o único – e controlado – acesso às porções relevantes da memória persistente 223. Nem toda a memória persistente 223 tem que estar dentro do perímetro seguro 120. Contudo, esse seria tipicamente o caso.

O circuito lógico de controle 221 é capaz de comunicações seguras com o processador seguro 211 por intermédio de meio criptográfico provido pelo cripto bloco 224. As comunicações seguras são conseguidas mediante proteção do canal de comunicação 105 criptograficamente através do uso de uma chave. A presente invenção provê o ASIC secundário com diferentes valores de estado de chave. Qual chave é usada para proteger o canal de comunicação depende do estado da chave atual no qual está o ASIC secundário 220. Dependendo do estado da chave é usada uma chave gravada em hardware K_H, uma chave de grupo K_G ou uma chave dedicada K_S. Deve ser observado, contudo, que embora as comunicações ocorrendo por intermédio do canal de comunicação 105 sejam seguras, o próprio canal de comunicação não está dentro de qualquer um dos perímetros confiáveis mencionados, porém está situado, nesse sentido, em uma zona não-protegida. O mesmo se aplica ao dispositivo de armazenagem, protegido 216.

O ASIC primário 210 e o ASIC secundário 220 são inicializados para trabalho em conjunto como um par seguro em um procedimento de inicialização. Durante a fabricação do chip, a chave gravada em hardware global K_H é codificada (ou gravada) dentro da lógica de controle 221 do ASIC secundário 220, e um identificador ID_S é atribuído ao chip. O identificador ID_S é um identificador singular identificando singularmente o ASIC secundário 220. Alternativamente, o identificador ID_S é um identificador de grupo. Em uma etapa subseqüente, a chave de grupo K_G é aplicada (ou gravada) no ASIC secundário. A chave de grupo é por definição uma chave específica para um grupo, por exemplo, um lote de chips. Quando a chave de grupo K_G é aplicada, o ASIC secundário é comutado a partir do estado de chave no qual ele utiliza a chave gravada em hardware K_H para criptografia ("estado de chave gravada em hardware") para o

estado de chave no qual a chave de grupo K_G é usada para criptografia ("estado de chave de grupo"). Vantajosamente, a configuração da chave de grupo K_G e a comutação relacionada a partir do "estado de chave gravada em hardware" para "estado de chave de grupo" é realizada quando o chip é fabricado.

A chave dedicada K_S é vantajosamente não aplicada ao ASIC secundário durante a fabricação do chip, porém, apenas posteriormente quando o módulo de montagem 200 é montado ou quando o dispositivo contendo o módulo de montagem 200 é montado em uma linha de montagem de fábrica de telefone. Essa parte da inicialização também pode ocorrer em um ponto de serviço.

A Figura 3 mostra um procedimento de inicialização de acordo com uma modalidade da invenção. O propósito do procedimento de inicialização da Figura 3 é o de atribuir uma chave compartilhada ou segredo, isto é, uma chave dedicada K_S ao processador seguro do ASIC primário 210 e ao seu símbolo de segurança, isto é, o ASIC secundário 220. Um servidor seguro 310 na linha de montagem atua como um servidor de distribuição de chave.

Na etapa S1 o ASIC primário 210 lê a informação de identificação do ASIC secundário 220. Como uma resposta (etapa S2) ele obtém o identificador ID_S do ASIC secundário 220.

Opcionalmente, o ASIC primário 210 também pode ler a informação de estado de chave atual a partir do ASIC secundário 220. Na etapa S3 o ASIC primário 210 solicita do servidor seguro 310 a chave dedicada K_S a ser compartilhada entre os ASICs 210 e 220. Essa solicitação contém vantajosamente o estado de chave do ASIC secundário 220, o identificador ID_S do ASIC secundário 220, e um identificador singular ID_P do ASIC primário 210. Opcionalmente, a solicitação pode ser autenticada utilizando-se uma chave K_P, uma chave secreta antecipadamente compartilhada entre o servidor de segurança 310 e o ASIC primário 210. Com base na informação recebida o servidor seguro 310 forma ou seleciona a chave dedicada K_S. O servidor seguro 310 pode ter um banco de dados no qual ele mantém informação relacionada a cada chave. Por exemplo, nesse caso o servidor seguro 310 pode vincular em conjunto os identificadores

ID_P e ID_S, o estado de chave do ASIC secundário 220 e a chave dedicada K_S. Na etapa S4, o servidor seguro 310 envia de volta uma resposta ao ASIC primário 210. A resposta compreende duas partes. A primeira parte é a carga útil para um comando GRAVAR CHAVE a ser emitido pelo ASIC primário 210 para o ASIC secundário 220. Ele compreende a chave dedicada K_S criptografada utilizando a chave K_G. A segunda parte compreende a chave dedicada K_S criptografada usando a chave K_P. Na etapa S5a chave dedicada é transferida e armazenada para a lógica do ASIC secundário 220 mediante emissão de um comando GRAVAR CHAVE com a primeira parte mencionada acima como a carga útil e o estado de chave do ASIC secundário 220 é atualizado conformemente para "estado de chave dedicada". Simultaneamente, o ASIC primário 210 também descriptografa a primeira parte e armazena a sua cópia de K_S em seu dispositivo de armazenagem, protegido 216. Na etapa S6, um código de sucesso ou falha é enviado ao ASIC primário 210 em retorno ao comando GRAVAR CHAVE. A chave K_S está agora pronta para ser usada.

Deve ser observado que embora o acima descreva o procedimento de inicialização para mudar o estado de chave do ASIC secundário 220 de modo que ele comuta de "estado de chave de grupo" para "estado de chave dedicada", um procedimento similar, opcionalmente, poderia ser usado para mudar o estado de chave do ASIC secundário 220 a partir de "estado de chave gravada em hardware" para "estado de chave de grupo". No que diz respeito à descrição acima, é apenas necessário substituir K_G por K_H e K_S por K_G. Todas as outras partes devem permanecer idênticas. Passar do estado de chave K_H para o estado de chave K_G é vantajosamente realizado no momento da fabricação do ASIC secundário. Porém, isso também pode ser feito na fábrica de telefone. O propósito de K_G (e analogamente K_H) é o de proteger a transferência de K_S (e analogamente K_G) para o ASIC secundário. A partir das chaves, apenas a chave K_H é gravada em hardware, as outras chaves não são gravadas em hardware, porém, simplesmente aplicadas pelo comando GRAVAR CHAVE.

Como mencionado na parte anterior, a chave compartilhada K_S é usada para

proteger a comunicação entre o ASIC primário 210 e o ASIC secundário 220. Conseqüentemente, em uma modalidade os comandos LER e GRAVAR, que pertencem a um protocolo a ser usado entre os ASICs, e os quais são usados para LER e GRAVAR informação de estado, segura (tal como informação ligada a um contador de tentativa de acesso ao PIN monotonicamente crescente) na memória persistente 223 do ASIC secundário 220, são protegidos por intermédio de algoritmos criptográficos de chave simétrica, tal como o algoritmo BES simétrico, utilizando DES simétrico, utilizando a chave dedicada K_S. Caso contrário o cenário básico de utilização dos comandos LER ou GRAVAR corresponde àquele apresentado na *US 2003/0079122 A1*. O ASIC primário 210 envia comandos de protocolo para o ASIC secundário 220 e o ASIC secundário 220 responde ao ASIC primário 210 mediante envio de resposta aos comandos.

Os dados que devem ter proteção de integridade são codificados e armazenados no dispositivo de armazenagem, protegido, não-volátil 216 pelo processador seguro 211 utilizando K_S. Esses dados ou suas partes cruciais são criptografados e armazenados também na memória 223 do ASIC secundário 220 utilizando K_S. Quando a energia é ligada, o processador seguro 211 compara os conteúdos dessas memórias. Se, por exemplo, o dispositivo de armazenagem 216 tiver sido violado, isso será percebido ao se comparar os componentes.

A seguir, são discutidos problemas de implementação, específicos.

Em primeiro lugar, as operações de gravar (GRAVAR ou CHAVE GRAVAR) não são atômicas. É possível que uma operação de gravação falhe. Uma operação de gravação que falhou pode fazer com que o ASIC secundário chegue a um estado de chave indeterminístico. Nesse caso, o ASIC secundário, por exemplo, não saberia qual chave utilizar. Para aliviar esse problema, de acordo com uma modalidade da invenção, pelo menos dois locais separados de memória (em vez de um) no símbolo de segurança interno, são usados para monitorar seu estado de chave indicando qual chave está sendo usada. Esses locais de memória contêm uma variável de estado de chave indicando o estado de chave ou a chave em uso. Em uma modalidade, redundância é adicionada a cada variável de estado

de chave. A redundância é adicionada mediante apresentação do valor de uma variável de estado de chave pelo menos parcialmente na forma de um valor mágico, um valor substancialmente mais longo do que o valor "real". Se a variável de estado de chave tem qualquer valor diferente do valor mágico, o dispositivo é arranjado para retornar ao uso de uma chave de nível de segurança mais segura (por exemplo, continuar a usar K_G se o processo de atualizar o estado de chave a partir de "estado de chave de grupo" para "estado de chave dedicada" tiver encontrado uma falha de GRAVAR). Outra modalidade provê meios para confirmar se uma operação de GRAVAR foi ou não bem-sucedida. Nessa modalidade, após emitir um comando GRAVAR, qualquer número de comandos GRAVAR é emitido para verificar o resultado do comando GRAVAR.

Em segundo lugar, com a finalidade de remoção de erros, deve ser possível reinicializar o símbolo de segurança interno mediante retorno do mesmo a um estado conhecido de tal modo que um dispositivo de teste externo pode ler e gravar os dados no mesmo. Naturalmente, isso deve ser possível sem danificar a segurança do sistema em operação normal. Para conseguir isso, em uma modalidade, uma operação de reinicialização é arranjada de tal modo que ela primeiramente zera uma variável de estado de chave e então apaga as chaves armazenadas e no símbolo de segurança interno de modo que o dispositivo é forçado a usar a chave gravada em hardware (ou absolutamente nenhuma). Em uma modalidade, o símbolo de segurança interno é arranjado de modo que sempre que o dispositivo for ligado, se essa variável de estado de chave não for o valor mágico, as chaves são apagadas.

Em terceiro lugar, se o símbolo de segurança interno não tem fonte de aleatoriedade dentro do símbolo de segurança interno, isso pode causar dificuldades no que diz respeito aos ataques de reprodução. Como descrito anteriormente, as comunicações entre o processador seguro e o símbolo de segurança interno são criptografadas e protegidas em termos de integridade. A ausência de fonte de aleatoriedade é discutida a seguir separadamente para operações de ler e gravar:

- operações de leitura: o símbolo de segurança interno não precisa necessariamente realizar detecção de reprodução, uma vez que o processador seguro pode realizar isso mediante inclusão de um desígnio de momento no comando LER.

- operações de gravação: detecção de reprodução seria apropriada para impedir ataques de reprodução. Em uma modalidade, o ASIC secundário verifica se, além de um novo valor, o comando GRAVAR recebido também inclui o valor atual armazenado no local de memória alvo (ou, em outras modalidades, também valores em outros locais de memória, ou o resultado de aplicar uma função mutuamente conhecida aos valores em alguns locais de memória). Caso contrário a operação GRAVAR não é permitida. Isso garante uma forma limitada de proteção contra reprodução: desde que a seqüência de valores armazenada no local de memória não tenha loops, a pessoa mal-intencionada não pode atacar o sistema mediante reprodução de um comando GRAVAR antigo. Em outra modalidade, para reduzir as possibilidades de uma pessoa mal-intencionada determinar se um local de memória mudou mediante reprodução de um comando LER, o ASIC secundário é provido com um registrador de deslocamento de retorno linear (LFSR) e alguns bits a partir do LFSR são adicionados a uma resposta. O LFSR é inicializado utilizando o conteúdo de um ou mais locais de memória, e é acionado por um relógio.

Desse modo, é garantido para os comandos LER e GRAVAR que um observador do canal de comunicação 105 não pode facilmente determinar quais foram os parâmetros comunicados, ou qual foi o efeito.

Em quarto lugar, processamento criptográfico nos ASICs é implementado utilizando primitivas criptográficas básicas. Se o ASIC secundário foi limitado em termos de recursos, o protocolo de comunicação seguro entre os ASICs deve ser projetado de tal modo que todo o processamento criptográfico necessário no ASIC secundário possa ser feito utilizando o menor número possível de primitivas criptográficas, mas ainda preservando as propriedades exigidas do protocolo como confidencialidade e integridade da mensagem. Isso pode ser conseguido, por

exemplo, conforme a seguir, utilizando um algoritmo de criptografia simétrica adequado como o AES (Padrão de Criptografia Avançado), DES (Padrão de Criptografia de Dados), ou DES tríplice. O algoritmo de criptografia simétrico consiste em uma transformação direta (normalmente usada para criptografia) e uma transformação reversa (normalmente usada para descriptografia).

Para as mensagens geradas no ASIC primário e enviadas para o ASIC secundário:

- a confidencialidade é obtida mediante uso da transformação direta como a operação básica no modo de Encadeamento de Blocos Cifrados (CBC); e
- a integridade é conseguida mediante uso de MAC de CBC (código de autenticação de mensagem), mas utilizando transformação reversa como a operação básica no modo CBC.

O modo CBC é um modo de operação geralmente conhecido daqueles versados na técnica e discutido mais adequadamente, por exemplo, no livro *"Handbook of Applied Cryptography"* de Alfred J. Menezes et al., ISBN: 0-8493-8523-7, Quinta Edição, agosto de 2001.

Para as mensagens geradas no ASIC secundário e enviadas a partir do ASIC secundário:

- a confidencialidade é obtida mediante uso da transformação reversa; e
- a integridade é obtida mediante uso de MAC de CBC com a transformação reversa como a operação básica.

Desse modo, o ASIC secundário precisa apenas implementar a transformação reversa da primitiva de criptografia simétrica. O ASIC primário precisa implementar ambas, a transformação direta e a transformação reversa.

Quando o algoritmo de criptografia simétrica é DES tríplice, então três transformações reversas do algoritmo DES básico são usadas em seqüência no ASIC secundário. Desse modo, o ASIC secundário precisa implementar apenas a transformação reversa de DES.

Se a mensagem enviada a partir do ASIC secundário tem apenas o tamanho de um bloco de comprimento, então nenhum encadeamento é necessário.

A Figura 4 mostra uma ilustração muito simplificada de uma estação móvel de uma rede de comunicação celular de acordo com uma modalidade da invenção. A estação móvel 400 compreende, além do ASIC de banda base seguro 210, o chip de gerenciamento de energia 220 e o barramento I^2C 105, uma interface de usuário 410 e uma parte de radiofreqüência (RF) 420. A interface de usuário 410 e a parte de radiofreqüência 420 são acopladas ao ASIC de banda base 210. A interface de usuário compreende um teclado e vídeo para uso do dispositivo. O teclado pode ser usado, por exemplo, para introduzir um PIN no dispositivo. De acordo com as tentativas de PIN, o ASIC de banda base seguro 210 mantém informação de estado (aqui: o número de tentativas de PIN mal-sucedidas) na memória não-volátil do chip de gerenciamento de energia 220. A parte de RF é usada para comunicação sem fio de radiofreqüência com a rede sem fio 430.

Implementações e modalidades específicas da invenção foram descritas. É evidente para aqueles versados na técnica que a invenção não é limitada aos detalhes das modalidades apresentadas acima, mas que ela pode ser implementada em outras modalidades utilizando meios equivalentes sem se desviar das características da invenção. Algumas características foram descritas como parte de exemplos no anteriormente apresentado e sempre que tecnicamente possível, as características devem ser consideradas como opcionais e combináveis com quaisquer outros exemplos diferentes da descrição. Por exemplo, a invenção é útil também em vários dispositivos eletrônicos, particularmente, em livros eletrônicos portáteis, dispositivos PDA, dispositivos de jogos, tocadores de música, conversores de sinal de freqüência habilitados para DRM capazes de prover acesso limitado a (alugado) conteúdo e dispositivos de posicionamento GPS. Portanto, o escopo da invenção limita-se apenas às reivindicações de patente, anexas.

REIVINDICAÇÕES

1. Dispositivo **CARACTERIZADO** pelo fato de que compreende:

- um primeiro circuito integrado para formar a primeira zona confiável, o primeiro circuito integrado compreendendo um processador seguro;

- um segundo circuito integrado separado do primeiro circuito integrado para forma a segunda zona confiável, o segundo circuito integrado compreendendo um dispositivo de armazenagem não-volátil seguro dentro da segunda zona confiável,

- onde o processador é configurado para comunicar a informação da primeira zona confiável para a segunda zona confiável de maneira segura para a informação segura ser armazenada seguramente em um dispositivo de armazenagem não-volátil seguro;

- o segundo circuito integrado é configurado para comunicar a informação armazenada no seu dispositivo de armazenagem não-volátil seguro da segunda zona confiável para o processador seguro dentro da primeira zona confiável de maneira segura, e

- onde o primeiro circuito integrado e o segundo circuito integrado são partes internas do dispositivo.

2. Dispositivo de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o primeiro e o segundo circuitos integrados são adaptados para inicializar seguramente uma única chave segura a ser compartilhada entre a primeira e a segunda zonas confiáveis.

3. Dispositivo de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que o primeiro circuito integrado é adaptado para compartilhar a chave com o servidor de distribuição de chave seguro e o segundo circuito integrado é adaptado para compartilhar outra chave com o servidor de distribuição de chave seguro para entrega segura da chave segura única do servidor de distribuição de chave seguro para o primeiro e o segundo circuitos integrados.

4. Dispositivo de acordo com as reivindicações 1 a 3, **CARACTERIZADO** pelo fato de que o primeiro e o segundo circuitos são

adaptados para estabelecer um protocolo de comunicação seguro a ser usado entre a primeira e a segunda zonas confiáveis.

5. Dispositivo de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o protocolo de comunicação seguro compreende algoritmos criptográficos a serem executados ao usar uma única chave segura para as comunicações seguras entre a primeira e a segunda zonas confiáveis.

6. Dispositivo de acordo com a reivindicação 4 ou 5, **CARACTERIZADO** pelo fato de que o protocolo contêm aos menos os comandos LER e ESCREVER e as operações de mudança de chave.

7. Dispositivo de acordo com as reivindicações 1 a 6, **CARACTERIZADO** pelo fato de que o dispositivo é provido com o gerenciamento de estado da chave permitindo mais de uma chave ser compartilhada entre a primeira e a segunda zonas confiáveis.

8. Dispositivo de acordo com a reivindicação 7, **CARACTERIZADO** pelo fato de que o dispositivo de armazenagem não-volátil da segunda zona confiável compreende ao menos um estado da chave mantido variável indicando que a chave compartilhada será usada na comunicação.

9. Dispositivo de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que o segundo circuito integrado é adaptado para escolher um estado de chave correto ao ler o valor atual do estado da chave variável na operação de energização.

10. Dispositivo de acordo com as reivindicações 1 a 6, **CARACTERIZADO** pelo fato de que o processador seguro é adaptado para incluir um valor randômico como parâmetro no comando LER, de forma que este possa verificar que o resultado subseqüente recebido do segundo circuito integrado é recente (não reproduzido).

11. Dispositivo de acordo com as reivindicações 1 a 6, 10, **CARACTERIZADO** pelo fato de que o segundo circuito integrado é adaptado para verificar se o valor antigo de uma célula de memória alvo do seu dispositivo de armazenagem não-volátil seguro está contido como um parâmetro no comando

ESCREVER recebido, e permite a operação de escrita apenas se for este o caso.

12. Dispositivo de acordo com as reivindicações 1 a 11, **CARACTERIZADO** pelo fato de que o segundo circuito integrado é configurado para cifrar os parâmetros de uma resposta a um comando recebido ao usar a chave segura única, e ao incluir um componente externamente imprevisível nos parâmetros, de forma que o mesmo comando resultará em diferentes respostas.

13. Dispositivo de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que o componente imprevisível é um valor derivado do registro de deslocamento de realimentação linear acionado por relógio.

14. Dispositivo de acordo com as reivindicações 1 a 13, **CARACTERIZADO** pelo fato de que o segundo circuito integrado é adaptado para usar apenas um único primitivo criptográfico para toda a sua operação criptográfica.

15. Dispositivo de acordo com as reivindicações 1 a 14, **CARACTERIZADO** pelo fato de que o primeiro circuito integrado é digital e o segundo circuito integrado é analógico.

16. Dispositivo de acordo com as reivindicações 1 a 15, **CARACTERIZADO** pelo fato de que o segundo circuito reside no chip de gerenciamento de energia do telefone móvel.

17. Dispositivo de acordo com as reivindicações 1 a 16, **CARACTERIZADO** pelo fato de que o primeiro circuito e o segundo circuito formam parte de um módulo de montagem.

18. Dispositivo de acordo com as reivindicações 1 a 17, **CARACTERIZADO** pelo fato de que a informação segura compreende a informação indicando o estado do dispositivo.

19. Dispositivo de acordo com as reivindicações 1 a 18, **CARACTERIZADO** pelo fato de que o dispositivo compreende uma segunda memória não-volátil para armazenar a informação segura e cifrar esta ao usar a chave.

20. Dispositivo de acordo com a reivindicação 19, **CARACTERIZADO**

pelo fato de que o dispositivo é disposto para comparar os conteúdos da segunda memória não-volátil com os conteúdos do dispositivo de armazenagem não-volátil da segunda zona confiável.

21. Dispositivo de acordo com as reivindicações 1 a 20, **CARACTERIZADO** pelo fato de que o dispositivo é um dispositivo de comunicação portátil, tal como um telefone móvel.

22. Método para inicializar uma chave segura a ser compartilhada entre o primeiro circuito integrado e o segundo circuito integrado, o método é **CARACTERIZADO** pelo fato de que compreende:

- distribuir a chave segura a ser compartilhada entre o primeiro circuito integrado e o segundo circuito integrado do servidor de distribuição de chave seguro para o primeiro e segundo circuitos integrados, onde o método compreende:

- proteger a distribuição da chave segura do servidor de distribuição de chave segura para o primeiro circuito integrado usando a primeira chave, a primeira chave sendo uma chave compartilhada anteriormente entre o primeiro circuito integrado e o servidor de distribuição de chave seguro;

- proteger a distribuição da chave segura do servidor de distribuição de chave segura para o segundo circuito integrado usando a segunda chave, a segunda chave sendo uma chave compartilhada anteriormente entre o segundo circuito integrado e o servidor de distribuição de chave seguro.

23. Circuito integrado **CARACTERIZADO** pelo fato de que compreende:

- um processador seguro para emitir e cifrar os comandos a serem transferidos para outro circuito integrado de acordo com o protocolo seguro, onde

- o protocolo seguro compreende uma operação de mudança de chave pela qual a chave segura compartilhada entre o circuito integrado e o outro circuito integrado pode ser alterada.

24. Programa de computador executável pelo processador seguro do circuito integrado, o programa é **CARACTERIZADO** pelo fato de que compreende:

- um código de programa para emitir os comandos a serem transferidos para outro circuito integrado de acordo com o protocolo seguro, onde

- um código de programa para ocasionar ao processador seguro para iniciar a operação de mudança de chave pela qual a chave segura compartilhada entre o circuito integrado e o outro circuito integrado é alterada.

25. Circuito integrado **CARACTERIZADO** pelo fato de que compreende:

- uma memória não-volátil para armazenar os dados seguros recebidos de outro circuito integrado;

- lógicas para acessar a memória não volátil, onde o circuito integrado é adaptado para comunicar os dados seguros armazenados na memória não-volátil e seguras por meio de criptografia para outro circuito integrado, e

- onde o circuito integrado é configurado para usar um único primitivo criptográfico.

26. Programa de computador executável em um circuito integrado, o programa é **CARACTERIZADO** pelo fato de que compreende:

- código de programa para assegurar as comunicações com outro circuito integrado ao usar uma chave compartilhada entre o circuito integrado e outro circuito integrado; e

- código de programa para mudar entre diferentes mudanças de chave de diferentes níveis de segurança.

27. Chip de gerenciamento de energia adaptado para executar o gerenciamento de energia do dispositivo, o chip de gerenciamento de energia é **CARACTERIZADO** pelo fato de que compreende uma memória não-volátil segura e lógicas, para prover um símbolo de segurança para um processador seguro externo ao chip de gerenciamento de energia.

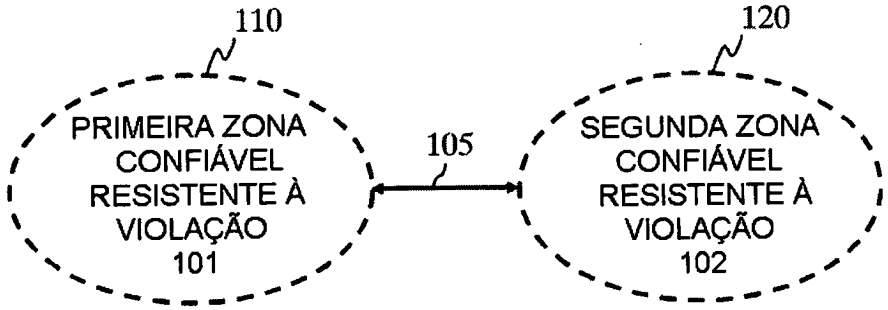

110
120
PRIMEIRA ZONA CONFIÁVEL RESISTENTE À VIOLAÇÃO 101
105
SEGUNDA ZONA CONFIÁVEL RESISTENTE À VIOLAÇÃO 102

Fig. 1

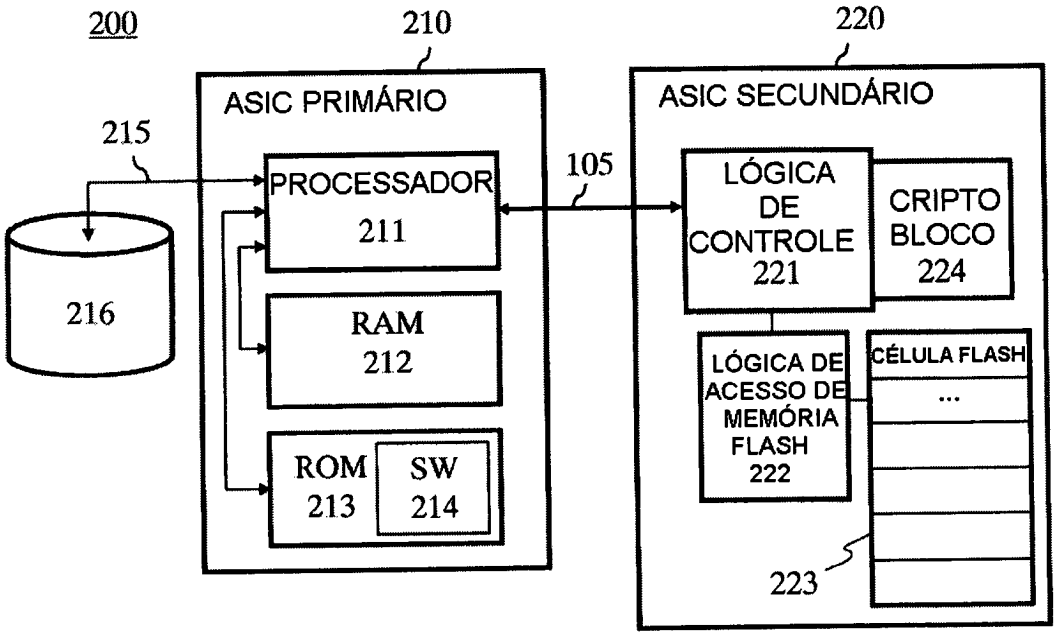

200
210
220
ASIC PRIMÁRIO
ASIC SECUNDÁRIO
215
PROCESSADOR 211
105
LÓGICA DE CONTROLE 221
CRIPTO BLOCO 224
216
RAM 212
LÓGICA DE ACESSO DE MEMÓRIA FLASH 222
CÉLULA FLASH
...
ROM 213
SW 214
223

Fig. 2

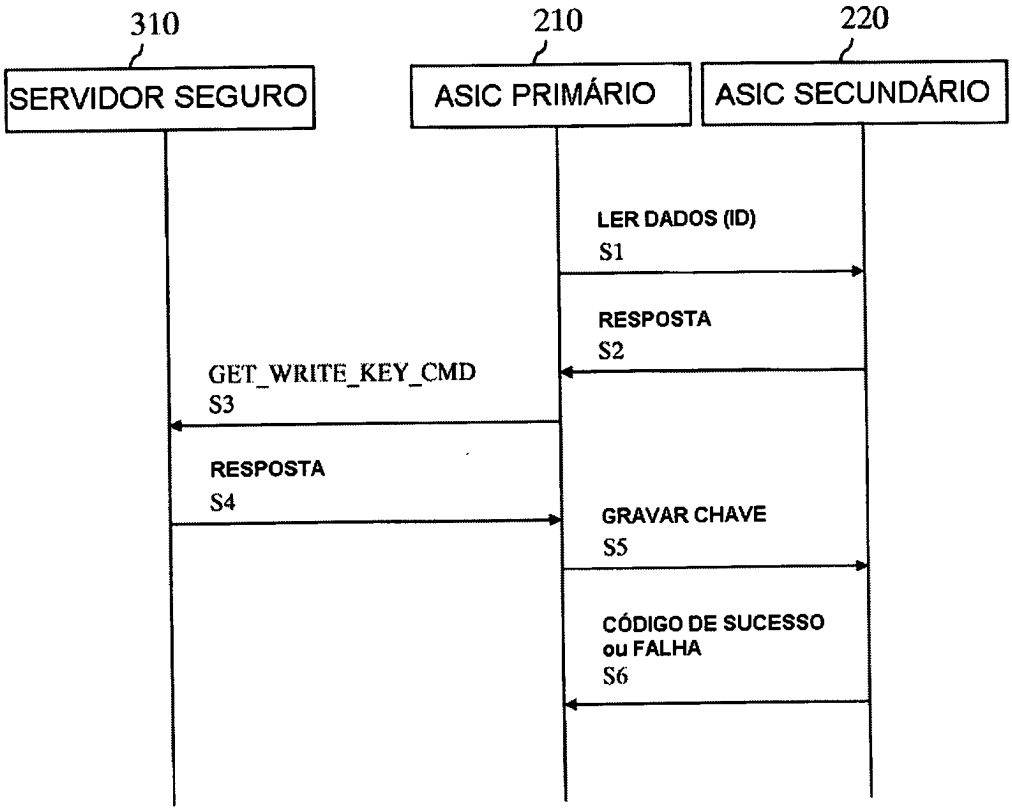

310
210
220
SERVIDOR SEGURO
ASIC PRIMÁRIO
ASIC SECUNDÁRIO
LER DADOS (ID)
S1
RESPOSTA
S2
GET_WRITE_KEY_CMD
S3
RESPOSTA
S4
GRAVAR CHAVE
S5
CÓDIGO DE SUCESSO
ou FALHA
S6

Fig. 3

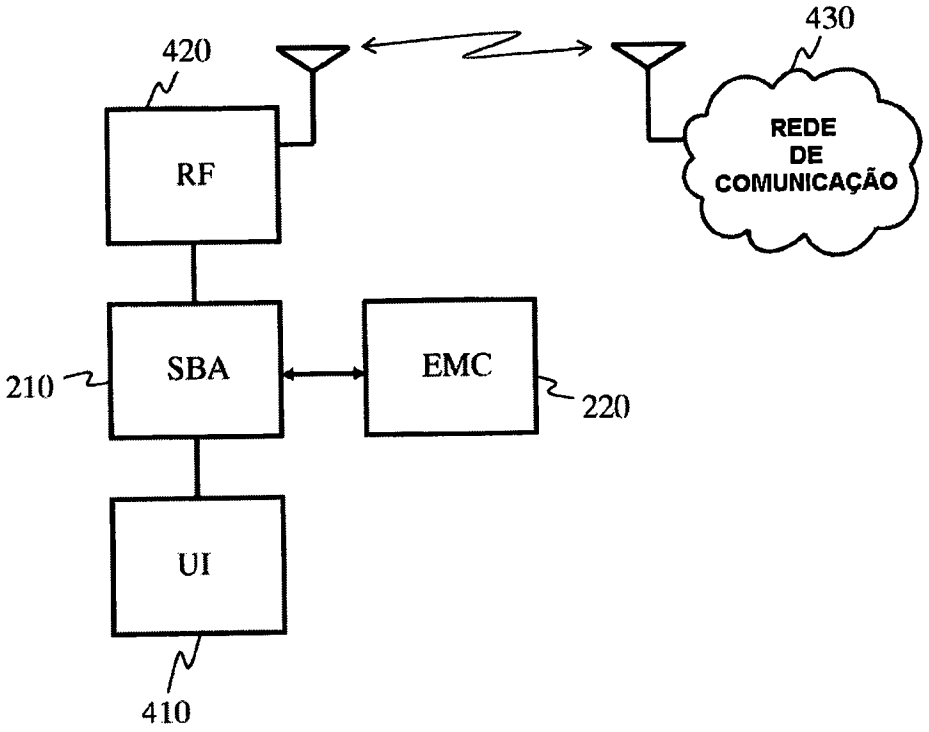


Fig. 4

 PI0612024-5

RESUMO

"DISPOSITIVO, MÉTODO PARA INICIALIZAR UMA CHAVE SEGURA A SER COMPARTILHADA ENTRE O PRIMEIRO CIRCUITO INTEGRADO E O SEGUNDO CIRCUITO INTEGRADO, CIRCUITO INTEGRADO, PROGRAMA DE COMPUTADOR EXECUTADO EM UM CIRCUITO INTEGRADO, E, CHIP DE GERENCIAMENTO DE ENERGIA ADAPTADO PARA EXECUTAR O GERENCIAMENTO DE ENERGIA DO DISPOSITIVO."

Um símbolo de segurança interno mas não integrado é fornecido para o dispositivo, que compreende um primeiro circuito integrado compreendendo um processador seguro. O símbolo de segurança é fornecido pelo segundo circuito integrado separado do primeiro circuito integrado. O segundo circuito integrado compreende um dispositivo de armazenagem não-volátil seguro. O processador seguro comunica a informação para o segundo circuito de maneira segura para a informação segura ser armazenada seguramente em um dispositivo de armazenagem não-volátil seguro, e o segundo circuito integrado comunica a informação armazenada em um dispositivo de armazenagem não-volátil seguro para o processador seguro de maneira segura. As comunicações são asseguradas por meio de criptografia. O primeiro circuito integrado e o segundo circuito integrado são partes internas do dispositivo. Um método de utilização para distribuir a chave segura a ser compartilhada entre os circuitos e a ser usado na criptografia é também descrito.