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

(21) PI 0718581-2 A2

* B R P I 0 7 1 8 5 8 1 A 2 *

(22) Data de Depósito: 07/11/2007
(43) Data da Publicação: 11/03/2014
(RPI 2253)

(51) Int.Cl.:
H04L 9/08

(54) Título: SISTEMAS E MÉTODOS PARA DISTRIBUIR E PROTEGER DADOS

(57) Resumo:

(30) Prioridade Unionista: 07/11/2006 US 60/857,345

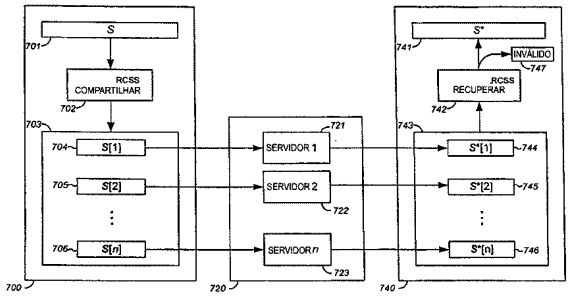
(73) Titular(es): Security First Corporation

(72) Inventor(es): Mihir Bellare, Philip Rogaway

(74) Procurador(es): Dannemann ,Siemsen, Bigler & Ipanema Moreira

(86) Pedido Internacional: PCT US2007023626 de 07/11/2007

(87) Publicação Internacional: WO 2008/127309de 23/10/2008



Relatório Descritivo da Patente de Invenção para **"SISTEMAS E MÉTODOS PARA DISTRIBUIR E PROTEGER DADOS".**

REFERÊNCIA CRUZADA A PEDIDOS RELACIONADO

Este pedido reivindica o benefício do Pedido Provisório U.S. Número 60/857.345, depositado em 07 de Novembro de 2006, o qual está por meio disto aqui incorporado por referência na sua totalidade.

CAMPO DA INVENÇÃO

A presente invenção refere-se em geral a um sistema para proteger dados de um acesso ou uso não-autorizado. A presente invenção também refere-se geralmente a técnicas criptográficas para a construção de esquemas de compartilhamento de segredo, e mais especificamente a sistemas e métodos para suportar um esquema de compartilhamento de segredo que pode tolerar danos a um ou mais compartilhamentos.

ANTECEDENTES DA INVENÇÃO

Na sociedade atual, os indivíduos e as empresas conduzem uma quantidade de atividades cada vez mais crescente em e por sistemas de computador. Estes sistemas de computador, que incluem redes de computador de propriedade e de não-propriedade, estão frequentemente armazenando, arquivando, e transmitindo todos os tipos de informações reservadas. Assim uma necessidade cada vez mais crescente existe para assegurar que os dados armazenados e transmitidos por estes sistemas não possam ser lidos ou de outro modo comprometidos.

Uma solução comum para proteger os sistemas de computador é prover uma funcionalidade de login e senha. No entanto, o gerenciamento de senhas provou ser bastante dispendioso com uma grande percentagem de chamadas a apoios do usuário relativas a problemas com senhas. Mais ainda, as senhas proveem pouca segurança pelo fato de que estas estão geralmente armazenadas em um arquivo susceptível a acesso impróprio, através de, por exemplo, ataques de força bruta.

Outra solução para proteger os sistemas de computador é prover infraestruturas criptográficas. A criptografia, em geral, refere-se a proteger os dados transformando-os, ou criptografando-os em um formato ilegí-

vel. Somente aqueles que possuem a(s) chave(s) para a criptografia podem decifrar os dados para um formato utilizável. A criptografia é utilizada para identificar os usuários, por exemplo, autenticação, para permitir acesso a privilégios, por exemplo, autorização, para criar certificados e assinaturas digitais, e similares. Um sistema de criptografia popular é um sistema de chave pública que utiliza duas chaves, uma chave pública conhecida de todos e uma chave privada conhecida somente de seu proprietário individual ou comercial. Geralmente, os dados criptografados com uma chave são decifrados com a outra e nenhuma chave é recriável da outra.

Infelizmente, mesmo os sistemas criptográficos de chave pública típicos acima são altamente dependentes do usuário para segurança. Por exemplo, os sistemas criptográficos emitem a chave provada para o usuário, por exemplo, através do navegador do usuário. Os usuários não-sofisticados então geralmente armazenam a chave provada em um disco rígido acessível a outros através de um sistema de computador aberto, tal como, por exemplo, a Internet. Por outro lado, os usuários podem escolher nomes ruins para os arquivos que contém a sua chave privada, tal como, por exemplo, "chave". O resultado do acima e outros atos é permitir que a chave ou chaves sejam susceptíveis de comprometimento.

Além dos comprometimentos acima, um usuário pode salvar a sua chave privada em um sistema de computador configurado com um sistema de arquivamento ou de backup, potencialmente resultando em cópias da chave privada deslocando-se através de múltiplos dispositivos de armazenamento de computador ou outros sistemas. Esta brecha de segurança é frequentemente referida como "migração de chave". Similar à migração de chave, muitos aplicativos proveem acesso á chave privada de um usuário através de, no máximo, um simples acesso de login e senha. Como acima mencionado, o acesso de login e senha frequentemente não provê uma segurança adequada.

Uma solução para aumentar a segurança dos sistemas de criptografia acima é incluir a biometria como parte da autenticação ou autorização. A biometria geralmente inclui características físicas mensuráveis, tais

como, por exemplo, impressões digitais ou voz que podem ser verificadas por um sistema automatizado, tal como, por exemplo, uma coincidência de padrões ou um reconhecimento de padrões de impressão digital ou de voz. Em tais sistemas a biometria e/ou as chaves de um usuário podem ser armazenadas em dispositivos de computação móveis, tais como, por exemplo, um cartão inteligente, um laptop, um assistente digital pessoal, ou telefone móvel, por meio disto permitindo que a biometria ou as chaves sejam utilizáveis em um ambiente móvel.

O sistema criptográfico biométrico móvel acima ainda sofre de uma variedade de desvantagens. Por exemplo, o usuário móvel pode perder ou quebrar o cartão inteligente ou dispositivo de computação portátil, por meio disto tendo o seu acesso a dados potencialmente importantes inteiramente cortado. Alternativamente, uma pessoa maliciosa pode roubar o cartão inteligente ou o dispositivo de computação portátil do usuário móvel e utilizá-lo para eficazmente roubar as credenciais digitais do usuário móvel. Por outro lado, o dispositivo de computação portátil pode ser conectado a um sistema aberto, tal como a Internet, e, como as senhas, o arquivo onde a biometria está armazenada pode ser susceptível a comprometimento através da falta de atenção do usuário à segurança e invasores maliciosos.

Um modo de proteger os dados de um acesso não-autorizado ou de utilização não-autorizada é utilizar um esquema de compartilhamento de segredo. Um esquema de compartilhamento de segredo é um método para dividir uma porção de dados reservados (por exemplo, arquivos confidenciais, uma chave de criptografia, ou qualquer tipo de comunicação), algumas vezes denominados o segredo, em uma coleção de porções, denominadas compartilhamentos, de modo que a possessão de um número suficiente de compartilhamentos permite a recuperação do segredo, mas a possessão de um número insuficiente de compartilhamentos provê pouca ou nenhuma informação sobre o segredo que foi compartilhado. Tais esquemas são importantes ferramentas em criptografia e segurança de informações.

Formalmente, um esquema de compartilhamento de segredo consiste em um par de algoritmos, o algoritmo de compartilhamento Share e

o algoritmo de recuperação Recover. O algoritmo de compartilhamento é tipicamente probabilístico (significando que este faz escolhas randomizadas), e o algoritmo de recuperação é tipicamente determinístico. O algoritmo de compartilhamento pode ser utilizado para desmontar, ou dividir, o segredo em uma coleção de compartilhamentos, e o algoritmo de recuperação pode ser utilizado para remontar estes compartilhamentos. No momento da remontagem, cada compartilhamento pode estar presente, em cujo caso uma cadeia pode ser provida para o algoritmo de recuperação, ou um compartilhamento pode estar faltando, em cujo caso um valor designado (referido como "0" aqui) pode ser provido para o algoritmo de recuperação. Um conjunto de participantes que esta autorizado a recuperar o segredo é denominado um conjunto autorizado, e o conjunto de todos tais participantes é algumas vezes denominado uma estrutura de acesso.

Os esquemas de compartilhamento de segredo foram projetados para funcionar em várias estruturas de acesso, mas a estrutura de acesso mais comum é a estrutura de acesso limite, onde qualquer subconjunto de m ou mais participantes, de um total de n participantes no todo, são ditos serem autorizados. Um esquema de compartilhamento de segredo para uma estrutura de acesso limite é algumas vezes denominado um esquema de limite. Existem duas propriedades de segurança para qualquer esquema de compartilhamento de segredo: uma propriedade de privacidade e uma propriedade de recuperabilidade. A propriedade de privacidade assegura que coalizões não-autorizadas de participantes não aprendam nada útil sobre o segredo. A propriedade de recuperabilidade assegura que as coalizões de participantes autorizadas possam no final recuperar o segredo subjacente.

O esquema de compartilhamento de segredo de Shamir é dito ser o esquema de compartilhamento de segredo perfeito (PSS). O termo "perfeito" refere-se à garantia de privacidade sendo informações teóricas e sem nenhum erro; assim, as coalizões de participantes não-autorizadas não podem aprender nada útil sobre o segredo subjacente nos esquemas de PSS.

Uma limitação com os esquemas de PSS é que o tamanho de

cada compartilhamento deve ser pelo menos tão longo quanto o tamanho do segredo que está sendo compartilhado. Quando o segredo inclui um grande arquivo ou uma longa cadeia de caracteres, no entanto, esta limitação pode tornar-se de difícil controle, aumentando a complexidade total do sistema. Em resposta a esta limitação, esquemas para o compartilhamento de segredos computacionais (CSS) foram desenvolvidos.

O esquema de CSS de Krawczyk, por exemplo, permite que os compartilhamentos sejam mais curtos do que o segredo. Por exemplo, em um esquema de limite de 2 de 3 (significando que quaisquer dois de três compartilhamentos são adequados para recuperar o segredo), o segredo S pode ser dividido em compartilhamentos de tamanho aproximadamente |S|/2 bits, onde |S| denota o comprimento de S. Os compartilhamentos não são possíveis no ambiente de PSS. Os esquemas de CSS, no entanto, a propriedade de privacidade pode não mais ser absoluta e as informações teóricas; ao contrário, uma coalizão de participantes não-autorizada pode obter uma pequena quantidade de informações sobre o segredo compartilhado de seus compartilhamentos. Mas, sob uma suposição de complexidade computacional, a quantidade de informações será insignificante e portanto, na prática, não muito preocupante.

Uma segunda limitação do esquema de PSS refere-se à falta de robustez delegada. Robustez significa que um participante faltoso ou adversário é incapaz de forçar a recuperação de um segredo incorreto. O modelo para PSS assume que cada compartilhamento é ou "correto" ou "faltante", mas este nunca pode estar errado (por exemplo, corrompido ou intencionalmente alterado). Na prática, esta é uma suposição altamente irracional porque os compartilhamentos podem estar errados devido a qualquer número de fatores, que incluem, por exemplo, erros em armazenamento, ruído em um canal de comunicação, ou devido a atividades genuinamente adversárias. Além disso, a falta de robustez não é apenas uma possibilidade teórica, mas um problema genuíno para os esquemas de PSS típicos, incluindo o esquema de compartilhamento de segredo de Shamir. Com o esquema de Shamir, um adversário pode de fato forçar a recuperação de qualquer se-

gredo desejado mudando apropriadamente apenas um compartilhamento. As aplicações práticas de esquemas de compartilhamento de segredo tipicamente requerem robustez.

SUMÁRIO DA INVENÇÃO

Com base no acima, esquemas de compartilhamento de segredo computacionais robustos que sejam simultaneamente eficientes e tenham fortes propriedades de segurança provável sob fracas suposições criptográficas são necessários.

Consequentemente, um aspecto da presente invenção é prover um método para proteger virtualmente qualquer tipo de dados de acesso ou uso não-autorizado. O método compreende uma ou mais etapas de decompor, dividir e/ou separar os dados a serem protegidos em duas ou mais partes ou porções. O método também compreende criptografar os dados a serem protegidos. A criptografia dos dados pode ser executada antes ou após a primeira decomposição, divisão e/ou separação dos dados. Além disso, a etapa de criptografar pode ser repetida para uma ou mais porções dos dados. Similarmente, as etapas de decompor, dividir e/ou separar podem ser repetidas para uma ou mais porções dos dados. O método também opcionalmente compreende armazenar os dados decompostos, divididos e/ou separados que foram criptografados em uma localização ou em múltiplas localizações. Este método também opcionalmente compreende reconstituir ou remontar os dados protegidos em sua forma original para um acesso ou uso autorizado. Este método pode ser incorporado nas operações de qualquer computador, servidor, máquina ou similar, que seja capaz de executar as etapas desejadas do método.

Outro aspecto da presente invenção provê um sistema para proteger virtualmente qualquer tipo de dados de acesso ou uso não-autorizado. Este sistema compreende um módulo de divisão de dados, um módulo de manipulação criptográfica, e, opcionalmente, um módulo de montagem de dados. O sistema pode, em uma modalidade, ainda compreender uma ou mais instalações de armazenamento de dados onde os dados protegidos podem ser armazenados.

Outro aspecto da invenção inclui utilizar qualquer algoritmo de decomposição ou de divisão para gerar os compartilhamentos de dados. Ou randômico, pseudorrandômico, determinístico, ou qualquer sua combinação podem ser empregados para decompor e dividir os dados.

Em ainda outras modalidades, um esquema de compartilhamento de segredo de n participantes com um espaço de mensagem S está provido. Uma família de adversários, A, pode ser definida. O esquema de compartilhamento de segredo de n participantes pode incluir um ou mais dos seguintes cinco primitivos: (1) um algoritmo de criptografia simétrico com chaves de k bits e um espaço de mensagem S; (2) um algoritmo de PSS de n participantes sobre os adversários A com um espaço de mensagem $\{0,1\}^k$; (3) um algoritmo de dispersão de informações (IDA) de n participantes; (4) um código de correção de erro (ECC) de n participantes sobre os adversários A com um espaço de mensagem $\{0,1\}^h$; e (5) um esquema de comprometimento randomizado (ou probabilístico). Os dados podem ser protegidos primeiramente aplicando um algoritmo de compartilhamento de segredo computacional nos dados a serem protegidos. Um valor randômico ou pseudorrandômico pode então ser gerado. Da saída do algoritmo de compartilhamento de segredo e do valor randômico ou pseudorrandômico, um conjunto de valores de validação e um conjunto de valores de não-validação podem ser computados. Uma pluralidade de compartilhamentos pode então ser formada combinando um compartilhamento emitido do algoritmo de compartilhamento de segredo, um valor de não-validação, e um ou mais valores de validação. Os compartilhamentos podem então ser armazenados em uma ou mais localizações físicas (por exemplo, em um disco rígido magnético), ou uma ou mais localizações geográficas (por exemplo, diferentes repositórios de dados ou servidores).

Em algumas modalidades, um esquema de comprometimento probabilístico pode ser utilizado para computar o conjunto de valores de validação e um conjunto de valores de não-validação. Cada compartilhamento pode ser definido por um compartilhamento emitido de um algoritmo de compartilhamento de segredo computacional, um valor de não-validação, e

um ou mais valores de validação do conjunto de valores de validação.

Em algumas modalidades, uma chave criptográfica pode ser gerada e utilizada para criptografar os dados do usuário para criar uma porção de texto cifrado. Um conjunto de n compartilhamentos de chave pode ser criado pela aplicação de um algoritmo de compartilhamento de segredo na chave criptográfica. Um conjunto de n blocos de textos cifrados pode então ser criado pela aplicação de um algoritmo de dispersão de informações (IDA) no texto cifrado. Um conjunto de n valores de validação e n valores de não-validação podem ser computados pela aplicação de um esquema de comprometimento probabilístico a cada um dos n compartilhamentos de chave e n blocos de textos cifrados. N fragmentos de dados podem ser formados, onde cada fragmento de dados pode ser uma função de um compartilhamento de chave, um texto cifrado, um valor de não-validação, e um ou mais valores de validação. Finalmente, os fragmentos de dados podem ser armazenados em um ou mais dispositivos de armazenamento lógicos (por exemplo, n dispositivos de armazenamento lógicos). Um ou mais destes dispositivos de armazenamento lógicos podem estar situados em diferentes localizações físicas ou geográficas. Os dados do usuário podem então ser reconstituídos combinando pelo menos um número predefinido dos fragmentos de dados. Em algumas modalidades, vários códigos de correção de erro podem ser utilizados para prover uma coleção adequada de valores de validação para cada participante.

BREVE DESCRIÇÃO DOS DESENHOS

A presente invenção está abaixo descrita em mais detalhes em conexão com os desenhos anexos, os quais pretendem ilustrar e não limitar a invenção, e nos quais:

Figura 1 ilustra um diagrama de blocos de um sistema criptográfico, de acordo com aspectos de uma modalidade de invenção;

Figura 2 ilustra um diagrama de blocos da máquina de confiança da Figura 1, de acordo com aspectos de uma modalidade da invenção;

Figura 3 ilustra um diagrama de blocos da máquina de transação da Figura 2, de acordo com aspectos de uma modalidade da invenção;

Figura 4 ilustra um diagrama de blocos do depositório da Figura 2, de acordo com aspectos de uma modalidade da invenção;

Figura 5 ilustra um diagrama de blocos da máquina de autenticação da Figura 2, de acordo com aspectos de uma modalidade da invenção;

Figura 6 ilustra um diagrama de blocos da máquina criptográfica da Figura 2, de acordo com aspectos de uma modalidade da invenção;

Figura 7 é um diagrama de blocos ilustrativo que apresenta a estrutura geral de um esquema de compartilhamento de segredo computacional robusto (RCSS) de acordo com uma modalidade da invenção;

Figura 8 ilustra o processo de compartilhamento de segredo de acordo com uma modalidade da invenção;

Figura 9 ilustra mais detalhes das etapas de validação na Figura 8 de acordo com uma modalidade da invenção;

Figura 10 ilustra o processo de compartilhamento com base em uma diferente abstração de construir um esquema de RCSS de um esquema de CSS e um esquema de compromisso; e

Figura 11 ilustra mais detalhes das etapas de verificação no esquema de comprometimento probabilístico mostrado na Figura 10.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Um aspecto da presente invenção é prover um sistema criptográfico onde um ou mais servidores seguros, ou uma máquina de confiança, armazena as chaves criptográficas e os dados de autenticação do usuário. Os usuários acessam a funcionalidade de sistemas criptográficos convencionais através de acesso de rede para a máquina de confiança, no entanto, a máquina de confiança não libera as chaves reais e outros dados de autenticação e portanto, as chaves e os dados permanecem seguros. Este armazenamento de chaves e de dados de autenticação centrado no servidor provê segurança, portabilidade, disponibilidade, e retidão independentes do usuário.

Como os usuários podem ser confiantes, ou confiar, no sistema criptográfico para executar a autenticação de usuário e de documentos e

outras funções criptográficas, uma ampla variedade de funcionalidades pode ser incorporada no sistema. Por exemplo, o provedor de máquina de confiança pode assegurar contra o repúdio de acordo, por exemplo, autenticando os participantes de acordo, assinando digitalmente o acordo em nome dos ou para os participantes, e armazenando um registro do acordo digitalmente assinado por cada participante. Além disso, o sistema criptográfico pode monitorar os acordos e determinar aplicar graus variáveis de autenticação, com base em, por exemplo, preço, usuário, vendedor, localização geográfica, local de uso, ou similares.

Para facilitar uma compreensão completa da invenção, o restante da descrição detalhada descreve a invenção com referência às figuras, em que os elementos iguais estão referenciados com números iguais através de toda a descrição.

A Figura 1 ilustra um diagrama de blocos de um sistema criptográfico 100, de acordo com aspectos de uma modalidade de invenção. Como mostrado na Figura 1, o sistema criptográfico 100 inclui um sistema do usuário 105, uma máquina de confiança 110, uma autoridade de certificado 115, e um sistema de vendedor 120, que comunicam através de uma conexão de comunicação 125.

De acordo com uma modalidade da invenção, o sistema do usuário 105 compreende um computador de uso geral convencional que tem um ou mais microprocessadores, tais como, por exemplo, um processador baseado em Intel. Mais ainda, o sistema do usuário 105 inclui um sistema operacional apropriado, tal como um sistema operacional capaz de incluir gráficos ou janelas, tais como Windows, Unix, Linux, ou similares. Como mostrado na Figura 1, o sistema do usuário 105 pode incluir um dispositivo biométrico 107. O dispositivo biométrico 107 pode vantajosamente capturar a biometria de um usuário e transferir a biometria capturada para a máquina de confiança 110. De acordo com uma modalidade da invenção, o dispositivo biométrico pode vantajosamente compreender um dispositivo que tem atributos e características similares àqueles descritos no Pedido de Patente U.S. Número 08/926.277, depositado em 05 de Setembro de 1997, intitulado

"GERADOR DE IMAGEM DE OBJETO EM RELEVO", no Pedido de Patente U.S. Número 09/558.634, depositado em 26 de Abril de 2000, intitulado "DISPOSITIVO DE FORMAÇÃO DE IMAGEM PARA UM OBJETO EM RELEVO E SISTEMA E MÉTODO PARA UTILIZAR O DISPOSITIVO DE FORMAÇÃO DE IMAGEM", no Pedido de Patente U.S. Número 09/435.011, depositado em 05 de Novembro de 1999, intitulado "ADAPTADOR DE SENSOR DE OBJETO EM RELEVO", no Pedido de Patente U.S. 09/477.943, depositado em 05 de Janeiro de 2000, intitulado "SENSOR DE IMAGEM ÓTICA PLANA E SISTEMA PARA GERAR UMA IMAGEM ELETRÔNICA DE UM OBJETO EM RELEVO PARA LEITURA DE IMPRESSÕES DIGITAIS", todos os quais são de propriedade do cedente presente, e todos os quais estão por meio disto aqui incorporados por referência.

Além disso, o sistema do usuário 105 pode conectar na conexão de comunicação 125 através de um provedor de serviços convencional, tal como, por exemplo, uma linha de discagem, uma linha de assinante digital (DSL), um modem de cabo, uma conexão de fibra, ou similares. De acordo com outra modalidade, o sistema do usuário 105 conecta na conexão de comunicação 125 através de uma conectividade de rede tal como, por exemplo, uma rede de área local ou ampla. De acordo com uma modalidade, o sistema operacional inclui uma pilha de TCP/IP que manipula todo o tráfego de mensagens de entrada e de saída passado pela conexão de comunicação 125.

Apesar do sistema do usuário 105 ser descrito com referência às modalidades acima, a invenção não pretende estar limitada a estas. Ao contrário, uma pessoa versada na técnica reconhecerá da descrição aqui, um amplo número de modalidades alternativas do sistema do usuário 105, incluindo praticamente qualquer dispositivo de computação capaz de enviar ou receber as informações de outro sistema de computador. Por exemplo, o sistema do usuário 105 pode incluir, mas não está limitado a, uma estação de trabalho de computador, uma televisão interativa, um quiosque interativo, um dispositivo de computação móvel pessoal, tal como um assistente digital, um telefone móvel, um laptop, ou similar, um dispositivo de comunicações sem fio, um cartão inteligente, um dispositivo de computação incorporado,

ou similares, os quais podem interagir com a conexão de comunicação 125. Em tais sistemas interativos, os sistemas operacionais provavelmente diferirão e serão adaptados para o dispositivo específico. No entanto, de acordo com uma modalidade, os sistemas operacionais vantajosamente continuam a prover os protocolos de comunicações apropriados necessários para estabelecer uma comunicação com a conexão de comunicação 125.

A Figura 1 ilustra a máquina de confiança 110. De acordo com uma modalidade, a máquina de confiança 110 compreende um ou mais servidores seguros para acessar e armazenar informações reservadas, as quais podem ser qualquer tipo ou forma de dados, tais como, mas não limitados a, texto, áudio, vídeo, dados de autenticação do usuário e chaves criptográficas públicas e privadas. De acordo com uma modalidade, os dados de autenticação incluem os dados designados a identificar singularmente um usuário do sistema criptográfico 100. Por exemplo, os dados de autenticação podem incluir um número de identificação do usuário, uma ou mais biometrias, e uma série de perguntas e respostas geradas pela máquina de confiança 110 ou pelo usuário, mas respondidas inicialmente pelo usuário no registro. As questões acima podem incluir dados demográficos, tais como local de nascimento, endereço, aniversário, ou similares, dados pessoais, tais como o nome de solteira da mãe, o sorvete favorito, ou similares, ou outros dados designados para identificar singularmente o usuário. A máquina de confiança 110 compara os dados de autenticação de um usuário associados com uma transação corrente, com os dados de autenticação providos em um momento anterior, tal como, por exemplo, durante o registro. A máquina de confiança 110 pode vantajosamente requerer que o usuário produza os dados de autenticação no momento de cada transação, ou, a máquina de confiança 110 pode vantajosamente permitir que o usuário produza periodicamente os dados de autenticação, tal como no início de uma cadeia de transações ou no registro em um site da Web de vendedor específico.

De acordo com a modalidade onde o usuário produz os dados biométricos, o usuário provê uma característica física, tal como, mas não limitado a, um escaneamento facial, um escaneamento de mão, um escane-

amento de orelha, um escaneamento de íris, um escaneamento de retina, um padrão vascular, um DNA, uma impressão digital, escrita ou voz, para o dispositivo biométrico 107. O dispositivo biométrico vantajosamente produz um padrão eletrônico, ou biométrico, da característica física. O padrão eletrônico é transferido através do sistema do usuário 105 para a máquina de confiança 110 ou para registro ou propósitos de autenticação.

Uma vez que o usuário produz os dados de autenticação apropriados e a máquina de confiança 110 determina uma coincidência positiva entre os dados de autenticação (dados de autenticação correntes) e os dados de autenticação providos no momento do registro (dados de autenticação de registro), a máquina de confiança 110 provê o usuário com uma funcionalidade criptográfica completa. Por exemplo, o usuário apropriadamente autenticado pode vantajosamente empregar a máquina de confiança 110 para executar um hash, assinar digitalmente, criptografar e decifrar (frequentemente juntos referidos somente como criptografar), criar ou distribuir certificados digitais, e similares. No entanto, as chaves criptográficas privadas utilizadas nas funções criptográficas não estarão disponíveis fora da máquina de confiança 110, por meio disto assegurando a integridade das chaves criptográficas.

De acordo com uma modalidade, a máquina de confiança 110 gera e armazena as chaves criptográficas. De acordo com outra modalidade, pelo menos uma chave criptográfica está associada com cada usuário. Mais ainda, quando as chaves criptográficas incluem a tecnologia de chave pública, cada chave privada associada com um usuário é gerada dentro da, e não-liberada da, máquina de confiança 110. Assim, desde que o usuário tenha acesso à máquina de confiança 110, o usuário pode executar funções criptográficas utilizando a sua chave privada ou pública. Tal acesso remoto vantajosamente permite que todos os usuários permanecem completamente móveis e acessem a funcionalidade criptográfica através de praticamente qualquer conexão de Internet, tal como os telefones celulares e de satélite, os quiosques, os laptops, os quartos de hotel, e similares.

De acordo com outra modalidade, a máquina de confiança 110

executa a funcionalidade criptográfica utilizando um par de chaves gerado pela máquina de confiança 110. De acordo com esta modalidade, a máquina de confiança 110 primeiro autentica o usuário, e após o usuário ter produzido apropriadamente os dados de autenticação que coincidem com os dados de autenticações de registro, a máquina de confiança 110 utiliza o seu próprio par de chaves criptográficas para executar as funções criptográficas em nome do usuário autenticado.

Uma pessoa versada na técnica reconhecerá da descrição aqui que as chaves criptográficas podem vantajosamente incluir algumas ou todas as chaves simétricas, as chaves públicas, e as chaves privadas. Além disso, uma pessoa versada na técnica reconhecerá da descrição aqui que as chaves acima podem ser implementadas com um amplo número de algoritmos disponíveis de tecnologias comerciais, tais como, por exemplo, RSA, ELGAMAL, ou similares.

A Figura 1 também ilustra a autoridade de certificado 115. De acordo com uma modalidade, a autoridade de certificado 115 pode vantajosamente compreender uma organização ou companhia de terceiros confiada que emite os certificados digitais tais como, por exemplo, VeriSign, Baltimore, Entrust, ou similares. A máquina de confiança 110 pode vantajosamente transmitir as solicitações para certificados digitais, através de um ou mais protocolos de certificado digital convencionais, tais como por exemplo PKCS10, para a autoridade de certificado 115. Em resposta, a autoridade de certificado 115 emitirá um certificado digital em um ou mais de um número de diferentes protocolos, tais como, por exemplo, PKCS7. De acordo com uma modalidade da invenção, a máquina de confiança 110 solicita os certificados digitais de diversas ou todas as autoridades de certificado 115 proeminentes de modo que a máquina de confiança 110 tenha acesso a um certificado digital que corresponde ao padrão de certificado de qualquer participante solicitante.

De acordo com outra modalidade, a máquina de confiança 110 internamente executa as emissões de certificados. Nesta modalidade, a máquina de confiança 110 pode acessar um sistema de certificado para gerar

os certificados e/ou pode gerar internamente os certificados quando estes são solicitados, tal como, por exemplo, no momento de geração de chave ou no padrão de certificado solicitado no momento da solicitação. A máquina de confiança 110 será abaixo descrita em maiores detalhes.

A Figura 1 também ilustra o sistema de vendedor 120. De acordo com uma modalidade, o sistema de vendedor 120 vantajosamente compreende um servidor da Web. Os servidores da Web típicos geralmente servem o conteúdo pela Internet utilizando uma ou diversas linguagens de marcação de Internet ou padrões de formato de documento, tais como a Linguagem de Marcação de Hipertexto (HTML) ou a Linguagem de Marcação Extensível (XML). O servidor da Web aceita as solicitações de navegadores tais como Netscape e Internet Explorer e então retorna os documentos eletrônicos apropriados. Um número de tecnologias de servidor ou de lado de cliente podem ser utilizadas para aumentar a potência do servidor da Web além de sua capacidade de fornecer documentos eletrônicos-padrão. Por exemplo, estas tecnologias incluem scripts de Interface de Porta Comum (CGI), segurança de Camada de Soquetes Seguros (SSL), e Páginas de Servidor Ativo (ASPs). O sistema de vendedor 120 pode vantajosamente prover um conteúdo eletrônico em relação a transações comerciais, pessoais, educacionais, ou outras.

Apesar do sistema de vendedor 120 ser descrito com referência às modalidades acima, a invenção não pretende estar limitada a estas. Ao contrário, alguém versado na técnica reconhecerá da descrição aqui que o sistema de vendedor 120 pode vantajosamente compreender qualquer um dos dispositivos descritos com referência ao sistema do usuário 105 ou suas combinações.

A Figura 1 também ilustra a conexão de comunicação 125 que conecta o sistema do usuário 105, a máquina de confiança 110, a autoridade de certificado 115, e o sistema de vendedor 120. De acordo com uma modalidade, a conexão de comunicação 125 de preferência compreende a Internet. A internet, como utilizada através de toda esta descrição é uma rede global de computadores. A estrutura da Internet, a qual é bem-conhecida

daqueles versados na técnica, inclui uma rede de backbone com redes ramificando do backbone. Estas ramificações, por sua vez, têm redes ramificando destas, e assim por diante. Os roteadores movem os pacotes de informações entre os níveis de rede, e então de rede para rede, até que o pacote chegue na vizinhança de seu destino. Do destino, o hospedeiro da rede de destino direciona o pacote de informações para o terminal apropriado, ou nodo. Em uma modalidade vantajosa, os hubs de roteamento de Internet compreendem servidores de sistema de nome de domínio (DNS) que utilizam um Protocolo de Controle de Transmissão / Protocolo de Internet (TCP/IP) como é bem-conhecido na técnica. Os hubs de roteamento conectam a um ou mais outros hubs de roteamento através de conexões de comunicação de alta velocidade.

Uma parte popular da Internet é a World Wide Web. A World Wide Web contém diferentes computadores, os quais armazenam os documentos capazes de exibir informações gráficas e textuais. Os computadores que proveem as informações para a World Wide Web são tipicamente denominados "sites da Web". Um site da Web é definido por um endereço de Internet que tem uma página eletrônica associada. A página eletrônica pode ser identificada por um Localizador de Recurso Uniforme (URL). Geralmente, uma página eletrônica é um documento que organiza a apresentação de texto, as imagens gráficas, o áudio, o vídeo, e assim por diante.

Apesar da conexão de comunicação 125 ser descrita em termos de sua modalidade preferida, alguém versado na técnica reconhecerá da descrição aqui que a conexão de comunicação 125 pode incluir uma ampla gama de conexões de comunicação interativas. Por exemplo, a conexão de comunicação 125 pode incluir as redes de televisão interativa, as redes telefônicas, os sistemas de transmissão de dados sem fio, os sistemas de cabo de duas vias, as redes de computador personalizadas privadas ou públicas, as redes de quiosques interativos, as redes de caixas automáticos, as conexões diretas, as redes de satélite ou celular, e similares.

A Figura 2 ilustra um diagrama de blocos da máquina de confiança 110 da Figura 1, de acordo com aspectos de uma modalidade da in-

venção. Como mostrado na Figura 2, a máquina de confiança 110 inclui uma máquina de transação 205, um depositório 210, uma máquina de autenticação 215, e uma máquina criptográfica 220. De acordo com uma modalidade da invenção, a máquina de confiança 110 também inclui um armazenamento de massa 225. Como adicionalmente mostrado na Figura 2, a máquina de transação 205 comunica com o depositório 210, a máquina de autenticação 215, e a máquina criptográfica 220, juntamente com o armazenamento de massa 225. Além disso, o depositório 210 comunica com a máquina de autenticação 215, a máquina criptográfica 220, e o armazenamento de massa 225. Mais ainda, a máquina de autenticação 215 comunica com a máquina criptográfica 220. De acordo com uma modalidade da invenção, algumas ou todas as comunicações acima podem vantajosamente compreender a transmissão de documentos de XML para os endereços de IP que correspondem ao dispositivo de recepção. Como mencionado acima, os documentos de XML vantajosamente permitem que os projetistas criem os seus próprios identificadores de documento personalizados, permitindo a definição, a transmissão, e validação, e a interpretação dos dados entre os aplicativos e entre as organizações. Mais ainda, algumas ou todas as comunicações acima podem incluir um SSL convencional.

De acordo com uma modalidade, a máquina de transação 205 compreende um dispositivo de roteamento de dados, tal como um servidor da Web convencional disponível da Netscape, Microsoft, Apache, ou similares. Por exemplo, o servidor da Web pode vantajosamente receber os dados que entram da conexão de comunicação 125. De acordo com uma modalidade da invenção, os dados que entram são endereçados para um sistema de segurança de interface inicial para a máquina de confiança 110. Por exemplo, o sistema de segurança de interface inicial pode vantajosamente incluir um firewall, um sistema de detecção de intrusão que procura por perfis de ataque conhecidos, e/ou um escaneador de vírus. Após ultrapassarem o sistema de segurança de interface inicial, os dados são recebidos pela máquina de transação 205 e roteados para um do depositório 210, da máquina de autenticação 215, da máquina criptográfica 220, e do armazena-

mento de massa 225. Além disso, a máquina de transação 205 monitora os dados que entram da máquina de autenticação 215 e da máquina criptográfica 220, e roteia os dados para os sistemas específicos através da conexão de comunicação 125. Por exemplo, a máquina de transação 205 pode vantajosamente rotear os dados para o sistema do usuário 105, a autoridade de certificado 115, ou o sistema de vendedor 120.

De acordo com uma modalidade, os dados são roteados utilizando as técnicas de roteamento de HTTP convencionais, tais como, por exemplo, empregando os URLs ou os Indicadores de Recurso Uniformes (URIs). Os URIs são similares aos URLs, no entanto, os URIs tipicamente indicam a fonte de arquivos ou ações, tais como, por exemplo, executáveis, scripts, e similares. Portanto, de acordo com uma modalidade, o sistema do usuário 105, a autoridade de certificado 115, o sistema de vendedor 120, e os componentes da máquina de confiança 110, vantajosamente incluem dados suficientes dentro dos URLs ou URIs de comunicação para a máquina de transação 205 rotear apropriadamente os dados através de todo o sistema criptográfico.

Apesar do roteamento de dados ser descrito com referência à sua modalidade preferida, alguém versado na técnica reconhecera um amplo número de possíveis soluções ou estratégias de roteamento de dados. Por exemplo, o XML ou outros pacotes de dados podem vantajosamente ser desempacotados e reconhecidos por seu formato, conteúdo, ou similares, de modo que a máquina de transação 205 possa rotear apropriadamente os dados através de toda a máquina de confiança 110. Mais ainda, alguém versado na técnica reconhecerá que o roteamento de dados pode vantajosamente ser adaptado aos protocolos de transferência de dados em conformidade com os sistemas de rede específicos, tais como, por exemplo, quando a conexão de comunicação 125 compreende uma rede local.

De acordo com ainda outra modalidade da invenção, a máquina de transação 205 inclui as tecnologias de criptografia de SSL convencionais, tais como os sistemas acima e pode autenticar a si próprio, e vice versa, com a máquina de transação 205, durante comunicações específicas. Como

será utilizado durante toda esta descrição, o termo "1/2 SSL" refere-se a comunicações onde um servidor mas não necessariamente o cliente, é autenticado por SSL, e o termo "SSL TOTAL" refere-se a comunicações onde o cliente e o servidor são autenticados por SSL. Quando a presente descrição utiliza o termo "SSL", a comunicação pode compreender 1/2 ou SSL TOTAL.

Conforme a máquina de transação 205 roteia os dados para os vários componentes do sistema criptográfico 100, a máquina de transação 205 pode vantajosamente criar um rastro de auditoria. De acordo com uma modalidade, o rastro de auditoria inclui um registro de pelo menos o tipo e o formato de dados roteados pela máquina de transação 205 através de todo o sistema criptográfico 100. Tais dados de auditoria podem vantajosamente ser armazenados no armazenamento de massa 225.

A Figura 2 também ilustra o depositório 210. De acordo com uma modalidade, o depositório 210 compreende uma ou mais instalações de armazenamento de dados, tais como, por exemplo, um servidor de diretório, um servidor de banco de dados, ou similares. Como mostrado na Figura 2, o depositório 210 armazena as chaves criptográficas e os dados de autenticação de registro. As chaves criptográficas podem vantajosamente corresponder à máquina de confiança 110 ou a usuários do sistema criptográfico 100, tal como o usuário ou o vendedor. Os dados de autenticação de registro podem vantajosamente incluir os dados designados para identificar singularmente um usuário, tais como, a ID de usuário, as senhas, as respostas a perguntas, dados biométricos, ou similares. Estes dados de autenticação de registro podem vantajosamente ser adquiridos no registro de um usuário ou outro momento posterior alternativo. Por exemplo, a máquina de confiança 110 pode incluir dados de autenticação periódicos ou outros dados de renovação ou re-emissão de registro.

De acordo com uma modalidade, a comunicação da máquina de transação 205 para a e da máquina de autenticação 215 e a máquina criptográfica 220 compreende uma comunicação segura, tal como, por exemplo, uma tecnologia de SSL convencional. Além disso, como acima mencionado, os dados das comunicações para o e do depositório 210 podem ser transfe-

ridos utilizando URLs, URIs, HTTP ou documentos de XML, com qualquer um dos acima vantajosamente tendo solicitações de dados e formatos incorporados nos mesmos.

Como acima mencionado, o depositório 210 pode vantajosamente compreender uma pluralidade de instalações de armazenamento de dados seguras. Em tal modalidade, as instalações de armazenamento de dados seguras podem ser configuradas de modo que um compromisso da segurança em uma instalação de armazenamento de dados individuais não comprometerá as chaves criptográficas ou os dados de autenticação armazenados na mesma. Por exemplo, de acordo com esta modalidade, as chaves criptográficas e os dados de autenticação são matematicamente operados de modo a substancialmente e estatisticamente randomizar os dados armazenados em cada instalação de armazenamento de dados. De acordo com uma modalidade, a randomização dos dados de uma instalação de armazenamento de dados individuais torna os dados indecifráveis. Assim, o compromisso de uma instalação de armazenamento de dados individuais produz somente um número indecifrável randomizado e não compromete a segurança de nenhuma chave criptográfica ou os dados de autenticação como um todo.

A Figura 2 também ilustra a máquina de confiança 110 que inclui a máquina de autenticação 215. De acordo com uma modalidade, a máquina de autenticação 215 compreende um comparador de dados configurado para comparar os dados da máquina de transação 205 com os dados do depositório 210. Por exemplo, durante a autenticação, um usuário supre dados de autenticação correntes para a máquina de confiança 110 de modo que a máquina de transação 205 recebe os dados de autenticação correntes. Como acima mencionado, a máquina de transação 205 reconhece as solicitações de dados, de preferência no URL ou URI, e roteia os dados de autenticação para a máquina de autenticação 215. Mais ainda, quando solicitado, o depositório 210 transfere os dados de autenticação de registro que correspondem ao usuário para a máquina de autenticação 215. Assim, a máquina de autenticação 215 tem tanto os dados de autenticação correntes quanto os

dados de autenticação de registro para comparação.

De acordo com uma modalidade, as comunicações para a máquina de autenticação compreendem comunicações seguras, tal como, por exemplo, uma tecnologia de SSL. Além disso, a segurança pode ser provida dentro dos componentes da máquina de confiança 110, tal como, por exemplo, uma supercriptografia utilizando as tecnologias de chave pública. Por exemplo, de acordo com uma modalidade, o usuário criptografa os dados de autenticação correntes com a chave pública da máquina de autenticação 215. Além disso, o depositório 210 também criptografa os dados de autenticação de registro com a chave pública da máquina de autenticação 215. Deste modo, somente a chave privada da máquina de autenticação pode ser utilizada para decifrar as transmissões.

Como mostrado na Figura 2, a máquina de confiança 110 também inclui a máquina criptográfica 220. De acordo com uma modalidade, a máquina criptográfica compreende um módulo de manipulação criptográfico, configurado para vantajosamente prover funções criptográficas convencionais, tais como, por exemplo uma funcionalidade de infraestrutura de chave pública (PKI). Por exemplo, a máquina criptográfica 220 pode vantajosamente emitir as chaves públicas e privadas para os usuários do sistema criptográfico 100. Deste modo, as chaves criptográficas são geradas na máquina criptográfica 220 e transferida para o depositório 210 de modo que pelo menos as chaves criptográficas privadas não sejam disponíveis fora da máquina de confiança 110. De acordo com outra modalidade, a máquina criptográfica 220 randomiza e divide pelo menos os dados de chave criptográfica privada, por meio disto armazenando somente os dados divididos randomizados. Similar à divisão dos dados de autenticação de registro, o processo de divisão assegura que as chaves armazenadas não sejam disponíveis fora da máquina criptográfica 220. De acordo com outra modalidade, as funções da máquina criptográfica podem ser combinadas com a e executadas pela máquina de autenticação 215.

De acordo com uma modalidade, as comunicações para a e da máquina criptográfica incluem comunicações seguras, tal como a tecnologia

de SSL. Além disso, os documentos de XML podem vantajosamente ser empregados para transferir os dados e/ou fazer solicitações de funções criptográficas.

A Figura 2 também ilustra a máquina de confiança 110 que tem o armazenamento de massa 225. Como acima mencionado, a máquina de transação 205 mantém os dados que correspondem a um rastro de auditoria e armazena tais dados no armazenamento de massa 225. Similarmente, de acordo com uma modalidade da invenção, o depositório 210 guarda dos dados que correspondem a um rastro de auditoria e armazena tais dados no dispositivo de armazenamento de massa 225. Os dados de rastro de auditoria de depositório são similares àqueles da máquina de transação 205 pelo fato de que os dados de rastro de auditoria compreendem um registro das solicitações recebidas pelo depositório 210 e a sua resposta. Além disso, o armazenamento de massa 225 pode ser utilizado para armazenar os certificados digitais que têm a chave pública de um usuário contido no mesmo.

Apesar da máquina de confiança 110 ser descrita com referência às suas modalidades preferidas e alternativas, a invenção não pretende ser limitada por isto. Ao contrário, alguém versado na técnica reconhecerá na descrição aqui, um amplo número de alternativas para a máquina de confiança 110. Por exemplo, a máquina de confiança 110, pode vantajosamente executar somente a autenticação, ou alternativamente, somente algumas ou todas as funções criptográficas, tais como a criptografia e a decifração de dados. De acordo com tais modalidades, uma da máquina de autenticação 215 e da máquina criptográfica 220 pode vantajosamente ser removida, por meio disto criando um projeto mais direto para a máquina de confiança 110. Além disso, a máquina criptográfica 220 pode também comunicar com uma autoridade de certificado de modo que a autoridade de certificado seja incorporada na máquina de confiança 110. De acordo com ainda outra modalidade, a máquina de confiança 110 pode vantajosamente executar a autenticação e uma ou mais funções criptográficas, tais como, por exemplo, a assinatura digital.

A Figura 3 ilustra um diagrama de blocos da máquina de transa-

ção 205 da Figura 2, de acordo com os aspectos de uma modalidade da invenção. De acordo com esta modalidade, a máquina de transação 205 compreende um sistema operacional 305 que tem uma cadeia de manipulação e uma cadeia de audição. O sistema operacional 305 pode vantajosamente ser similar àqueles encontrados nos servidores de alto volume convencionais, tais como, por exemplo, os servidores da Web disponíveis da Apache. A cadeia de audição monitora a comunicação que entra de uma da conexão de comunicação 125, da máquina autenticação, 215 e da máquina criptográfica 220 quanto ao fluxo de dados que entram. A cadeia de manipulação reconhece as estruturas de dados específicas do fluxo de dados que entram, tais como, por exemplo, as estruturas de dados acima, por meio disto roteando os dados que entram para uma da conexão de comunicação 125, do depositório 210, da máquina de autenticação 215, da máquina criptográfica 220, ou do armazenamento de massa 225. Como mostrado na Figura 3, os dados que entram e saem podem vantajosamente ser protegidos através, por exemplo, da tecnologia de SSL.

A Figura 4 ilustra um diagrama de blocos do depositório 210 da Figura 2 de acordo com os aspectos de uma modalidade da invenção. De acordo com esta modalidade, o depositório 210 compreende um ou mais servidores de protocolo de acesso de diretório leve (LDAP). Os servidores de diretório LDAP são disponíveis de uma ampla variedade de fabricantes tais como Netscape, ISO, e outros. A Figura 4 também mostra que o servidor de diretório de preferência armazena os dados 405 que correspondem às chaves criptográficas e dados 410 que correspondem aos dados de autenticação de registro. De acordo com a modalidade, o depositório 210 compreende uma única estrutura de memória lógica que indexa os dados de autenticação e os dados de chave criptográfica a uma única ID de usuário. A única estrutura de memória lógica de preferência inclui mecanismos para assegurar um alto grau de confiança, ou de segurança, nos dados armazenados na mesma. Por exemplo, a localização física do depositório 210 pode vantajosamente incluir um amplo número de medidas de segurança convencionais, tal como um acesso a empregados limitado, sistemas de vigilância moder-

nos, e similares. Além das, ou no lugar das, seguranças físicas, o sistema de computador ou servidor pode vantajosamente incluir soluções de software para proteger os dados armazenados. Por exemplo, o depositório 210 pode vantajosamente criar e armazenar os dados 415 que correspondem a um rastro de auditoria de ações tomadas. Além disso, as comunicações que entram e saem podem vantajosamente ser criptografadas com criptografia de chave pública acoplada com as tecnologias de SSL convencionais.

De acordo com outra modalidade, o depositório 210 pode compreender instalações de armazenamento de dados fisicamente separadas, como adicionalmente descrito com referência à Figura 7.

A Figura 5 ilustra um diagrama de blocos da máquina de autenticação 215 da Figura 2 de acordo com os aspectos de uma modalidade da invenção. Similar à máquina de transação 205 da Figura 3, a máquina autenticação 215 compreende um sistema operacional 505 que tem pelo menos uma cadeia de audição e uma de manipulação de uma versão modificada de um servidor da Web convencional, tal como, por exemplo, os servidores da Web disponíveis da Apache. Como mostrado na Figura 5, a máquina de autenticação 215 inclui um acesso a pelo menos uma chave privada 510. A chave privada 510 pode vantajosamente ser utilizada, por exemplo, para decifrar os dados da máquina de transação 205 ou do depositório 210, os quais foram criptografados com uma chave pública correspondente da máquina de autenticação 215.

A Figura 5 também ilustra a máquina de autenticação 215 que compreende um comparador 515, um módulo de divisão de dados 520, e um módulo de montagem de dados 525. De acordo com a modalidade preferida da invenção, o comparador 515 inclui uma tecnologia capaz de comparar padrões potencialmente complexos relativos aos dados de autenticação biométricos acima. A tecnologia pode incluir soluções de hardware, software, ou combinadas para as comparações de padrões, tais como, por exemplo, aqueles que representam os padrões de impressão digital ou os padrões de voz. Além disso, de acordo com uma modalidade, o comparador 515 da máquina de autenticação 215 pode vantajosamente comparar os hashes de

documentos convencionais de modo a passar um resultado de comparação. De acordo com uma modalidade da invenção, o comparador 515 inclui a aplicação de heurística 530 à comparação. A heurística 530 pode vantajosamente resolver as circunstâncias que envolvem uma tentativa de autenticação, tais como, por exemplo, a hora do dia, o endereço de IP ou a máscara de sub-rede, perfil de aquisição, endereço de e-mail, o número de série ou ID de processador, ou similares.

Mais ainda, a natureza de comparações de dados biométricos pode resultar em graus variáveis de confiança sendo produzidos da coincidência dos dados de autenticação biométricos correntes com os dados de registro. Por exemplo, ao contrário de uma senha tradicional a qual pode somente retornar uma coincidência positiva ou negativa, uma impressão digital pode ser determinada ser uma coincidência parcial, por exemplo uma coincidência de 90%, uma coincidência de 75%, ou uma coincidência de 10%, ao invés de ser simplesmente correto ou incorreto. Outros identificadores biométricos tais como a análise de impressão de voz ou reconhecimento de face podem compartilhar esta propriedade de autenticação probabilística, ao invés de uma autenticação absoluta.

Quando trabalhando com tal autenticação probabilística ou em outros casos onde uma autenticação é considerada menos do que absolutamente confiável, é desejável aplicar a heurística 530 para determinar se o nível de confiança na autenticação provida é suficientemente alto para autenticar a transação a qual está sendo feita.

Será algumas vezes o caso que a transação em questão é uma transação de valor relativamente baixo onde é aceitável ser autenticada a um nível de confiança mais baixo. Isto poderia incluir uma transação a qual tem um baixo valor em dólares associado com a mesma (por exemplo, uma compra de $10) ou uma transação com baixo risco (por exemplo, a admissão a um site da Web de membros somente).

Ao contrário, para autenticar outras transações, pode ser desejável requerer um alto grau de confiança na autenticação antes de permitir que a transação prossiga. Tais transações podem incluir as transações de

grande valor em dólares (por exemplo, assinar um contrato de suprimento de muitos milhões de dólares) ou uma transação com um alto risco de uma autenticação imprópria ocorrer (por exemplo, registrar remotamente em um computador do governo).

A utilização de heurística 530 em combinação com os níveis de confiança e valores de transação pode ser utilizada como será abaixo descrito para permitir que o comparador provenha um sistema de autenticação dinâmico sensível ao conteúdo.

De acordo com outra modalidade da invenção, o comparador 515 pode vantajosamente rastrear as tentativas de autenticação para uma transação específica. Por exemplo, quando uma transação falha, a máquina de confiança 110 pode solicitar ao usuário reinserir os seus dados de autenticação correntes. O comparador 515 da máquina de autenticação 215 pode vantajosamente empregar um limitador de tentativas 535 para limitar o número de tentativas de autenticação, por meio disto proibindo as tentativas de força bruta para personificar os dados de autenticação de um usuário. De acordo com uma modalidade, o limitador de tentativas 535 compreende um módulo de software que monitora as transações para repetir as tentativas de autenticação e, por exemplo, limitar as tentativas de autenticação para uma dada transação em três. Assim, o limitador de tentativas 535 limitará uma tentativa automatizada de personificar os dados de autenticação de um indivíduo a, por exemplo, três "palpites". Quando de três falhas, o limitador de tentativas 535 pode vantajosamente negar tentativas de autenticação adicionais. tal negação pode vantajosamente ser implementada através, por exemplo, do comparador 515 retornando um resultado negativo independentemente dos dados de autenticação correntes serem transmitidos. Por outro lado, a máquina de transação 205 pode vantajosamente bloquear quaisquer tentativas de autenticação adicionais pertencentes a uma transmissão na qual três tentativas anteriormente falharam.

A máquina de autenticação 215 também inclui o módulo de divisão de dados 520 e o módulo de montagem de dados 525. O módulo de divisão de dados 520 vantajosamente compreende um módulo de software, de

hardware ou de combinação que tem a capacidade de operar matematicamente sobre vários dados de modo a substancialmente randomizar e dividir os dados em porções. De acordo com uma modalidade, os dados originais não são recriáveis de uma porção individual. O módulo de montagem de dados 525 vantajosamente compreende um módulo de software, de hardware ou de combinação configurado para operar matematicamente sobre as porções substancialmente randomizadas acima, de modo que a sua combinação provenha os dados decifrados originais. De acordo com uma modalidade, a máquina de autenticação 215 emprega o módulo de divisão de dados 520 para randomizar e dividir os dados de autenticação de registro em porções, e emprega o módulo de montagem de dados 525 para remontar as porções em dados de autenticação de registro utilizáveis.

A Figura 6 ilustra um diagrama de blocos da máquina criptográfica 220 da máquina de confiança 110 da Figura 2 de acordo com os aspectos de ma modalidade da invenção. Similar à máquina de transação 205 da Figura 3, a máquina criptográfica 220 compreende um sistema operacional 605 que tem pelo menos uma cadeia de audição e uma de manipulação de uma versão modificada de um servidor da Web convencional, tal como, por exemplo, os servidores da Web disponíveis da Apache. Como mostrado na Figura 6, a máquina criptográfica 220 compreende um módulo de divisão de dados 610 e um módulo de montagem de dados 620 que funcionam similar àqueles da Figura 5. No entanto, de acordo com uma modalidade, o módulo de divisão de dados 610 e o módulo de montagem de dados 620 processam os dados de chave criptográfica, em oposição aos dados de autenticação de registro acima. Apesar de que, alguém versado na técnica reconhecerá da descrição aqui que o módulo de divisão de dados 610 e o módulo de montagem de dados 620 podem ser combinados com aqueles da máquina de autenticação 215.

A máquina criptográfica 220 também compreende um módulo de manipulação criptográfica 625 configurado para executar uma, algumas ou todas de um amplo número de funções criptográficas. De acordo com uma modalidade, o módulo de manipulação criptográfica 625 pode compreender

módulos ou programas de software, hardware, ou ambos. De acordo com outra modalidade, o módulo de manipulação criptográfica 625 pode executar comparações de dados, análise de dados, divisão de dados, separação de dados, hash de dados, criptografia ou decifração de dados, verificação ou criação de assinatura digital, geração, armazenamento, ou solicitações de certificado digital, geração de chave criptográfica, ou similares. Mais ainda, alguém versado na técnica reconhecerá da descrição aqui que o módulo de manipulação criptográfica 625 pode vantajosamente compreender uma infraestrutura de chave pública, tal como Pretty Good Privacy (PGP), um sistema de chave pública baseado em RSA, ou um amplo número de sistemas de gerenciamento de chave alternativos. Além disso, o módulo de manipulação criptográfica 625 pode executar a criptografia de chave pública, a criptografia de chave simétrica, ou ambas. Além disso, o módulo de manipulação criptográfica 625 pode incluir um ou mais programas ou módulos de computador, hardware, ou ambos, para implementar funções de interoperabilidade contínuas transparentes.

Alguém versado na técnica também reconhecerá da descrição aqui a funcionalidade criptográfica pode incluir um amplo número ou variedade de funções geralmente relativas a sistemas de gerenciamento de chave criptográfica.

Em esquema de compartilhamento de segredo computacional robusto (RCSS) está ilustrado na Figura 7. Um participante referido como o negociante 700 tem um segredo 701 que o negociante deseja distribuir. Para este fim, o negociante 700 pode aplicar um mecanismo de compartilhamento 702 de um esquema de RCSS. O mecanismo de compartilhamento 702 pode resultar em algum número, n, de compartilhamentos sendo gerados, como indicado pelos compartilhamentos 704, 705, e 706. Uma coleção 703 de todos compartilhamentos pode ser um vetor S probabilisticamente derivado do segredo 701. A coleção 703 dos compartilhamentos podem então ser enviada através de uma rede ou distribuída de uma banda, de modo que cada compartilhamento seja armazenado em seu próprio repositório de dados (ou em diferentes localizações físicas ou geográficas em um ou mais

repositórios de dados). O armazenamento dos compartilhamentos no repositório de dados lógicos 720 pode ter o benefício de uma segurança aumentada, pelo fato de que pode ser mais difícil para um adversário obter acesso a todos os compartilhamentos, os quais podem estar armazenados nos servidores de dados 721, 722, e 723, do que um subconjunto apropriado destes compartilhamentos. Um ou mais dos servidores 721, 722, 723 pode estar localizado em locais fisicamente diferentes, operados sob um diferente controle administrativo, ou protegidos por controles de acesso de hardware e de software heterogêneos. O repositório de dados lógicos 720 pode também incluir um sistema de arquivos distribuído ou em rede.

Quando um participante deseja recuperar o segredo que foi distribuído no repositório de dados lógicos 720, a entidade 740 pode tentar coletar os compartilhamentos. O primeiro compartilhamento coletado S* [1] 744 pode ser o mesmo que o compartilhamento 704, mas este também poderia deferir a uma modificação não intencional em transmissão ou armazenamento (por exemplo, corrupção de dados), ou uma modificação intencional devido às atividades de um agente adversário. Similarmente, o segundo compartilhamento coletado S* [2] 745 pode ser o mesmo que o compartilhamento 705, e o último compartilhamento coletado S* [n] 746 pode ser o mesmo que o compartilhamento 706, mas estes compartilhamentos poderiam também diferir por razões similares. Além da possibilidade de ser um compartilhamento "errado", um ou mais compartilhamentos na coleção 743 poderia também ser o valor "faltante" distinguido, representado pelo símbolo "◊". Este símbolo pode indicar que o sistema (por exemplo, a entidade 740, é incapaz de encontrar ou coletar este compartilhamento específico. O vetor de compartilhamentos referidos S* pode então ser provido para o algoritmo de recuperação 742 do esquema de RCSS, o qual pode retornar ou o segredo recuperado S* 741 ou o valor designado como inválido 747. O segredo compartilhado 701 deve ser igual ao segredo recuperado 741 a menos que o grau de atividade adversária na corrupção dos compartilhamentos exceder aquele o qual o sistema foi projetado para suportar.

O objetivo do RCSS é útil através de dois domínios principais:

proteger os dados em repouso e proteger os dados em movimento. No cenário inicial, um servidor de arquivos, por exemplo, mantém os seus dados em uma variedade de servidores remotos. Mesmo se algum subconjunto destes servidores for corrompido (por exemplo, por administradores desonestos) ou indisponível (por exemplo, devido a um desligamento de rede), os dados podem ainda ser disponíveis e privados. NO cenário de dados em movimento, o remetente pode ser conectado por uma multiplicidade de percursos, somente alguns dos quais podem ser observados pelo adversário. Enviando os compartilhamentos por estes diferentes percursos, o remetente pode transmitir com segurança o segredo S apesar da possibilidade de alguns percursos serem temporariamente indisponíveis ou adversariamente controlados. Por exemplo, em algumas modalidades, cada compartilhamento pode ser transmitido por um diferente canal de comunicação lógico. Os sistemas e métodos para proteger os dados, e especificamente os sistemas e métodos para proteger os dados em movimento, estão descritos em mais detalhes no Pedido de Patente U.S. Número 10/458.928, depositado em 11 de Junho de 2003, no Pedido de Patente U.S. Número 11/258.839, depositado em 25 de Outubro de 2005, e no Pedido de Patente U.S. Número 11/602.667, depositado em 20 de Novembro de 2006. As descrições de cada um dos pedidos de patente anteriormente depositados acima mencionados estão por meio disto aqui incorporadas por referência em suas totalidades.

Apesar de pelo menos um esquema de RCSS com tamanhos de compartilhamento curtos ter sido proposto por Krawczyk, o estudo científico deste esquema revela que este não é um esquema de RCSS válido sob fracas suposições sobre o esquema de criptografia, e não é conhecido ser um esquema válido para todas as estruturas de acesso (por exemplo, estruturas de acesso outras que os esquemas de limite). Por pelo menos estas razões, as Figuras 8-11 descrevem outras propostas para o compartilhamento de segredos. Estas outras propostas são algumas vezes aqui referidas como ESX ou HK2.

O mecanismo da proposta de ESX ou HK2 pode incluir um esquema de compartilhamento de segredo computacional robusto que pode ser

construído das seguintes cinco primitivas: (1) um gerador de números randômicos ou pseudorrandômicos; (2) um esquema de criptografia; (3) um esquema de compartilhamento de segredo perfeito (PSS); (4) um algoritmo de dispersão de informações (IDA); e (5) um esquema de comprometimento probabilístico. Estas cinco primitivas estão abaixo descritas em mais detalhes.

(1) Um gerador de número randômico ou pseudorrandômico, Rand. Tal gerador de números pode tomar um número k como entrada e retornar k bits randômicos ou pseudorrandômicos. Nas Figuras 8-11, a entrada k é omitida para facilidade de ilustração.

(2) Um esquema de criptografia, o qual pode incluir um par algoritmos, um denominado Encrypt e o outro denominado Decrypt. O algoritmo de criptografia Encrypt pode tomar uma chave K de um dado comprimento k e uma mensagem de entrada M que é referida como texto puro. O algoritmo Encrypt pode retornar uma cadeia C que é referida como o texto cifrado. O algoritmo Encrypt pode opcionalmente empregar bits randômicos, mas tais bits randômicos não estão expressamente mostrados nos desenhos. O algoritmo de decifração Decrypt pode tomar uma chave K de um dado comprimento k e uma mensagem de entrada C que é referida como texto cifrado. O algoritmo Decrypt pode retornar uma cadeia M que é referida como o texto puro. Em alguns casos, o algoritmo de decifração pode retornar um valor de falha designado, o qual pode indicar que o texto cifrado C não corresponde à criptografia de qualquer texto puro possível.

(3) Um esquema de compartilhamento de segredo perfeito (PSS), o qual pode incluir um par de algoritmos $Share^{PSS}$ e $Recover^{PSS}$. O primeiro destes algoritmos, conhecido como o algoritmo de compartilhamento do PSS, pode ser um mapa probabilístico que toma como entrada uma cadeia K, denominada o segredo, e retorna uma sequência de n cadeias, K[1], ..., K[n], referidas como compartilhamentos. Cada K[i] pode incluir um compartilhamento ou os n compartilhamentos que foram negociados, ou distribuídos, pelo negociante (a entidade que executa o processo de compartilhamento). O número n pode ser um parâmetro programável pelo usuário do esquema de compartilhamento de segredo, e este pode incluir qualquer nú-

mero positivo adequado. Em algumas modalidades, o algoritmo de compartilhamento é probabilístico pelo fato de que este emprega bits randômicos ou pseudorrandômicos. Tal dependência pode ser realizada provendo os bits randômicos ou pseudorrandômicos de algoritmo de compartilhamento, como providos pelo algoritmo Rand. O segundo algoritmo, conhecido como o algoritmo de recuperação do PSS, pode tomar como entrada um vetor de n cadeias referidas como os compartilhamentos pretendidos. Cada compartilhamento pretendido é ou uma cadeia ou um símbolo distinguido "◊" o qual é lido como faltante. Este símbolo pode ser utilizado para indicar que algum compartilhamento específico está indisponível. O algoritmo de recuperação para o esquema de compartilhamento de segredo perfeito pode retornar uma cadeia S, ou o segredo recuperado. Duas propriedades do esquema de PSS podem ser assumidas. A primeira propriedade, a propriedade de privacidade, assegura que nenhum conjunto de usuários não-autorizados obtenha nenhuma informação útil sobre o segredo que foi compartilhado de seus compartilhamentos. A segunda propriedade, a propriedade de recuperabilidade, assegura que um conjunto de participantes autorizados pode sempre recuperar o segredo, assumindo que os participantes autorizados contribuam compartilhamentos corretos para o algoritmo de recuperação e que nenhum participante adicional contribua ou um compartilhamento correto ou o valor faltante distinguido ("◊"). Este esquema de PSS pode incluir o esquema de Shamir comumente referido como "Compartilhamento de Segredo de Shamir" ou o esquema de compartilhamento de segredo de Blakley.

(4) Um algoritmo de dispersão de informações (IDA), o qual pode incluir um par de algoritmos $Share^{IDA}$ e $Recover^{IDA}$. O primeiro destes algoritmos, conhecido como o algoritmo de compartilhamento do IDA, pode incluir um mecanismo que toma como entrada uma cadeia C, a mensagem a ser dispersa, e retorna uma sequência de n cadeias, C[1], ..., C[n], as quais podem ser referidas como os blocos dos dados que resultaram da dispersão. O valor de n pode ser um parâmetro programável pelo usuário ou o IDA, e pode ser qualquer número positivo adequado. O algoritmo de compartilhamento do IDA pode ser probabilístico ou determinístico. Nas Figuras 8-11, a

possibilidade de utilizar bits randômicos no IDA não está explicitamente mostrada; no entanto, deve ser compreendido que os bits randômicos podem ser utilizados no IDA em outras modalidades.

O segundo algoritmo, conhecido como o algoritmo de recuperação do IDA, pode tomar como entrada um vetor de n cadeias, os blocos supridos. Cada bloco suprido pode ser uma cadeia ou o símbolo distinguido "◊", o qual é lido como faltante e é utilizado para indicar que algum bloco de dados específico está indisponível. O algoritmo de recuperação para o IDA pode retornar uma cadeia S, o segredo recuperado. O IDA pode ser assumido ter uma propriedade de recuperabilidade; assim, um conjunto de participantes autorizados pode sempre recuperar os dados dos blocos supridos, assumindo que os participantes autorizados contribuam blocos corretos para o algoritmo de recuperação do IDA e que nenhum participante adicional que participa na reconstrução contribua ou um bloco correto ou então o valor faltante distinguido ("◊"). Ao contrário do caso para um esquema de PSS, pode não existir uma propriedade de privacidade associada com o IDA e, de fato, um IDA simples e prático é replicar a entrada C por n vezes, e fazer com que o algoritmo de recuperação utilize o valor que ocorre mais frequentemente como os dados recuperados. IDAs mais eficientes são conhecidos (por exemplo, o IDA de Rabin).

(5) Um esquema de comprometimento probabilístico, o qual pode incluir um par de algoritmos, Ct e Vf, denominados o algoritmo de validação e o algoritmo de verificação. O algoritmo de validação Ct pode ser um algoritmo probabilístico que toma uma cadeia N para validar e retorna um valor de validação, H (a cadeia que um participante pode utilizar para comprometer a M) e também um valor de não-validação, R (a cadeia que um participante pode utilizar para descomprometer à validação H para M). O algoritmo de validação pode ser probabilístico e, como tal, pode tomar um argumento final, R*, o qual é referido como as moedas do algoritmo. Estas moedas podem ser anteriormente geradas por uma chamada para um gerador de números randômicos ou pseudorrandômicos, Rand. A notação "Ct(M; R*)" é algumas vezes aqui utilizada para indicar explicitamente o valor de

retorno do algoritmo de validação Ct na entrada M com moedas randômica R*. O algoritmo de verificação, Vf, pode ser um algoritmo determinístico que toma três cadeias de entrada: um valor de validação H, uma cadeia M, e um valor de não-validação R. Este algoritmo pode retornar um bit 0 ou 1, com 0 indicando que a não-validação é inválida (não convincente) e um indicando que a não-validação é válida (convincente).

Em geral, um esquema de comprometimento pode satisfazer duas propriedades: uma propriedade de ocultação e uma propriedade de ligação. A propriedade de ocultação impõe que, dada uma validação H randomicamente determinada para uma mensagem adversariamente escolhida M_0 ou M_1, o adversário é incapaz de determinar a qual mensagem H a validação corresponde. A propriedade de ligação impõe que um adversário, tendo comprometido a uma mensagem M_0 por meio de uma validação H_0 e uma não-validação R_0 correspondente, é incapaz de encontrar qualquer mensagem M_1 distinta de M_0 e qualquer não-validação R_1 tal que $Vf(H_0, M_1, R_1) = 1$. Na maioria dos casos, o valor de não-validação R produzido por um esquema de comprometimento Ct (M; R*) é precisamente as moedas randômicas R* providas para o algoritmo (isto é, R = R*). No entanto, esta propriedade não é requerida em todos os casos. Os esquemas de comprometimento probabilístico mais naturais podem ser obtidos por meio de funções hash criptográficas adequadas, tais como SHA-1. Existe uma variedade de técnicas naturais para processar o valor ao qual está sendo comprometido, M, e as moedas, R*, antes de aplicar as funções hash criptográficas. Qualquer esquema de comprometimento que contém um mecanismo de comprometimento Ct e um algoritmo de verificação Vf pode gerar um mecanismo de comprometimento Commit e um mecanismo de verificação Verify que aplicam-se a vetores de cadeias ao invés de cadeias individuais. O algoritmo de comprometimento Commit pode aplicar o algoritmo de Ct no sentido do componente, e o algoritmo de verificação Verify pode aplicar o algoritmo de Vf no sentido do componente. Para Ct, moedas randômicas separadas podem ser utilizadas para cada cadeia de componentes em algumas modalidades.

A Figura 8 mostra um diagrama de blocos simplificado do meca-

nismo de compartilhamento do esquema de RCSS de acordo com uma modalidade da invenção. O segredo, S, 800 pode incluir o segredo que o negociante deseja distribuir ou compartilhar. O segredo 800 pode ser um arquivo em um sistema de arquivos, uma mensagem que surge em um protocolo de comunicações, ou qualquer outra porção de dados reservados. O segredo 800 pode ser representado como qualquer cadeia codificada adequada (por exemplo, uma cadeia codificada binária ou ASCII). Em implementações reais, no entanto, as cadeias binárias podem ser utilizadas como o segredo 800 para facilidade de implementação. O segredo S pode ser primeiramente criptografado utilizando o algoritmo de criptografia 803 de um esquema de criptografia de chave compartilhada para obter um texto cifrado C 804. A chave K 802 para executar esta criptografia pode ser obtida utilizando a saída do gerador de números randômicos ou pseudorrandômicos 801 de modo a produzir o número apropriado de bits randômicos ou pseudorrandômicos para a chave 802.

A chave 802 pode ser utilizada para somente um compartilhamento, e portanto pode ser referida como uma chave de uma vez. Além de ser utilizada para criptografar o segredo 800, a chave 802 pode também ser compartilhada ou distribuída utilizando um esquema de compartilhamento de segredo perfeito (PSS) 806. O esquema de PSS 806 pode incluir qualquer esquema de compartilhamento de segredo perfeito, incluindo os esquemas de compartilhamento de segredo de Shamir ou de Blakley. O esquema de compartilhamento de segredo perfeito 806 pode ser randomizado, requerendo a sua própria fonte de bits randômicos (ou pseudorrandômicos). Os bits randômicos ou pseudorrandômicos podem ser providos por um gerador de números randômicos ou pseudorrandômicos separado, tal como o gerador de números 805. O esquema de PSS 806 pode emitir um vetor de compartilhamentos de chave K = K[1], ..., K[n] 808 o qual, conceitualmente, pode ser enviado para os diferentes "participantes", um compartilhamento por participante. Primeiramente, no entanto, os compartilhamentos de chave podem ser combinados com informações adicionais em algumas modalidades. O texto cifrado C 804 pode ser dividido em blocos 809 utilizando o algoritmo de dispersão de informações (IDA) 807, tal como o mecanismo de IDA de Ra-

bin. O IDA 807 pode emitir um vetor de blocos de texto cifrado C[1], ..., C[n] 809. Então, o mecanismo de comprometimento 812 de um esquema de comprometimento probabilístico pode ser empregado. Um número suficiente de bits randômicos é gerado para o processo de comprometimento utilizando o gerador de números randômicos ou pseudorrandômicos 810, e a cadeia randômica 811 resultante é utilizada para todas as validações no mecanismo de comprometimento 812. O mecanismo de comprometimento 812 pode determinar um valor de validação H[i] e um valor de não-validação R[i], coletivamente mostrados no vetor 813, para cada mensagem M[i] = K[i] C[i] (dispersa através de 808 e 809). O i^{o} compartilhamento (o qual não está explicitamente representado na Figura 8) pode codificar K[i] 808, C[i] 809, R[i], e H[1], ..., H[n] 813. Cada participante i pode receber no seu compartilhamento a validação H[j] para cada K[j], C[j] (para j em 1 ... n) e não simplesmente a validação para o seu próprio compartilhamento.

A Figura 9 mostra o processo de comprometimento ilustrativo do mecanismo de comprometimento 812 (Figura 8) em mais detalhes. O processo de comprometimento impõe n diferentes chamadas para o mecanismo de Ct de nível mais baixo do esquema de comprometimento. A randomicidade é gerada pelo gerador de números randômicos ou pseudorrandômicos 900 e a cadeia randômica ou pseudorrandômica R* resultante é particionada em n segmentos, R*[1], R*[2], ... R*[n] 901. A i^{a} porção da randomicidade (uma das porções 921, 922, ou 923 quando i é 1, 2, ou n) é utilizada para comprometer com a i^{a} mensagem que está sendo comprometida, M[i] = K[i] C[i] (mostrada como as mensagens 910, 911, 912) utilizando os algoritmos de comprometimento Ct 931, 932, e 933 de um esquema de comprometimento. Pares de validação e não-validação 941, 942, e 943 podem ser emitidos pelo algoritmo de CT. É provável que cada R[i] é simplesmente R*[i], mas isto não é estritamente requerido ou assumido.

O algoritmo identificado "Share" na Tabela 1, abaixo, explica adicionalmente o esquema de compartilhamento apresentado nas Figuras 8 e 9. Este algoritmo toma como entrada uma cadeia S, o segredo que deve ser compartilhado. Na linha 10, um número suficiente de lançamentos de moeda

randômica é gerado para prover uma chave de criptografia K para um esquema de criptografia simétrico que consiste nos algoritmos Encrypt e Decrypt. Na linha 11, a cadeia reservada S que deve ser compartilhada é criptografada utilizando a chave K de modo a criar um texto cifrado C. A criptografia pode ser randomizada, mas não precisa ser para o mecanismo funcionar corretamente. A seguir, na linha 12, o algoritmo de compartilhamento de um esquema de compartilhamento de segredo perfeito (tal como o esquema de Shamir) pode ser invocado. O algoritmo de compartilhamento é probabilístico, apesar disto não estar explicitamente indicado no código. Os resultados de compartilhamento em um vetor de compartilhamentos de chave, K = K[i], ..., K[n]. Na linha 13, o texto cifrado C pode ser dividido em uma coleção de blocos dos quais uma subcoleção de blocos autorizada será adequada para recuperar o segredo. Isto pode ser executado utilizando o algoritmo de compartilhamento de um IDA (por exemplo, o IDA 807 da Figura 8). Qualquer IDA válido pode ser utilizado, tal como o mecanismo de Rabin, uma replicação, ou qualquer esquema ad hoc com a propriedade de IDA anteriormente descrito. As linhas 15 e 16 compreendem um comprometimento probabilístico da mensagem KC[i] = K[i] C[i], com as moedas necessárias sendo geradas na linha 15 e a validação H[i] e a não-validação R[i] sendo computadas utilizando estas moedas. A linha 17 computa o compartilhamento resultante (algumas vezes aqui referido como "fragmento") S[i] dos valores já computados. O compartilhamento no esquema de RCSS em assunto é S[i] = R[i] K[i] C[i] H[1] ... H[n]. Os compartilhamentos podem então ser retornados para o chamador, para serem armazenados em diferentes locais ou transmitidos por uma variedade de canais, de acordo com a intenção do chamador.

O algoritmo de recuperação do esquema de RCSS está também mostrado na Tabela 1, abaixo. Desta vez, o chamador provê um vetor inteiro de compartilhamentos pretendidos, S = S[1] ... S[n]. Cada compartilhamento pretendido S[i] pode ser uma cadeia ou o símbolo distinguido "◊", o que novamente significa um compartilhamento faltante. Pode também ser assumido, em algumas modalidades, que o chamador provê a identidade de um compartilhamento j, onde j está entre 1 e n inclusive, o qual é conhecido ser

válido. Nas linhas 20-21, cada S[i] pode ser decomposto em suas cadeias componentes R[i] K[i] C[i] H[1] ... H[n]. É compreendido que o símbolo faltante, "◊", pode decompor em componentes todos os quais são estes mesmos o símbolo faltante ◊. Na linha 23, o algoritmo de verificação do esquema de comprometimento pode ser executado para determinar se a mensagem KC[i] = K[i] C[i] parece ser válida. O compartilhamento j "conhecido ser válido" pode então ser utilizado como o "valor de referência" para cada comprometimento $H_j[i]$. Sempre que um valor de K[i] C[i] parece ser inválido, este pode ser substituído pelo símbolo faltante. O vetor de valores de K[i] que foram assim revisados pode agora ser suprido o algoritmo de recuperação do esquema de compartilhamento de segredo na linha 25, enquanto que o vetor de valores de C[i] revisados pode ser suprido para o algoritmo de recuperação do IDA na linha 26. Neste ponto, precisa-se somente decifrar o texto cifrado C recuperado do IDA sob a chave K recuperada do esquema de PSS para conseguir o valor S que é recuperado pelo próprio esquema de RCSS.

```
Algorithm Share (S)
10  K ← Rand(k)
11  C ← Encrypt_K(S)
12  K ← Share^PSS(K)
13  C ← Share^IDA(C)
14  for i←1 to n do
15      R*[i] ← Rand(k')
16      (H[i], R[i]) ← Ct(K[i]C[i]; R*[i])
17      S[i] ← R[i]K[i] C[i] H[1] ... H[n]
18  return S

Algorithm Recover (S, j)
20  for i←1 to n do
21      R[i]K[i] C[i] H_j[1] ... H_j[n] ← S[i]
22  for i←1 to n do
23      if S[i] ≠ ◊ and Vf(H_j[i], K[i]C[i], R[i])
24          then K[i] ← ◊, C[i] ← ◊
25  K ← Recover^PSS(K)
26  C ← Recover^IDA(C)
27  S ← Decrypt_K(C)
28  return S
```

Tabela 1: mecanismos de Share e Recover do esquema de RCSS

Como acima indicado o algoritmo Recover da Tabela 1 assume que o usuário supre a localização de um compartilhamento conhecido ser válido. Na ausência disto, outros meios podem ser empregados para determinar um valor de consenso para H[i]. A possibilidade mais natural utilizada em algumas modalidades é o voto de maioria. Por exemplo, no lugar de $H_j[i]$ na linha 23 um valor de H[i] pode ser utilizado que ocorre mais frequentemente entre os valores de $H_j[i]$ recuperados, para j variando de 1 a n.

Retornando brevemente à Figura 8, a porção da figura que está identificada 801 até 807 pode ser implementada ou considerada como um único processo que inclui um compartilhamento de segredo computacional (CSS) de S para obter o vetor de compartilhamentos KC = (KC[1], ..., KC[n]) onde KC[i] = K[i] C[i], com uma validação probabilística aplicada ao vetor de compartilhamentos resultante. A Figura 10 mostra um esquema descrito desta modalidade alternativa. Nesta modalidade, os três primitivos seguintes são empregados, ao invés dos cinco primitivos anteriores definidos em conexão com as Figuras 8 e 9: (1) um gerador de números randômicos ou pseudorrandômicos, Rand; (2) um esquema de compartilhamento de segredo computacional (CSS); e (3) um esquema de comprometimento probabilístico.

O gerador de números randômicos ou pseudorrandômicos, Rand, pode ser definido como anteriormente. O esquema de compartilhamento de segredo computacional pode incluir um par de algoritmos $Share^{CSS}$ e $Recover^{CSS}$. O primeiro destes algoritmos, conhecido como o algoritmo de compartilhamento do CSS, pode ser um mapa probabilístico que toma como entrada uma cadeia K, denominada o segredo, e retorna uma sequência de n cadeias, K[1], ..., K[n], referidas como compartilhamentos. Cada K[i] pode incluir um compartilhamento ou os n compartilhamentos que foram negociados, ou distribuídos, pelo negociante (a entidade que executa o processo de compartilhamento). O número n pode ser um parâmetro do esquema de compartilhamento de segredo, e este pode ser um número positivo arbitrário. O algoritmo de compartilhamento pode ser probabilístico pelo fato de que este pode empregar bits randômicos ou pseudorrandômicos. Tal dependên-

cia pode ser realizada provendo os bits randômicos ou pseudorrandômicos de algoritmo de compartilhamento, como providos pelo gerador de números randômicos ou pseudorrandômicos, Rand.

O segundo algoritmo, conhecido como o algoritmo de recuperação do CSS, toma como entrada um vetor de n cadeias referidas como os compartilhamentos pretendidos. Cada compartilhamento pretendido é ou uma cadeia ou um símbolo distinguido "◊", o qual é lido como faltante e é utilizado para indicar que algum compartilhamento específico está indisponível ou é desconhecido. O algoritmo de recuperação para o esquema de compartilhamento de segredo computacional pode retornar uma cadeia S, o segredo recuperado. Como o par de algoritmos compõe um esquema de compartilhamento de segredo computacional, duas propriedades podem ser assumidas. A primeira propriedade, a propriedade de privacidade, pode assegurar que nenhum conjunto de usuários não-autorizados obtenha nenhuma informação significativa (computacionalmente extraível) sobre o segredo que foi compartilhado de seus compartilhamentos. A segunda propriedade, a propriedade de recuperabilidade, assegura que um conjunto de participantes autorizados pode sempre recuperar o segredo, assumindo que os participantes autorizados contribuam compartilhamentos corretos para o algoritmo de recuperação e que nenhum participante adicional contribua ou um compartilhamento correto ou então o valor faltante distinguido ("◊").

A terceira primitiva nesta modalidade é um esquema de comprometimento probabilístico, o qual pode ser implementado como acima descrito em conexão com as Figuras 8 e 9.

Referindo à Figura 10, a cadeia de segredo S 1000 pode ser compartilhada ou distribuída, utilizando o algoritmo Share 1001 de um esquema de compartilhamento de segredo computacional (probabilístico). Isto pode resultar em n compartilhamentos, KC[1], ..., KC[n] 1002. O esquema de comprometimento probabilístico 1005 pode então ser empregado para obter o vetor 1006 de validações e não-validações. A validação probabilística pode empregar lançamentos de moeda 1004 gerados por algum gerador de números randômicos ou pseudorrandômicos 1003. O compartilhamento 1 do

esquema de RCSS, S[1], pode incluir o compartilhamento KC[1] do esquema de CSS 1002 juntamente com a não-validação R[1] do esquema de comprometimento 1006 juntamente com o vetor de validações H[1] ... H[n] do esquema de comprometimento 1006. O compartilhamento 2 do esquema de RCSS, S[2], pode incluir o compartilhamento KC[2] do esquema de CSS 1002 juntamente com a não-validação R[2] do esquema de comprometimento 1006 juntamente com o vetor de validações H[1] ... H[n] do esquema de comprometimento 1006. Este processo pode continuar, com o compartilhamento n do esquema de RCSS, S[n], que inclui o compartilhamento KC[n] do esquema de CSS 1002 juntamente com a não-validação R[n] do esquema de comprometimento 1006 juntamente com o vetor de validações H[1] ... H[n] do esquema de comprometimento 1006.

A Figura 11 ilustra o processo de recuperação do esquema RCSS apenas descrito. O algoritmo Recover 1130 está provido de um vetor de compartilhamentos pretendidos, os quais são algumas vezes aqui denominados fragmentos, para distinguir estes compartilhamentos dos compartilhamentos do esquema de CSS. O iº fragmento recebido pelo algoritmo Recover 1130 é decomposto para formar uma cadeia KC[i],um valor de não-validação R[i], e um vetor de validações $H_i = H_i[1] \ldots H_i[n]$. Da coleção de vetores de validações $H_1[i] \ldots H_n[i]$, o algoritmo Recover 1130 deve determinar uma validação de consenso H[i]. Para o ambiente no qual o algoritmo Recover 1130 está provido um índice j para um participante cujo compartilhamento é conhecido ser válido, o valor de consenso H[i] pode ser selecionado para ser $H_j[i]$. Para o caso onde nenhum tal compartilhamento é conhecido ser autêntico, o valor de consenso pode ser selecionado como um valor de cadeia que ocorre mais frequentemente entre $H_1[i] \ldots H_n[i]$. A Figura 11 apresenta os compartilhamentos KC[1] 1100, KC[2] 1110, e KC[n] 1120 decompostos do 1º, 2º, e nº fragmentos providos para o algoritmo Recover de RCSS, respectivamente. O exemplo mostrado na Figura 11 do mesmo modo apresenta os valores de não-validação R[1] 1102, R[2] 1112, e R[n] 1122 decompostos do 1º, 2º, e nº fragmentos providos para o algoritmo Recover de RCSS, respectivamente. A Figura 11 também apresenta os valores

de validação de consenso H[1] 1101, H[2] 1111, e H[n] 1121, determinados no modo acima descrito. Focalizando no processamento do primeiro fragmento, o algoritmo de verificação Vf 1104 do esquema de comprometimento probabilístico é chamado na validação H[1], na mensagem KC[1], e na não-validação R[1]. O algoritmo pode retornar um bit, com, por exemplo, 0 indicando que a mensagem KC[1] não deve ser aceita como tendo sido não-validada, e 1 indicando que esta deve. Consequentemente, a um demultiplexador 1106 é alimentado o bit de decisão do algoritmo de verificação, com, por exemplo, um 0 indicando que o valor recuperado deve ser considerado como faltante ("◊") 1105 e um 1 indicando que o valor recuperado deve ser considerado como o próprio KC[1] 1100. A saída A é a primeira entrada suprida para o algoritmo Recover 1130 de um esquema de CSS. Continuando deste modo, o fragmento 2 é processado (mostrado em 1110-1116 no exemplo da Figura 11) e cada fragmento adicional é processado, até que o enésimo seja processado (mostrado em 1120-1126 no exemplo da Figura 11). A coleção de compartilhamentos é então provida para o algoritmo Recover 1130 do esquema de CSS de modo a recuperar o segredo. Este valor recuperado pode ser o valor emitido pelo próprio esquema de RCSS.

Aqueles versados na técnica perceberão que um grande número de variantes é possível. Por exemplo, um código de correção de erro pode ser utilizado em algumas modalidades para prover uma coleção adequada de validações H[1] ... H[n] para cada participante, efetivamente substituindo o código de replicação simples mas um tanto ineficiente da modalidade anterior.

Apesar de alguns aplicativos comuns serem acima descritos, deve ser claramente compreendido que a presente invenção pode ser integrada com qualquer aplicativo de rede de modo a aumentar a segurança, a tolerância a falhas, o anonimato, ou qualquer combinação adequada dos acima.

Além disso, outras combinações, adições, substituições e modificações serão aparentes para aqueles versados na técnica em vista da descrição aqui. Consequentemente, a presente invenção não pretende ser limitada pela reação das modalidades preferidas mas deve ser definida por uma referência às reivindicações anexas

REIVINDICAÇÕES

1. Método para proteger dados pela geração de uma coleção de fragmentos dos dados, o método compreendendo:

aplicar um mecanismo de compartilhamento de um esquema de compartilhamento de segredo computacional aos dados para produzir uma coleção de compartilhamentos;

gerar um valor randômico ou pseudorrandômico;

computar um conjunto de valores de validação e um conjunto de valores de não-validação do valor randômico ou pseudorrandômico e da coleção de compartilhamentos;

produzir cada fragmento na coleção de fragmentos pela combinação de um compartilhamento, um valor de não-validação, e pelo menos um valor de validação do conjunto de valores de validação; e

armazenar cada fragmento em pelo menos um repositório de dados.

2. Método de acordo com a reivindicação 1, em que produzir cada fragmento na coleção de fragmentos compreende combinar um compartilhamento, um valor de não-validação e o conjunto inteiro de valores de validação.

3. Método de acordo com a reivindicação 1, em que armazenar cada fragmento em pelo menos um repositório de dados compreende armazenar cada fragmento em diferentes localizações geográficas.

4. Método de acordo com a reivindicação 1, em que armazenar cada fragmento em pelo menos um repositório de dados compreende armazenar cada fragmento em diferentes localizações físicas no pelo menos um repositório.

5. Método de acordo com a reivindicação 1, em que o pelo menos um repositório de dados compreende um sistema de arquivo distribuído.

6. Método de acordo com a reivindicação 1, em que o esquema de compartilhamento de segredo computacional é selecionado do grupo que consiste em esquemas de compartilhamento de segredo de Shamir, Blakley, e Krawczyk.

7. Método de acordo com a reivindicação 1, em que computar um conjunto de valores de validação e um conjunto de valores de não-validação compreende empregar um esquema de comprometimento probabilístico.

8. Método de acordo com a reivindicação 1, ainda compreendendo transmitir os fragmentos produzidos por uma pluralidade de canais de comunicação.

9. Método de acordo com a reivindicação 8, em que transmitir os fragmentos produzidos por uma pluralidade de canais de comunicação compreende transmitir cada fragmento produzido por um canal de comunicação diferente.

10. Método para proteger dados pela geração de uma coleção de fragmentos dos dados, o método compreendendo:

aplicar um mecanismo de compartilhamento de um esquema de compartilhamento de segredo computacional aos dados para produzir uma coleção de compartilhamentos;

utilizar um esquema de comprometimento probabilístico para computar um conjunto de valores de validação e um conjunto de valores de não-validação da coleção de compartilhamentos;

produzir uma pluralidade de fragmentos, em que cada fragmento compreende um compartilhamento da coleção de compartilhamentos, um valor de não-validação do conjunto de valores de não-validação, e o conjunto de valores de validação; e

armazenar cada fragmento em pelo menos um repositório de dados.

11. Método de acordo com a reivindicação 10, em que armazenar cada fragmento em pelo menos um repositório de dados compreende armazenar cada fragmento em diferentes localizações geográficas.

12. Método de acordo com a reivindicação 10, em que armazenar cada fragmento em pelo menos um repositório de dados compreende armazenar cada fragmento em diferentes localizações físicas no pelo menos um repositório.

13. Método de acordo com a reivindicação 10, em que o pelo menos um repositório de dados compreende um sistema de arquivo distribuído.

14. Método de acordo com a reivindicação 10, em que o esquema de compartilhamento de segredo computacional é selecionado do grupo que consiste em esquemas de compartilhamento de segredo de Shamir, Blakley, e Krawczyk.

15. Método de acordo com a reivindicação 10, ainda compreendendo transmitir os fragmentos produzidos por uma pluralidade de canais de comunicação.

16. Método de acordo com a reivindicação 15, em que transmitir os fragmentos produzidos por uma pluralidade de canais de comunicação compreende transmitir cada fragmento produzido por um canal de comunicação diferente.

17. Método para proteger dados, que compreende:

gerar uma chave criptográfica;

criptografar os dados com a chave criptográfica para criar um texto cifrado;

produzir uma coleção de n compartilhamentos de chave para aplicar um esquema de compartilhamento de segredo na chave criptográfica;

produzir uma coleção de n blocos de textos cifrados pela aplicação de um algoritmo de dispersão de informações no texto cifrado;

computar n valores de validação e n valores de não-validação pela aplicação de um esquema de comprometimento probabilístico a cada um dos n compartilhamentos de chave e n blocos de textos cifrados;

produzir n fragmentos de dados, em que cada fragmento de dados é uma função de um compartilhamento de chave, um bloco de textos cifrados, um valor de não-validação, e os valores de validação; e

armazenar os n fragmentos de dados em diferentes dispositivos de armazenamento lógicos, por meio de que os dados são recuperáveis de um número predefinido dos fragmentos de dados.

18. Método de acordo com a reivindicação 17, em que armaze-

nar os n fragmentos de dados em diferentes dispositivos de armazenamento lógicos compreende armazenar os n fragmentos de dados em n diferentes dispositivos de armazenamento lógicos.

19. Método de acordo com a reivindicação 17, ainda compreendendo transmitir os n fragmentos de dados por n canais de comunicação antes de armazenar os n fragmentos de dados.

20. Método para recuperar os dados de uma coleção de compartilhamentos supostos, que compreende:

receber um compartilhamento suposto designado da coleção de compartilhamentos supostos, em que o compartilhamento suposto designado é declarado ser válido;

separar cada compartilhamento suposto em uma porção de conteúdo e um vetor de somas de verificação;

utilizar o vetor de somas de verificação associado com o compartilhamento suposto designado para classificar cada compartilhamento da coleção de compartilhamentos supostos como um compartilhamento real ou como um compartilhamento fictício; e

aplicar o algoritmo de recuperação de um esquema de compartilhamento de segredo computacional nos compartilhamentos classificados como compartilhamentos reais para recuperar os dados.

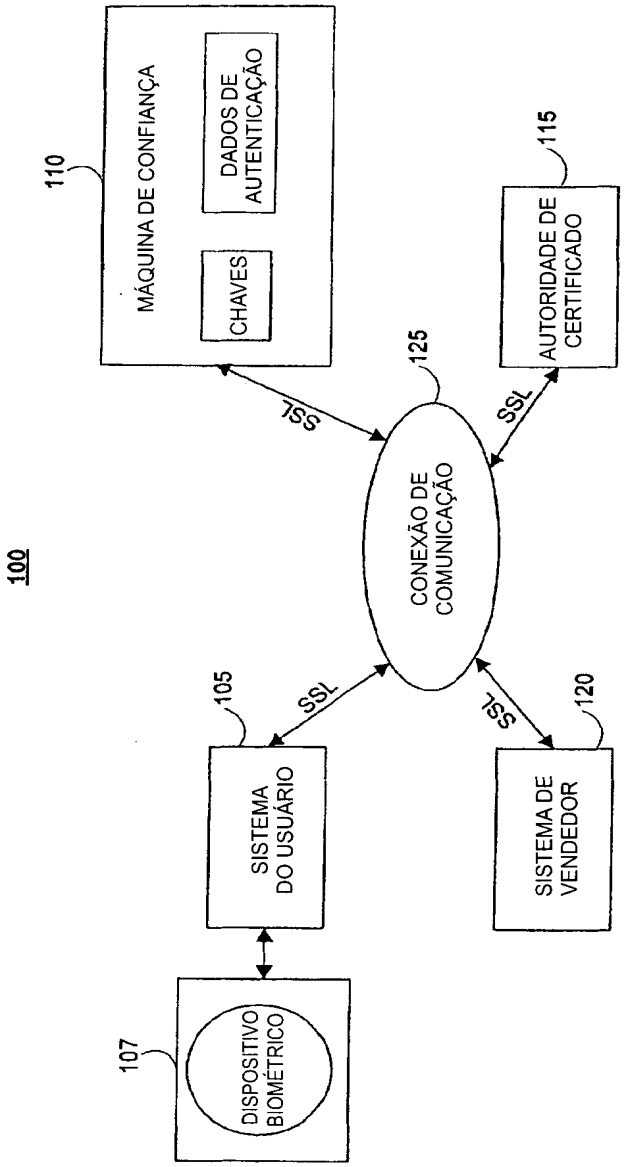

100
110
MÁQUINA DE CONFIANÇA
CHAVES
DADOS DE AUTENTICAÇÃO
115
AUTORIDADE DE CERTIFICADO
125
CONEXÃO DE COMUNICAÇÃO
SSL
SSL
SSL
SSL
105
SISTEMA DO USUÁRIO
120
SISTEMA DE VENDEDOR
107
DISPOSITIVO BIOMÉTRICO

FIG. 1

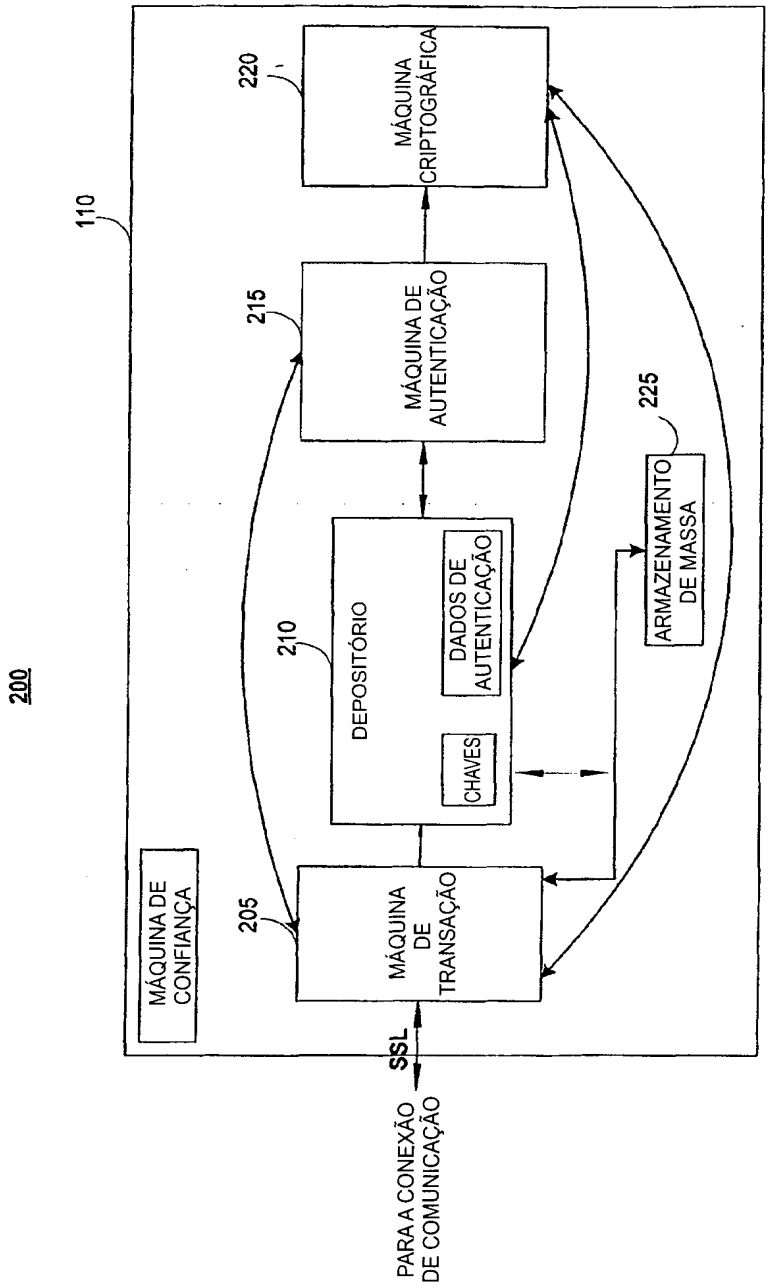

200
110
MÁQUINA DE CONFIANÇA
205
MÁQUINA DE TRANSAÇÃO
210
DEPOSITÓRIO
CHAVES
DADOS DE AUTENTICAÇÃO
215
MÁQUINA DE AUTENTICAÇÃO
220
MÁQUINA CRIPTOGRÁFICA
225
ARMAZENAMENTO DE MASSA
SSL
PARA A CONEXÃO DE COMUNICAÇÃO

FIG. 2

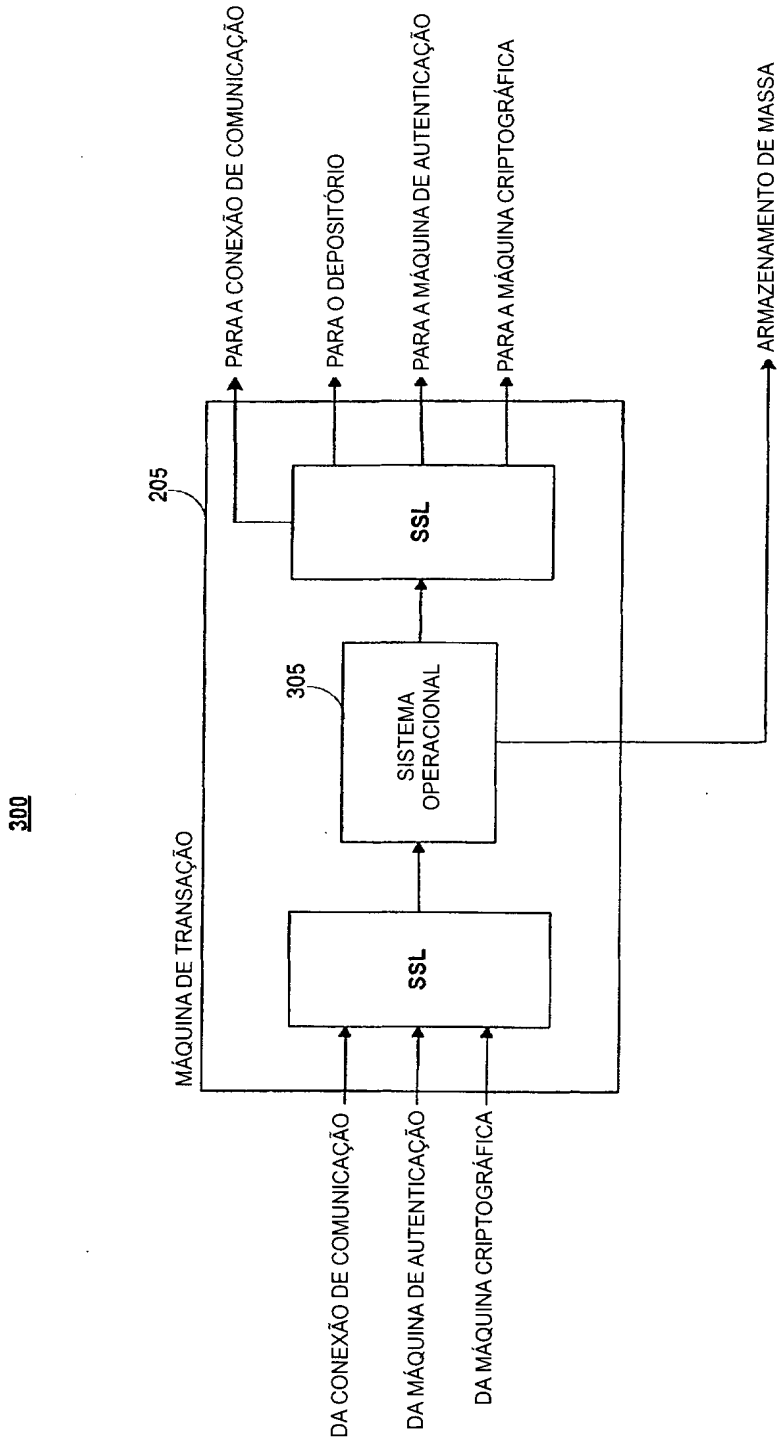

300
MÁQUINA DE TRANSAÇÃO
205
SSL
SSL
305
SISTEMA OPERACIONAL
DA CONEXÃO DE COMUNICAÇÃO
DA MÁQUINA DE AUTENTICAÇÃO
DA MÁQUINA CRIPTOGRÁFICA
PARA A CONEXÃO DE COMUNICAÇÃO
PARA O DEPOSITÓRIO
PARA A MÁQUINA DE AUTENTICAÇÃO
PARA A MÁQUINA CRIPTOGRÁFICA
ARMAZENAMENTO DE MASSA

FIG. 3

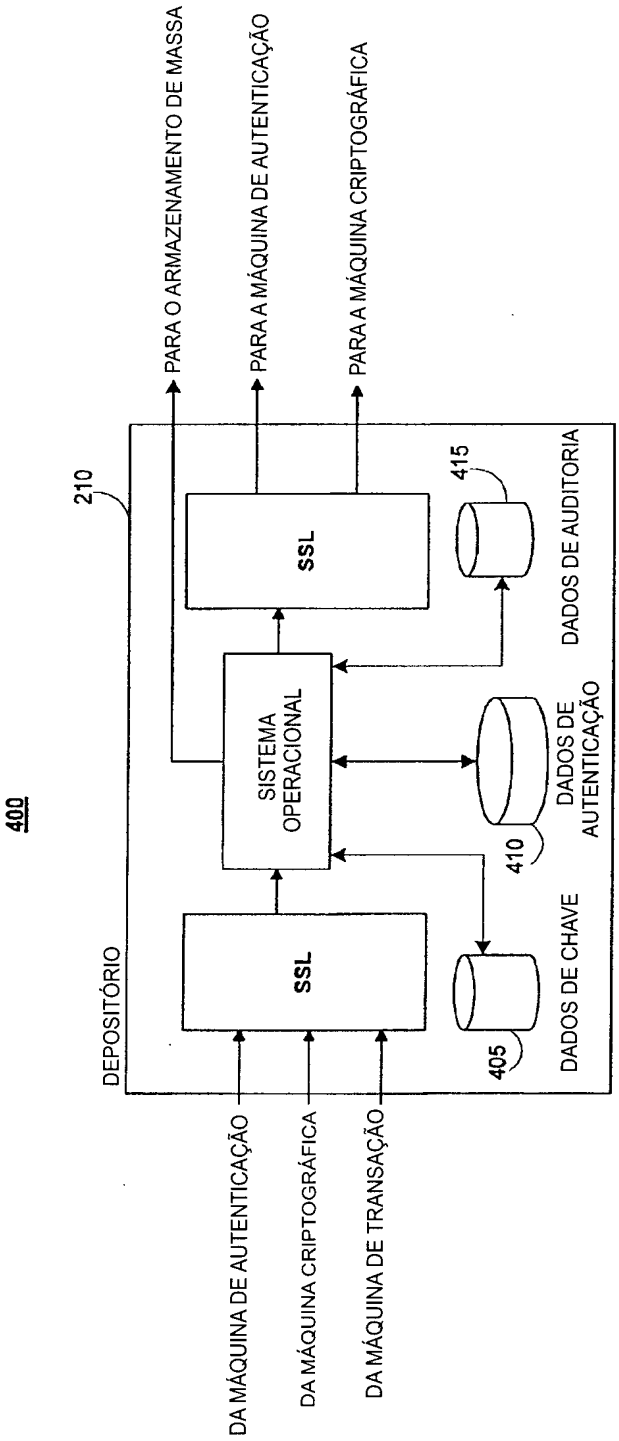

400
210
DEPOSITÓRIO
DA MÁQUINA DE AUTENTICAÇÃO
DA MÁQUINA CRIPTOGRÁFICA
DA MÁQUINA DE TRANSAÇÃO
SSL
SSL
SISTEMA OPERACIONAL
PARA O ARMAZENAMENTO DE MASSA
PARA A MÁQUINA DE AUTENTICAÇÃO
PARA A MÁQUINA CRIPTOGRÁFICA
405
DADOS DE CHAVE
410
DADOS DE AUTENTICAÇÃO
415
DADOS DE AUDITORIA

FIG. 4

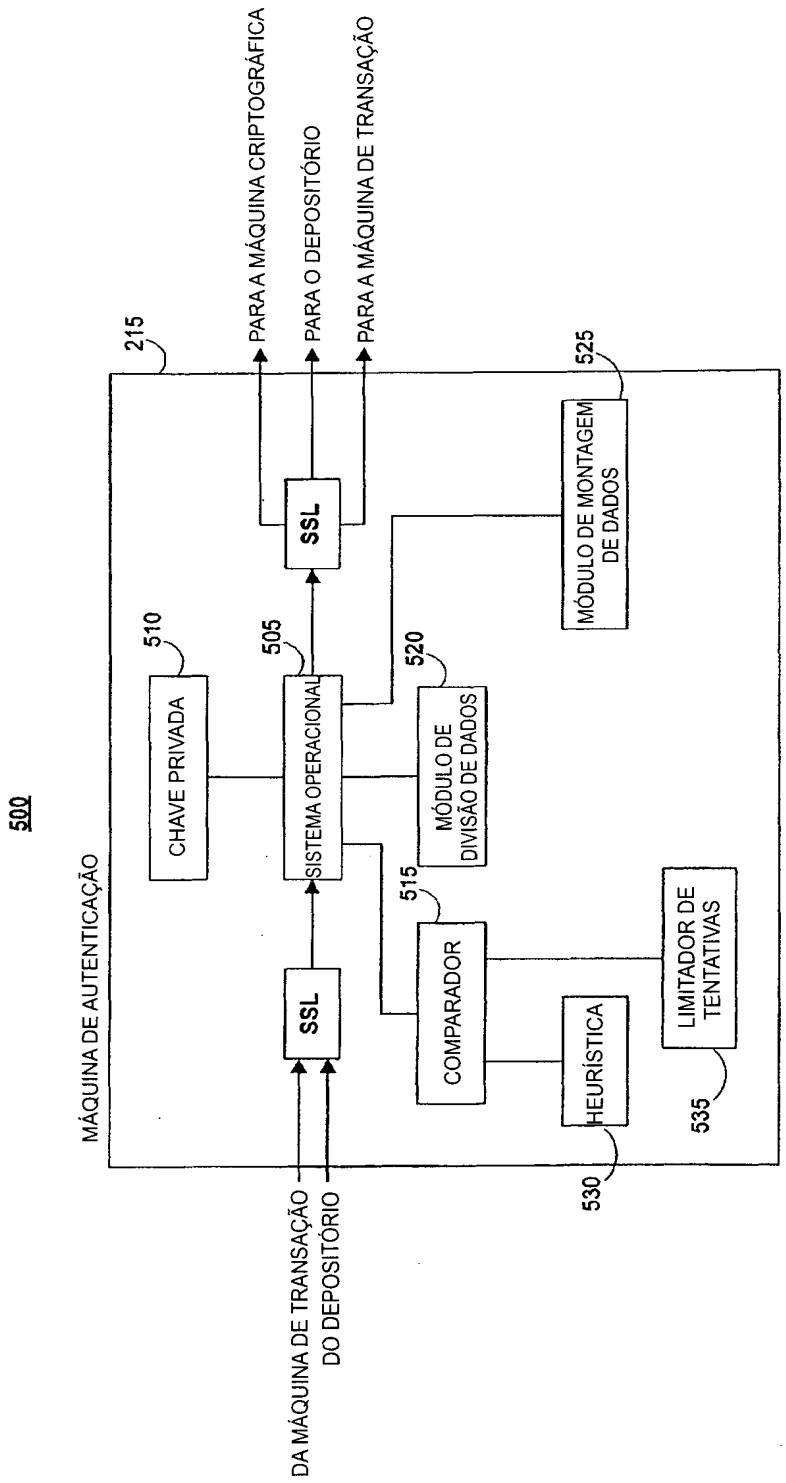

500
MÁQUINA DE AUTENTICAÇÃO
215
CHAVE PRIVADA
510
SISTEMA OPERACIONAL
505
SSL
SSL
MÓDULO DE DIVISÃO DE DADOS
520
MÓDULO DE MONTAGEM DE DADOS
525
COMPARADOR
515
HEURÍSTICA
530
LIMITADOR DE TENTATIVAS
535
DA MÁQUINA DE TRANSAÇÃO DO DEPOSITÓRIO
PARA A MÁQUINA CRIPTOGRÁFICA
PARA O DEPOSITÓRIO
PARA A MÁQUINA DE TRANSAÇÃO

FIG. 5

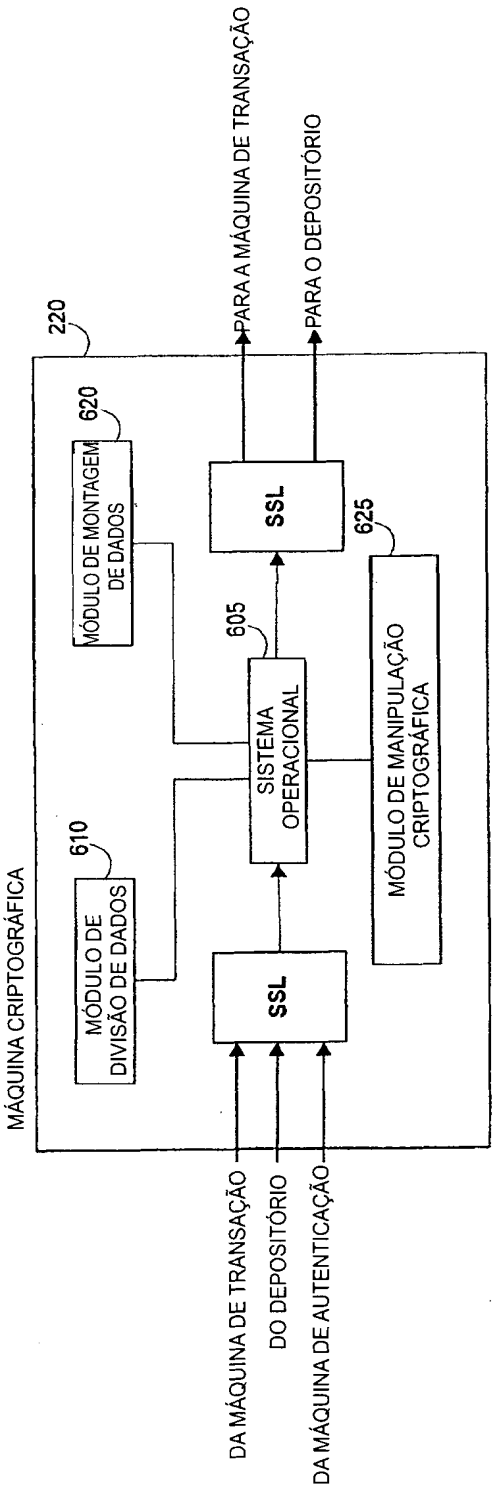

600
MÁQUINA CRIPTOGRÁFICA
220
610
MÓDULO DE DIVISÃO DE DADOS
620
MÓDULO DE MONTAGEM DE DADOS
605
SISTEMA OPERACIONAL
625
MÓDULO DE MANIPULAÇÃO CRIPTOGRÁFICA
SSL
SSL
DA MÁQUINA DE TRANSAÇÃO
DO DEPOSITÓRIO
DA MÁQUINA DE AUTENTICAÇÃO
PARA A MÁQUINA DE TRANSAÇÃO
PARA O DEPOSITÓRIO

FIG. 6

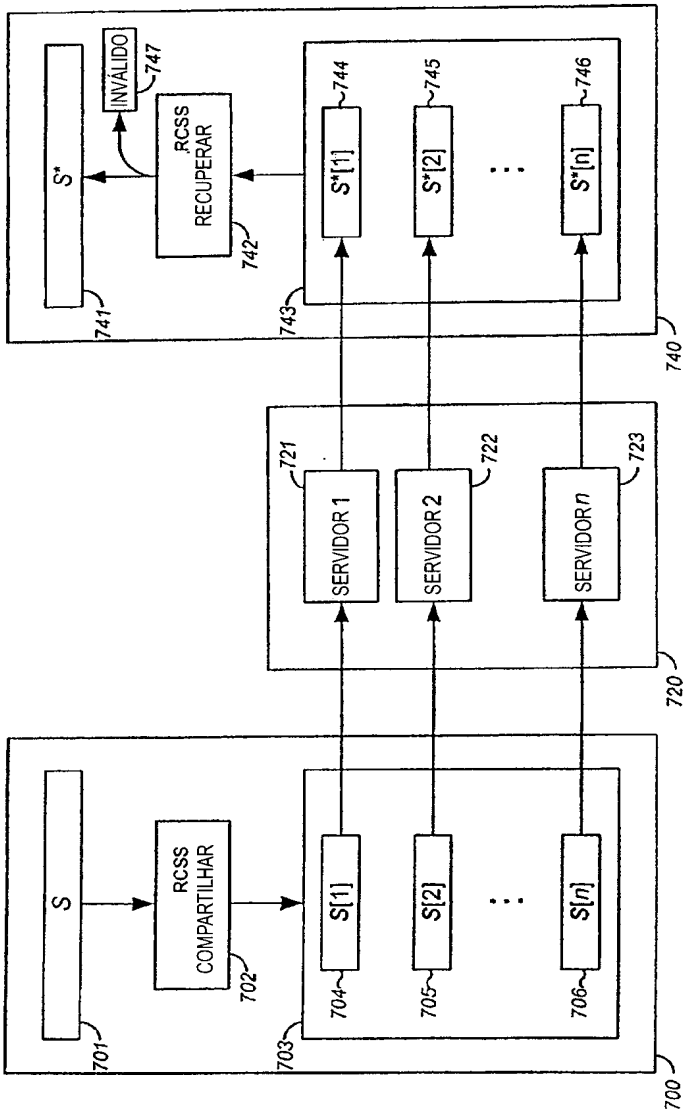

S
RCSS COMPARTILHAR
S[1]
S[2]
S[n]
701
702
703
704
705
706
700
SERVIDOR 1
SERVIDOR 2
SERVIDOR n
721
722
723
720
S*
INVÁLIDO
RCSS RECUPERAR
S*[1]
S*[2]
S*[n]
741
742
743
744
745
746
747
740

Fig 7

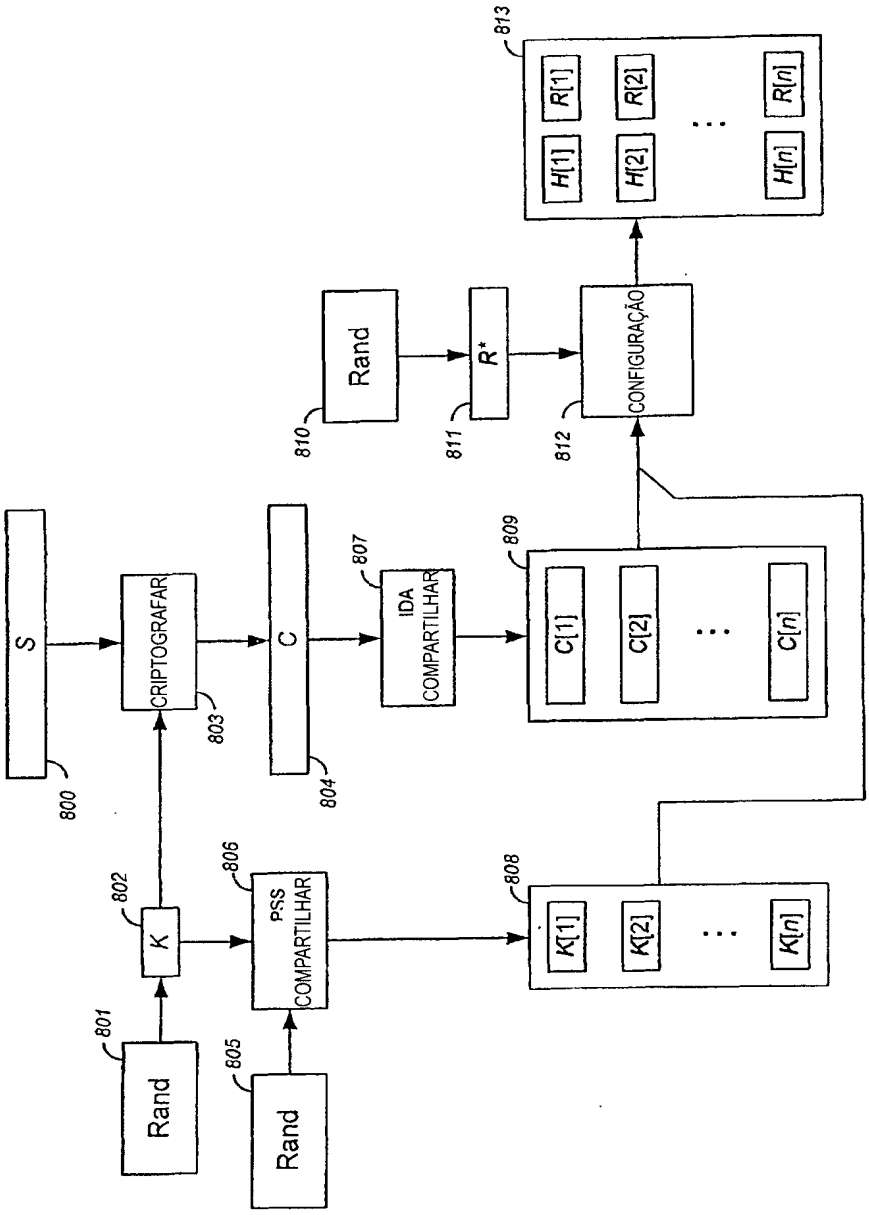

S
800
CRIPTOGRAFAR
803
C
804
IDA
COMPARTILHAR
807
C[1]
C[2]
C[n]
809
Rand
810
R*
811
CONFIGURAÇÃO
812
H[1]
H[2]
H[n]
R[1]
R[2]
R[n]
813
Rand
801
K
802
PSS
COMPARTILHAR
806
Rand
805
K[1]
K[2]
K[n]
808

Fig 8

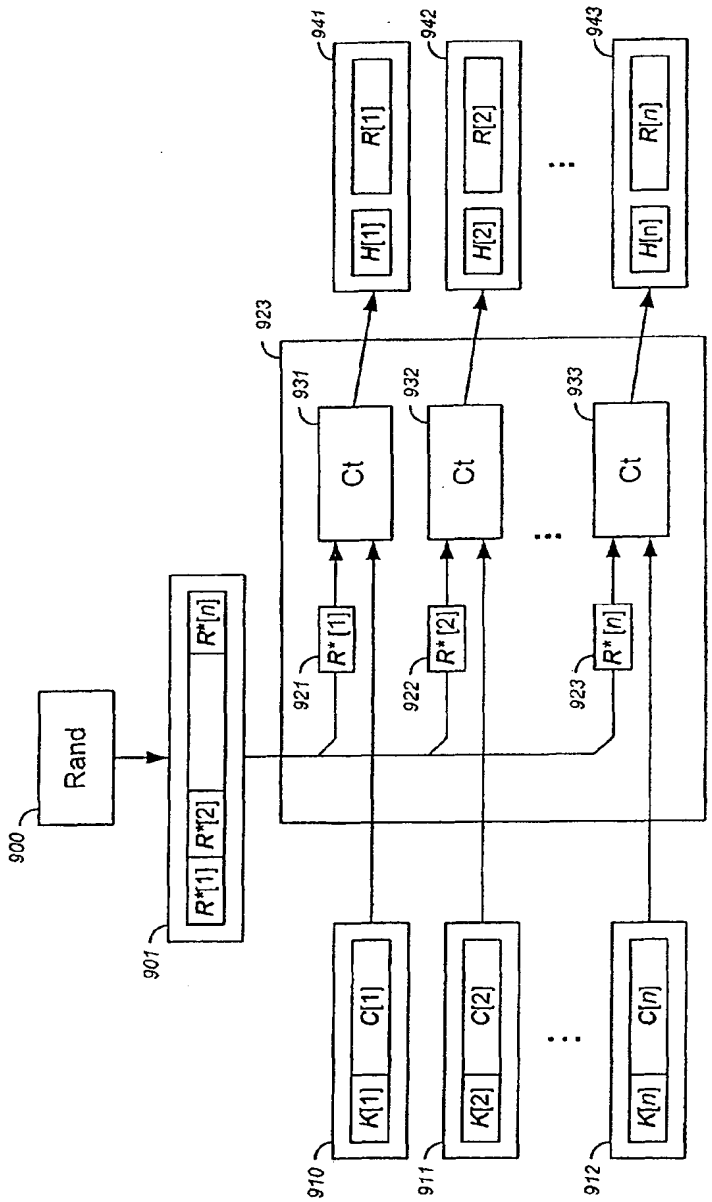

900
Rand
901
R*[1]
R*[2]
R*[n]
910
911
912
K[1]
C[1]
K[2]
C[2]
K[n]
C[n]
923
931
932
933
Ct
Ct
Ct
921
922
923
R*[1]
R*[2]
R*[n]
941
942
943
H[1]
R[1]
H[2]
R[2]
H[n]
R[n]

Fig 9

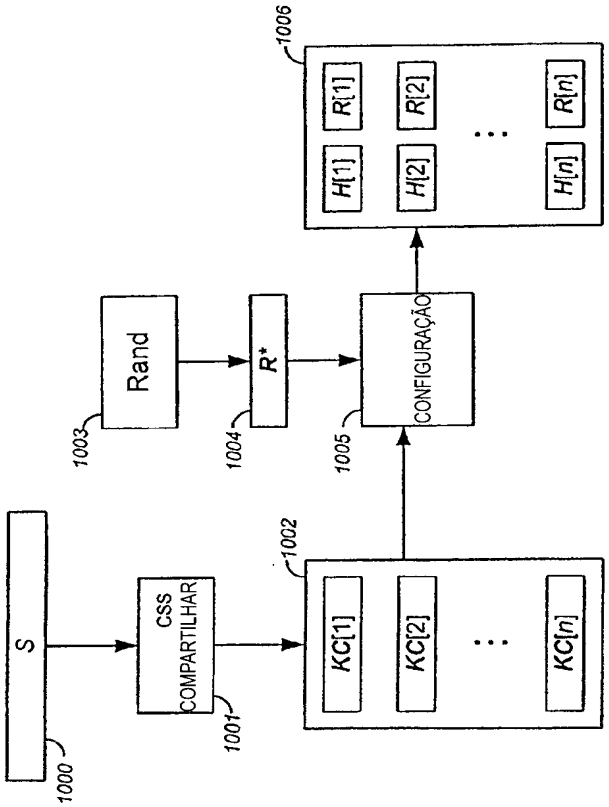

S
1000
CSS
COMPARTILHAR
1001
KC[1]
KC[2]
KC[n]
1002
Rand
1003
R*
1004
CONFIGURAÇÃO
1005
H[1]
H[2]
H[n]
R[1]
R[2]
R[n]
1006

Fig 10

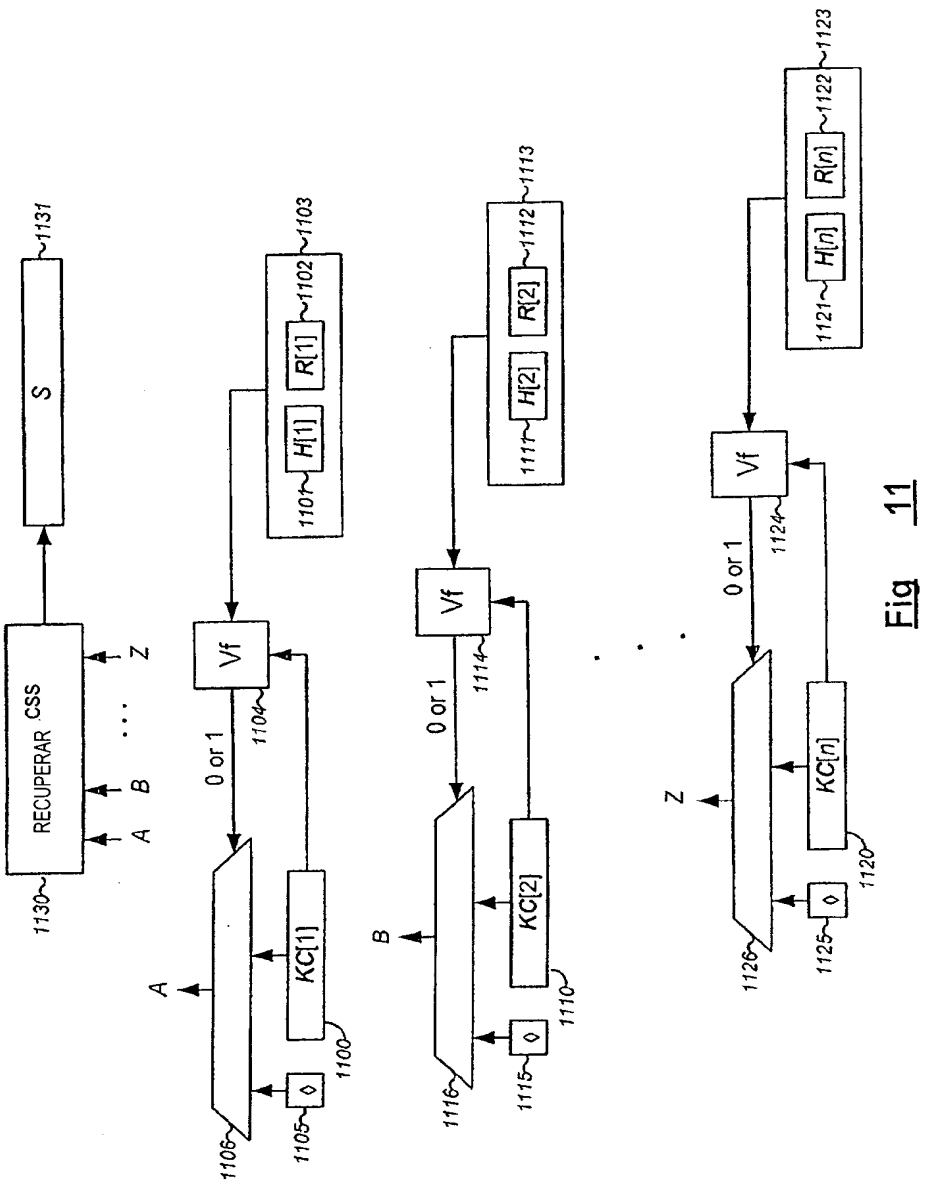

1131
S
1130
RECUPERAR CSS
A
B
Z
1106
1105
0
KC[1]
1100
0 or 1
Vf
1104
1101
H[1]
R[1]
1102
1103
A
1116
1115
0
KC[2]
1110
B
0 or 1
Vf
1114
1111
H[2]
R[2]
1112
1113
Z
1126
1125
0
KC[n]
1120
0 or 1
Vf
1124
1121
H[n]
R[n]
1122
1123

Fig 11

RESUMO

Patente de Invenção: **"SISTEMAS E MÉTODOS PARA DISTRIBUIR E PROTEGER DADOS".**

A presente invenção refere-se a um esquema de compartilhamento de segredo computacional robusto que provê uma distribuição eficiente e uma recuperação subsequente de dados privados. Uma chave criptográfica pode ser randomicamente gerada e então compartilhada utilizando um algoritmo de compartilhamento de segredo para gerar uma coleção de compartilhamentos de chave. Os dados provados podem ser criptografados utilizando a chave, resultando em um texto cifrado. O texto cifrado pode então ser quebrado em fragmentos de texto cifrado utilizando um Algoritmo de Dispersão de Informações. Cada compartilhamento de chave e fragmento de texto cifrado é provido como uma entrada para um método de validação de um esquema de comprometimento probabilístico, resultando em um valor de validação e um valor de não-validação. O compartilhamento para o esquema de compartilhamento de segredo computacional robusto pode ser obtido combinando o compartilhamento de chave, o fragmento de texto cifrado, o valor de não-validação, e o vetor de valores de validação.