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

(11) **PI 0006085-2 B1**

(22) Data do Depósito: 28/04/2000

(45) Data de Concessão: 10/05/2016

(RPI 2366)

(54) Título: SISTEMAS E MÉTODOS DE ASSINATURA DE CHAVE PÚBLICA

(51) Int.Cl.: H04L 9/32

(30) Prioridade Unionista: 29/04/1999 EP 99401048.6

(73) Titular(es): CP8 TECHNOLOGIES

(72) Inventor(es): JACQUES PATARIN, AVIAD KIPNIS, LOUIS GOUBIN

SISTEMAS E MÉTODOS DE ASSINATURA DE CHAVE PÚBLICA

CAMPO DA INVENÇÃO

A presente invenção refere-se em geral à criptografia, e mais particularmente à criptografia de chave pública.

ANTECEDENTES DA INVENÇÃO

O primeiro esquema de criptografia de chave pública foi introduzido em 1975. Desde então, muitos esquemas de chaves públicas foram desenvolvidos e publicados. Muitos esquemas de chave pública necessitam alguns cálculos aritméticos módulo de um inteiro n, onde atualmente n é tipicamente entre 512 e 1024 bits.

Devido ao número relativamente grande de n bits, tais esquemas de chave pública são relativamente lentos em operação e são considerados consumidores pesados de memória de acesso aleatório (RAM) e de outros recursos computacionais. Estes problemas são particularmente graves em aplicações nas quais os recursos computacionais são limitados, tais como aplicações de cartão inteligente. Assim, de modo a suplantar estes problemas, outras famílias de esquemas de chave pública as quais não necessitam muitos cálculos aritméticos módulo n foram desenvolvidas. Dentre estas outras famílias estão esquemas onde a chave pública é dada como um conjunto de k equações polinomiais multivariáveis sobre um campo matemático finito K o qual é relativamente pequeno, por exemplo, entre 2 e 2^{64}.

O conjunto de k equações polinomiais multivariáveis pode ser escrito como a seguir:

$$y_1 = P_1(x_1, \ldots, x_n)$$
$$y_2 = P_2(x_1, \ldots, x_n)$$
$$-$$
$$-$$
$$-$$
$$y_k = P_k(x_1, \ldots, x_n),$$

onde $P_1,\ldots, P_k$ são polinômios multivariáveis de grau total pequeno, tipicamente, menor do que ou igual a 8, e em muitos casos, exatamente dois.

Exemplos de tais esquemas incluem o esquema C* de T. Matsumoto e H. Imai, o esquema HFE de Jacques Patarin, e a forma básica do esquema "Óleo e Vinagre" de Jacques Patarin.

O esquema C* é descrito num artigo entitulado "Public Quadratic Polynomial-tuples for Efficient Signature Verification and Message-encryption" em Procedimentos de EUROCRYPT'88, Springer-Verlag, pp. 419-453. O esquema HFE é descrito num artigo entitulado "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP):Two New Families of Asymetric Algorithms" em Procedimentos de EUROCRYPT'96, Springer-Verlag, pp. 33-48. A forma básica do esquema "Óleo e Vinagre" de Jacques Patarin é descrito num artigo entitulado "The Oil and Vinegar Signature Scheme" apresentado no Workshop de Dagstuhl em Criptografia em setembro de 1997.

Entretanto, o esquema C* e a forma básica do esquema "Óleo e Vinagre" foram demonstrados como inseguros pelo fato que as decifrações de criptogramas tanto do esquema C* quanto da forma básica do esquema "Óleo e Vinagre" foram descobertas e publicadas por Aviad Kipnis e Adi Shamir num artigo entitulado "Cryptanalysis of the Oil and Vinegar Signature Scheme" em Procedimentos de CRYPTO'98, Springer-Verlag LNCS No. 1462, pp. 257-266.

As deficiências na construção do esquema HFE foram descritas em dois artigos não publicados entitulados "Cryptanalysis of the HFE Public Key Cryptosystem" e "Practical Cryptanalysis of the Hidden Fields Equations (HFE)", mas atualmente, o esquema HFE não é considerado comprometido já que para parâmetros bem escolhidos e ainda razoáveis, o número de cálculos necessário para quebrar o esquema HFE é ainda muito grande.

Alguns aspectos de tecnologias relacionadas são descritos nas seguintes publicações:

Patente US 5.263.085 para Shamir descreve um novo tipo de esquema de assinatura digital cuja segurança é baseada na dificuldade de solucionar sistemas de k equações polinomiais em m desconhecidos módulo um composto n; e

Patente US 5.375.170 para Shamir descreve um novo esquema de assinatura digital o qual é baseado numa nova classe de permutações biracionais as quais têm chaves pequenas e necessitam poucas operações aritméticas.

Os relatos de todas as referências acima mencionadas e através de todo o presente relatório são aqui incorporados a título de referência.

RESUMO DA INVENÇÃO

A presente invenção procura aperfeiçoar a segurança dos esquemas criptográficos de assinatura digital nos quais a chave pública é dada como um conjunto de k equações polinomiais multivariáveis, tipicamente, sobre um campo matemático finito K. Particularmente, a presente invenção procura aperfeiçoar a segurança da forma básica dos esquemas "Óleo e Vinagre" e HFE. Um esquema "Óleo e Vinagre" o qual é modificado para aperfeiçoar a segurança de acordo com a presente invenção é neste contexto referenciado como um esquema "Óleo e Vinagre" desequilibrado. Um esquema HFE o qual é modificado para aperfeiçoar a

segurança de acordo com a presente invenção é neste contexto referenciado como um esquema HFEV.

Na presente invenção, um conjunto S1 de k funções polinomiais é suprido como uma chave pública. O conjunto S1 de preferência inclui as funções $P_1(x_1,...,x_{n+v}, y_1,...,y_k),...,$ $P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, onde k, v, e n são inteiros, $x_1,...,x_{n+v}$, são n+v variáveis de um primeiro tipo, e $y_1,...,y_k$ são k variáveis de um segundo tipo. O conjunto S1 é de preferência obtido pela aplicação de uma operação de chave secreta num conjunto S2 de k funções polinomiais $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ onde $a_1,...,a_{n+v}$ são n+v variáveis as quais incluem um conjunto de n variáveis "óleo" $a_1,...,a_n$, e um conjunto de v variáveis "vinagre" $a_{n+1},...,a_{n+v}$. É apreciado que a operação de chave secreta pode incluir uma transformação s afim secreta sobre as n+v variáveis $a_1,...,a_{n+v}$.

Quando uma mensagem a ser assinada é provida, uma função de informação não significativa pode ser aplicada na mensagem para produzir uma série de k valores $b_1,...,b_k$. A série de k valores $b_1,...,b_k$ é de preferência substituída pelas variáveis $y_1,...,y_k$ do conjunto S2 respectivamente de modo a produzir um conjunto S3 de k funções polinomiais $P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$. Então, v valores $a'_{n+1},...,a'_{n+v}$ podem ser selecionados para as v variáveis "vinagre" $a_{n+1},...,a_{n+v}$, quer aleatoriamente, quer de acordo com um algoritmo de seleção predeterminado.

Uma vez que os v valores de $a'_{n+1},...,a'_{n+v}$ são selecionados, um conjunto de equações $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ é resolvido de preferência para obter uma solução para $a'_1,...,a'_n$. Então, a operação de chave secreta pode ser aplicada para transformar $a'_1,...,a'_{n+v}$ para a assinatura digital $e_1,...,e_{n+v}$.

A assinatura digital gerada $e_1,...,e_{n+v}$ pode ser verificada por um verificador o qual pode incluir, por

exemplo, um computador ou um cartão inteligente. De modo a verificar a assinatura digital, o verificador de preferência obtém a assinatura $e_1,...,e_{n+v}$, a mensagem, a função de informação não significativa e a chave pública. Então, o verificador pode aplicar a função de informação não significativa na mensagem para produzir a série de k valores $b_1,...,b_k$. Uma vez que os k valores $b_1,...,b_k$ são produzidos, o verificador de preferência verifica a assinatura digital ao verificar que as equações $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,\ P_k(e_1,...,e_{n+v},\ b_1,...,b_k)=0$ foram satisfeitas.

É assim provido de acordo com um modo de realização preferido da presente invenção um método criptográfico de assinatura digital incluindo as etapas de suprir um conjunto S1 de k funções polinomiais como a chave pública, o conjunto S1 incluindo as funções $P_1(x_1,...,x_{n+v}, y_1,...,y_k),...,\ P_k(x_1,...,x_{n+v},\ y_1,...,y_k)$, onde k, v, e n são inteiros, $x_1,...,x_{n+v}$, são n+v variáveis de um primeiro tipo, $y_1,...,y_k$ são k variáveis de um segundo tipo e o conjunto S1 é obtido pela aplicação de uma operação de chave secreta num conjunto S2 de k funções polinomiais $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ onde $a_1,...,a_{n+v}$ são n+v variáveis as quais incluem um conjunto de n variáveis "óleo" $a_1,...,a_n$, e um conjunto de v variáveis "vinagre" $a_{n+1},...,a_{n+v}$, provendo uma mensagem a ser assinada, aplicando uma função de informação não significativa na mensagem para produzir uma série de k valores $b_1,...,b_k$ substituindo a série de k valores $b_1,...,b_k$ pelas variáveis $y_1,...,y_k$ do conjunto S2 respectivamente para produzir um conjunto S3 de k funções polinomiais $P''_1(a_1,...,a_{n+v}),...,\ P''_k(a_1,...,a_{n+v})$, selecionando os v valores de $a'_{n+1},...,a'_{n+v}$ para as v variáveis "vinagre" $a_{n+1},...,a_{n+v}$, solucionando um conjunto de equações $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,\ P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ para obter uma solução para $a'_1,...,a'_n$ e aplicar a operação de

chave secreta para transformar $a'_1,...,a'_{n+v}$ para a assinatura digital $e_1,...,e_{n+v}$.

De preferência, o método inclui também a etapa de verificar a assinatura digital. A etapa de verificação inclui as etapas de obter a assinatura $e_1,...,e_{n+v}$, a mensagem, a função de informação não significativa e a chave pública, aplicar a função de informação não significativa na mensagem para produzir a série de k valores $b_1,...,b_k$, e verificar que as equações $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,..., P_k(e_1,...,e_{n+v}, b_1,...,b_k)=0$ estão satisfeitas.

A operação de chave secreta de preferência inclui uma transformação s afim secreta nas n+v variáveis $a_1,...,a_{n+v}$.

De preferência o conjunto S2 inclui o conjunto f(a) de k funções polinomiais do método HFEV. Em tal caso, o conjunto S2 de preferência inclui uma expressão incluindo k funções que são derivadas de um polinômio univariável. O polinômio univariável preferivelmente inclui um polinômio univariável de grau menor do que ou igual a 100.000.

Alternativamente, o conjunto S2 inclui o conjunto S de k funções polinomiais do esquema UOV.

A etapa de suprimento pode preferivelmente incluir a etapa de selecionar o número v de variáveis "vinagre" para ser superior ao número n de variáveis "óleo". De preferência, v é selecionado de modo que q^v é maior do que 2^{32}, onde q é o número de elementos de um campo finito K.

De acordo com um modo de realização preferido da presente invenção, a etapa de suprimento inclui a etapa de obter o conjunto S1 de um subconjunto S2' de k funções polinomiais do conjunto S2, o subconjunto S2' sendo caracterizado pelo fato que todos os coeficientes de componentes envolvendo quaisquer das variáveis $y_1,...,y_k$ nas k funções polinomiais $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ são zero, e o

número v de variáveis "vinagre" é maior do que o número n de variáveis "óleo".

De preferência, o conjunto S2 inclui o conjunto S de k funções polinomiais do método UOV, e o número v de variáveis "vinagre" é selecionado de modo a satisfazer uma das seguintes condições: (a) para cada característica p diferente de 2 de um campo K num esquema "Óleo e Vinagre" de grau 2, v satisfaz a desigualdade $q^{(v-n)*} n^4>2^{40}$, (b) para p=2 num esquema "Óleo e Vinagre" de grau 3, v é maior do que n*(1 + sqrt(3)) e inferior ou igual a $n^3/6$, e (c) para cada p diferente de 2 num esquema "Óleo e Vinagre" de grau 3, v é maior do que n e inferior ou igual a n^4. De preferência, o número v de variáveis "vinagre" é selecionado de modo a satisfazer as desigualdades $v<n^2$ e $q^{(v-n)-1*} n^4>2^{40}$ para uma característica p=2 de um campo K num esquema "Óleo e Vinagre" de grau 2.

Também é provido de acordo com um modo de realização preferido da presente invenção um aperfeiçoamento de um método de assinatura "Óleo e Vinagre", o aperfeiçoamento incluindo a etapa de utilizar mais variáveis "vinagre" do que variáveis "óleo". De preferência, o número v de variáveis "vinagre" é selecionado de modo a satisfazer uma das seguintes condições: (a) para cada característica p diferente de 2 de um campo K e para um grau 2 do esquema de assinatura "Óleo e Vinagre", v satisfaz a desigualdade $q^{(v-n)*} n^4>2^{40}$, (b) para p=2 para um grau 3 do esquema de assinatura "Óleo e Vinagre", v é maior do que n*(1 + sqrt(3)) e inferior ou igual a $n^3/6$, e (c) para cada p diferente de 2 num esquema de assinatura "Óleo e Vinagre" de grau 3, v é maior do que n e inferior ou igual a n^4. De preferência, o número v de variáveis "vinagre" é selecionado de modo a satisfazer as desigualdades $v<n^2$ e $q^{(v-n)-1*} n^4>2^{40}$ para uma

característica p=2 de um campo K num esquema "Óleo e Vinagre" de grau 2.

BREVE DESCRIÇÃO DOS DESENHOS

A presente invenção será entendida e apreciada mais completamente a partir da descrição detalhada a seguir, tomada em conjunto com os desenhos, nos quais:

A Fig. 1 é uma ilustração de um diagrama de bloco simplificado de uma implementação preferida de um sistema para gerar e verificar uma assinatura digital para uma mensagem, o sistema sendo construído e operacional de acordo com um modo de realização preferido da presente invenção;

A Fig. 2A é uma ilustração de um fluxograma simplificado de um método criptográfico de assinatura digital preferido para gerar uma assinatura digital para uma mensagem, o método sendo operacional de acordo com um modo de realização preferido da presente invenção, e

A Fig. 2B é uma ilustração de um fluxograma simplificado de um método criptográfico de assinatura digital preferido para verificar a assinatura digital da Fig. 2A, o método sendo operacional de acordo com um modo de realização preferido da presente invenção.

O Anexo I é um artigo por Aviad Kipnis, Jacques Patarin e Louis Goubin submetido para publicação por Springer-Verlag em Procedimentos de EUROCRYPT'99, o artigo descrevendo variações dos métodos UOV e HFEV.

DESCRIÇÃO DETALHADA DE UM MODO DE REALIZAÇÃO PREFERIDO

Fazemos referência agora à Fig. 1 a qual é uma ilustração de diagrama de bloco simplificado de uma implementação preferida de um sistema 10 para gerar e verificar uma assinatura digital para uma mensagem, o

sistema 10 sendo construído e operacional de acordo com um modo de realização preferido da presente invenção.

De preferência, o sistema 10 inclui um computador 15, tal como um computador de uso geral, o qual se comunica com um cartão inteligente 20 via um leitor de cartão inteligente 25. O computador pode preferivelmente incluir um gerador de assinatura digital 30 e um verificador de assinatura digital 35 os quais podem se comunicar via um bus de comunicação 40. O cartão inteligente 20 pode preferivelmente incluir um gerador de assinatura digital 45 e um verificador de assinatura digital 50 os quais podem comunicar dados via um bus de comunicação 55.

É apreciado que em aplicações de método de assinatura de chave pública típicos, um assinante de uma mensagem e um receptor de uma mensagem concordam com uma chave pública a qual é publicada, e numa função de informação não significativa a ser utilizada. Num caso em que a função de informação não significativa é comprometida, o assinante e o receptor podem concordar em mudar a função de informação não significativa. É apreciado que um gerador de uma chave pública não necessita ser o assinante ou o receptor.

De preferência, o verificador de assinatura digital 35 pode verificar uma assinatura gerada por um dos gerador de assinatura digital 30 e gerador de assinatura digital 45. Similarmente, o verificador de assinatura digital 50 pode verificar a assinatura gerada por um dos gerador de assinatura digital 30 e gerador de assinatura digital 45.

Fazemos referência agora à Fig. 2A a qual é uma ilustração de fluxograma simplificado de um método criptográfico de assinatura digital preferido para gerar uma assinatura digital para uma mensagem num primeiro processador (não ilustrado), e à Fig. 2B a qual é uma ilustração simplificada de um fluxograma de um método criptográfico de assinatura digital preferido para verificar a

assinatura digital da Fig. 2A num segundo processador (não ilustrado), os métodos das Figs. 2A e 2B sendo operacionais de acordo com um modo de realização preferido da presente invenção.

É apreciado que os métodos das Figs. 2A e 2B podem ser implementados em hardware, em software ou numa combinação de hardware e software. Além disso, o primeiro processador e o segundo processador podem ser idênticos. Alternativamente, o método pode ser implementado pelo sistema 10 da Fig. 1 na qual o primeiro processador pode estar compreendido, por exemplo, no computador 15, e o segundo processador pode estar compreendido no cartão inteligente 20, ou vice-versa.

Os métodos das Figs. 2A e 2B, e as aplicações dos métodos das Figs. 2A e 2B são descritos no Anexo I o qual é incorporado nesta invenção. As aplicações dos métodos das Figs. 2A e 2B podem ser empregadas para modificar a forma básica do esquema "Óleo e Vinagre" e o esquema HFE para com isso produzir o UOV e o HFEV respectivamente.

O Anexo I inclui um artigo não publicado por Aviad Kipnis, Jacques Patarin e Louis Goubin submetido para publicação por Springer-Verlag em Procedimentos de EUROCRYPT'99 o qual está programado para 2 – 6 de maio de 1999. O artigo incluído no Anexo I também descreve variações dos esquemas UOV e HFEV com pequenas assinaturas.

No método criptográfico de assinatura digital da Fig. 2A, um conjunto S1 de k funções polinomiais é de preferência suprido como uma chave pública (etapa 100) por um gerador da chave pública (não ilustrado) o qual, por exemplo, pode ser o gerador 30 da Fig. 1, o gerador 45 da Fig. 1, ou um gerador de chave pública externo (não ilustrado).

O conjunto S1 de preferência inclui as funções $P_1(x_1,\ldots,x_{n+v}, y_1,\ldots,y_k),\ldots, P_k(x_1,\ldots,x_{n+v}, y_1,\ldots,y_k)$, onde k, v, e n são inteiros, $x_1,\ldots,x_{n+v}$, são n+v variáveis de um primeiro

tipo, e $y_1,...,y_k$ são k variáveis de um segundo tipo. O conjunto S1 é de preferência obtido pela aplicação de uma operação de chave secreta num conjunto S2 de k funções polinomiais $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ onde $a_1,...,a_{n+v}$ são n+v variáveis as quais incluem um conjunto de n variáveis "óleo" $a_1,...,a_n$, e um conjunto de v variáveis "vinagre" $a_{n+1},...,a_{n+v}$. É apreciado que a operação de chave secreta pode incluir uma transformação s afim secreta nas n+v variáveis $a_1,...,a_{n+v}$.

Os termos variáveis "óleo" e variáveis "vinagre" referem-se a variáveis "'oleo" e variáveis "vinagre" como definidos na forma básica do esquema "Óleo e Vinagre" de Jacques Patarin o qual é descrito no artigo acima mencionado entitulado "The Oil and Vinegar Signature Scheme" apresentado na Workshop de Dagstuhl sobre Criptografia em setembro de 1997.

De preferência, quando uma mensagem a ser assinada é provida (etapa 105), um assinante pode aplicar uma função de informação não significativa na mensagem para produzir uma série de k valores $b_1,...,b_k$ (etapa 110). O assinante, por exemplo, pode ser o gerador 30 ou o gerador 45 da Fig. 1. A série de k valores $b_1,...,b_k$ é substituída de preferência pelas variáveis $y_1,...,y_k$ do conjunto S2 respectivamente de modo a produzir um conjunto S3 de k funções polinomiais $P''_1(a_1,...,a_{n+v}),...,P''_k(a_1,...,a_{n+v})$ (etapa 115). Então, v valores $a'_{n+1},...,a'_{n+v}$ podem ser selecionados de acordo com um algoritmo de seleção predeterminado.

Uma vez que os v valores $a'_{n+1},...,a'_{n+v}$ são selecionados, um conjunto de equações $P''_1(a_1,...,a_n, a'_{n+1},...,a'_{n+v})=0,...,\ P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ é de preferência resolvido para obter uma solução para $a'_1,...,a'_n$ (etapa 125). Então, a operação de chave secreta pode ser aplicada para transformar $a'_1,...,\ a'_{n+v}$ para uma assinatura digital $e_1,...e_{n+v}$ (etapa 130).

A assinatura digital gerada $e_1,...e_{n+v}$ pode ser verificada de acordo com o método descrito com referência á Fig. 2B por um verificador da assinatura digital (não ilustrado) o qual pode incluir, por exemplo, o verificador 35 ou o verificador 50 da Fig. 1. De modo a verificar a assinatura digital, o verificador de preferência obtém a assinatura $e_1,...e_{n+v}$, a mensagem, a função de informação não significativa e a chave pública (etapa 200). Então, o verificador pode aplicar a função de informação não significativa na mensagem para produzir a série de k valores $b_1,...,b_k$ (etapa 205). Logo que os k valores $b_1,...,b_k$ são produzidos, o verificador preferivelmente verifica a assinatura digital ao verificar que as equações $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,\ P_k(e_1,...,e_{n+v},\ b_1,...,b_k)=0$ foram satisfeitas (etapa 210).

É apreciado que a geração e verificação da assinatura digital como mencionado acima podem ser utilizadas para o UOV ao possibilitar que o conjunto S2 inclua o conjunto S de k funções polinomiais do esquema UOV como descrito no Anexo I. Alternativamente, a geração e verificação da assinatura digital como mencionado acima podem ser utilizadas para o HFEV ao permitir que o conjunto S2 inclua o conjunto f(a) de k funções polinomiais do esquema HFEV como descrito no Anexo I.

Como mencionado no Anexo I, os métodos das Figs. 2A e 2B possibilitam a obtenção de assinaturas digitais as quais são tipicamente menores do que as assinaturas digitais obtidas em esquemas teóricos de criptografia de número convencionais, tal como o esquema RSA bem conhecido.

De acordo com um modo de realização preferido da presente invenção, quando o conjunto S2 inclui o conjunto S de k funções polinomiais do esquema UOV, o conjunto S1 pode ser suprido com o número v de variáveis "vinagre" sendo

selecionado para ser maior do que o número n de variáveis "óleo". Preferivelmente, v também pode ser selecionado tal que q^v é maior do que 2^{32} , onde q é o número de elementos de um campo finito K sobre o qual os conjuntos S1, S2 e S3 são providos.

Ainda preferivelmente, o S1 pode ser obtido de um subconjunto S2' de k funções polinomiais do conjunto S2, o subconjunto S2' sendo caracterizado pelo fato que todos os coeficientes de componentes envolvendo quaisquer das variáveis $y_1,\ldots,y_k$ nas k funções polinomiais $P'_1(a_1,\ldots,n_{a+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,\ldots,n_{a+v},y_1,\ldots,y_k)$ são zero, e o número v de variáveis "vinagre"é maior do que o número n de variáveis "óleo".

No esquema "Óleo e Vinagre" básico, o número v de variáveis "vinagre" é escolhido para ser igual ao número n de variáveis "óleo". Para tal seleção das v variáveis, Aviad Kipnis, que é um dos inventores da presente invenção, e Adi Shamir demonstraram, no acima mencionado Procedimentos de CRYPTO 98, Springer, LNCS no. 1462, nas páginas 257-266, uma decifração de criptogramas do esquema de assinatura "Óleo e Vinagre" básico que torna o esquema "Óleo e Vinagre" básico inseguro. Adicionalmente, ao aplicar o mesmo método descrito por Kipnis e Shamir, o esquema "Óleo e Vinagre" básico pode ser mostrado como inseguro para qualquer número v de variáveis "vinagre"o qual é menor do que o número n de variáveis "óleo".

Os inventores da presente invenção descobriram, como descrito no Anexo I, que se o esquema "Óleo e Vinagre" é feito desequilibrado pela modificação do esquema "Óleo e Vinagre" de modo que o número v de variáveis "vinagre" é maior do que o número n de variáveis "óleo", um esquema "Óleo e Vinagre" (UOV) desequilibrado resultante pode ser seguro.

Especificamente, para um UOV de grau 2 e para todos os valores de p diferentes de 2, onde p é uma

característica do campo K, p sendo a ordem aditiva de 1, o esquema UOV é considerado seguro para valores de v os quais satisfaçam a desigualdade $q^{(v-n)-1*}n^4>2^{40}$. Para um UOV de grau 2 e para p=2, o número v de variáveis "vinagre" pode ser selecionado de modo a satisfazer as desigualdades $v<n^2$ e $q^{(v-n)-1*}n^4>2^{40}$. É apreciado que para valores de v os quais são superiores a $n^2/2$ porém inferiores ou igual a n^2, o UOV é também considerado seguro, e resolver o conjunto S1 é considerado ser tão difícil como resolver um conjunto de k equações aleatórias. Para valores de v os quais são superiores a n^2, acredita-se que o UOV seja inseguro.

Além disso, para um UOV de grau 3 e para p=2, o esquema UOV é considerado seguro para valores de v os quais são substancialmente maiores do que n*(1 + sqrt(3)) e inferiores ou iguais a $n^3/6$. É apreciado que para valores de v os quais são maiores do que $n^3/6$ porém inferiores ou iguais a $n^3/2$, o UOV é também considerado seguro, e resolver o conjunto S1 é considerado ser tão difícil quanto resolver um conjunto aleatório de k equações. Para valores de v os quais são superiores a $n^3/2$, e para valores de v os quais são inferiores a n*(1 + sqrt(3)), acredita-se que o UOV seja inseguro.

Adicionalmente, para um UOV de grau 3 e para p diferente de 2, o esquema UOV é considerado seguro para valores de v os quais são substancialmente maiores do que e inferiores ou iguais a n^4. É apreciado que para valores de v os quais são maiores do que $n^3/6$ porém menores do que ou iguais a n^4, o UOV é também considerado seguro, e solucionar o conjunto S1 é considerado ser tão difícil quanto solucionar um conjunto aleatório de k equações. Para valores de v os quais são maiores do que n^4, e para valores de v os quais são menores do que n, acredita-se que o UOV seja inseguro.

De preferência, num caso em que o conjunto S2 inclui o conjunto f(a) de k funções polinomiais do esquema

HFEV, o conjunto S2 pode incluir uma expressão a qual inclui k funções que são derivadas de um polinômio univariável. De preferência, o polinômio univariável pode incluir um polinômio de grau inferior ou igual a 100.000 num campo de extensão de grau n sobre K.

Exemplo de parâmetros selecionados para os esquemas UOV e HFEV são mostrados no Anexo I.

É apreciado que várias características da invenção as quais, para clareza, são descritas nos contextos de modos de realização diferentes podem também ser providas em combinação num modo de realização único. De modo inverso, várias características da invenção as quais, por concisão, são descritas no contexto de um modo de realização único podem também ser providas separadamente ou em qualquer sub-combinação adequada.

Será apreciado pelos técnicos no assunto que a presente invenção não está limitada pelo que foi particularmente mostrado e descrito anteriormente acima. Ao invés, o escopo da invenção é definido apenas pelas reivindicações seguintes.

APÊNDICE I

ESQUEMAS DE ASSINATURA ÓLEO E VINAGRE DESBALANCEADOS

Aviad Kipnis
NDS Technologies
5 Hamarpe St. Har Hotzvim
Jerusalem – Israel
akipnis@ndsisrael.com

Jacques Patarin, Louis Goubin
Bull SmartCards and Terminals
68, route de Versailles – BP45
78431 Louveciennes Cedex–França
{J.Patarin,L.Goubin}@frlv.bull.fr

Resumo

Em [16] J. Patarin projetou um novo esquema, denominado "Óleo e Vinagre", para computar assinaturas assimétricas. É muito simples, pode ser computado muito rápido (tanto em chave secreta quanto pública) e necessita muito pouca RAM nas implementações de cartões inteligentes. A idéia consiste em esconder equações quadráticas em n incógnitas denominadas "óleo" e $v=n$ incógnitas denominadas "vinagre" sobre um campo finito K, com funções lineares secretas. Este esquema original foi quebrado em [10] por A. Kipnis e A. Shamir. Neste trabalho, estudamos algumas variações muito simples do esquema original em que $v>n$ (ao invés de $v=n$).

Estes esquemas são denominados "Óleo e Vinagre Desbalanceados" (UOV) já que temos mais incógnitas "vinagre" do que incógnitas "óleo". Mostramos que, quando $v \cong n$, o ataque de [10] pode ser estendido, porém quando por exemplo $v \geq 2n$, a segurança do esquema ainda é um problema aberto. Além disso, quando $v \cong \frac{n^2}{2}$, a segurança do esquema é exatamente equivalente (se aceitamos uma propriedade muito natural mas não provada) ao problema de se resolver um conjunto randômico de n equações quadráticas em $\frac{n^2}{2}$ incógnitas (sem porta de armadilha). Entretanto, mostramos que (na característica 2) quando $v \geq n^2$, encontrar uma solução é geralmente fácil. Então veremos que é muito fácil combinar a idéia de Óleo e Vinagre e os esquemas HFE de [14]. O esquema resultante, denominado HFEV, parece atualmente também muito interessante tanto de um ponto de vista teórico quanto prático. A extensão de uma assinatura UOV pode ser tão curta quanto 192 bits e para HFEV ela pode ser tão curta quanto 80 bits.

Nota: Uma versão mais extensa deste relatório pode ser obtida dos autores.

1 Introdução

Desde 1985, vários autores (veja [7], [9], [12], [14], [16], [17], [18], [21] por exemplo) sugeriram alguns esquemas de

chave públicas onde a chave pública é dada como um conjunto de equações quadráticas multivariáveis (ou de grau mais elevado) sobre um campo finito pequeno K.

O problema geral de resolver tal conjunto de equações é NP-difícil (cf [8]) (mesmo no caso quadrático). Além disso, quando o número de incógnitas é, digamos, $n \geq 16$, os melhores algoritmos conhecidos freqüentemente não são significativamente melhores do que pesquisa exaustiva (quando n é muito pequeno, algoritmos de base Gröbner são mais eficientes, cf [6]).

Os esquemas são freqüentemente muito eficientes em termos de velocidade ou da RAM necessária numa implementação de cartão inteligente. (Entretanto, o comprimento da chave pública é geralmente ≥1 Kbyte. Não obstante, algumas vezes é útil observar que as computações de chave secreta podem ser realizadas sem a chave pública). O problema mais sério é que, de modo a introduzir uma porta de armadilha (para permitir a computação de assinaturas ou para permitir a decifração de mensagens quando um segredo é conhecido), o conjunto gerado de equações públicas geralmente se torna um pequeno subconjunto de todas as equações possíveis e, em muitos casos, os algoritmos foram quebrados. Por exemplo [7] foi quebrado por seus autores, e [12], [16], [21] foram quebrados. Entretanto, muitos esquemas ainda não foram quebrados (por exemplo [14], [17], [18],

[20]), e também em muitos casos, algumas variações muito simples foram sugeridas de modo a reparar os esquemas.

Portanto, atualmente, não sabemos se esta idéia de projetar algoritmos de chave pública com polinomiais multivariáveis sobre pequenos campos finitos é uma idéia muito poderosa (onde apenas alguns esquemas muito simples são inseguros) ou não.

Neste trabalho, apresentaremos dois novos esquemas: UOV e HFEV. UOV é um esquema muito simples: o esquema original de assinatura Óleo e Vinagre (de [16]) foi quebrado (veja [10]), porém se temos significativamente mais incógnitas "vinagre" do que incógnitas "óleo" (uma definição das incógnitas "óleo" e "vinagre" pode ser encontrada na seção 2), então o ataque de [10] não funciona e a segurança deste esquema mais geral (denominado UOV) é ainda um problema aberto.

Estudaremos também esquemas Óleo e Vinagre de grau três (ao invés de dois). Então, apresentaremos um outro esquema, denominado HFEV. HFEV combina as idéias de HFE (de [14]) e variáveis vinagre. HFEV parece mais eficiente do que o esquema HFE original.

Finalmente, na seção 13, apresentamos o que sabemos sobre os esquemas principais nesta área de polinomiais multivariáveis.

2 O (Original e Desbalanceado) Óleo e Vinagre de grau dois

Deixe $K=\mathbf{F}_q$ ser um campo finito pequeno (por exemplo $K=\mathbf{F}_2$). Deixe n e v serem dois inteiros. A mensagem a ser assinada (ou sua informação não significativa) é representada como um elemento de K^n, denotado por $y=(y_1, \ldots, y_n)$. Tipicamente, $q^n \cong 2^{128}$ (na seção 8, veremos que $q^n \cong 2^{64}$ também é possível). A assinatura x é representada como um elemento de K^{n+v} denotado por $x = (x_1, \ldots, x_{n+v})$.

Chave secreta

A chave secreta é feita de duas partes:

1. Uma função bijetiva e afim S: $K^{n+v} \rightarrow K^{n+v}$. Por "afim", queremos dizer que cada componente da saída pode ser escrito como um polinomial de grau um nas $n+v$ incógnitas de entrada, e com coeficientes em K.
2. Um conjunto (S) de n equações do seguinte tipo:

$$\forall_i,\ 1 \le i \le n,\ y_i = \sum \gamma_{ijk} a_j a_k + \sum \lambda_{ijk} a_j a_k + \sum \xi_{ij} a_j + \sum \xi'_{ij} a_j + \delta_i(S).$$

Os coeficientes γ_{ijk}, λ_{ijk}, ε_{ij}, ε'_{ij} e δ_i são os coeficientes secretos destas n equações. Os valores $a_1, \ldots, na$ (as incógnitas "óleo") e $a_1, \ldots, a_v$ (as incógnitas "vinagre") estão em K. Observe que estas equações (S) não contêm termos em $a_i a_j$

Chave pública

Deixe A ser o elemento de K^{n+v} definido por $A = (a_1, \ldots, a_n, a'_1, \ldots, a'_v)$. A é transformado em $x=s^{-1}(A)$, onde s é a função secreta, bijetiva e afim de K^{n+v} para K^{n+v}.

Cada valor y_i, $1 \leq i \leq n$, pode ser escrito como um polinomial P_i de grau total dois nas x_j incógnitas, $1 \leq j \leq n+v$. Designamos por (P) o conjunto das seguintes n equações:

$$\forall i,\ 1 \leq i \leq n,\ y_i = P_i(x_1, \ldots, x_{n+v}) \qquad (P).$$

Estas n equações quadráticas (P) (nas $n+v$ incógnitas x_j) são a chave pública.

Computação de uma assinatura (com a chave secreta)

A computação de uma assinatura x de y é executada como a seguir:

Etapa 1: Descobrimos n incógnitas $a_1, \ldots, a_n$ de K e v incógnitas $a'_1, \ldots, a'_v$ de K tal que as n equações (S) sejam satisfeitas. Isto pode ser feito como segue: escolhemos randomicamente as v incógnitas vinagre a'_i, e então computamos as incógnitas a_i de (S) por reduções Gaussianas (porque – já que não há termos $a_i a_j$ – as equações (S) são afim nas incógnitas a_i quando a'_i são fixadas).

Observação: Se não encontramos solução, então simplesmente tentamos novamente com novas incógnitas aleatórias vinagre.

Após muito poucas tentativas, a probabilidade de obter ao menos uma solução é muito alta, porque a probabilidade para uma matriz n x n sobre $\mathbf{F}_q$ para ser invertível não é desprezível. (É exatamente $\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)\ldots\left(1-\frac{1}{q^{n-1}}\right)$. Para q = 2, isto dá aproximadamente 30 %, e para q > 2, esta probabilidade é até maior).

Etapa 2: Computamos $x = s^{-1}(A)$, onde $A = (a_1, \ldots, a_n, a'_1, \ldots, a'_v)$. x é uma assinatura de y.

Verificação pública de uma assinatura

Uma assinatura *x* de *y* é válida apenas e se todos os (P) são satisfeitos. Como resultado, nenhum segredo é necessário para verificar se uma assinatura é válida: este é um esquema assimétrico de assinatura.

Nota: O nome "Óleo e Vinagre" vem do fato que – nas equações (*S*) – as "incógnitas óleo" a_i e as "incógnitas vinagre" a'_j não estão todas misturadas juntas: não existem produtos $a_i a_j$. Entretanto, em (*P*), esta propriedade é ocultada pela "mistura" das incógnitas pela transformação s. Está esta

propriedade "bastante escondida"? Na verdade, esta questão significa exatamente: "o esquema é seguro ?". Quando $v = n$, chamamos os esquema "Óleo e Vinagre Original", já que este caso foi apresentado primeiramente em [16]. Este caso foi quebrado em [10]. É muito fácil ver que a cripto-análise de [10] também funciona, exatamente do mesmo modo, quando $v < n$. Entretanto, os casos $v > n$ são, como veremos, muito mais difíceis. Quando $v > n$, chamamos o esquema "Óleo e Vinagre Desbalanceado".

3 Cripto-análise do caso v = n (de [10])

A idéia do ataque de [10] é essencialmente a seguinte: De modo a separar as variáveis óleo e as variáveis vinagre, olhamos para as formas quadráticas das n equações públicas de (P), omitimos por um tempo os termos lineares. Deixe G_i para $1< i \leq n$ ser a respectiva matriz da forma quadrática de P_i das equações públicas (P). A parte quadrática das equações no conjunto (S) é representada como uma forma quadrática com uma matriz correspondente $2n$ x $2n$ da forma: $\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$, a submatriz superior à esquerda zero n x n é devido ao fato que uma variável óleo não é multiplicada por uma variável óleo. Após ocultar as variáveis internas com a função linear s,

conseguimos uma representação para as matrizes $G_i = S\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix}S^{-1}$, onde S é uma matriz $2n$ x $2n$ invertível.

Definição 3.1: Definimos o subespaço óleo para ser o subespaço linear de todos os vetores K^{2n} cuja segunda metade contém apenas zeros.

Definição 3.2: Definimos o subespaço vinagre como o subespaço linear de todos os vetores em K^{2n} cuja primeira metade contém apenas zeros.

Proposição 1: *Deixe E e F serem matrizes 2n x 2n com uma submatriz superior esquerda n x n de zeros. Se F é invertível então o subespaço óleo é um subespaço invariante de* EF^{-1}.

Prova: veja [10]

Definição 3.4: Para uma matriz invertível G_j, defina $G_{ij} = G_i G_j^{-1}$.

Definição 3.5: Deixe *0* ser a imagem do subespaço óleo por S^{-1}.

De modo a achar o subespaço óleo, usamos o seguinte teorema:

Teorema 3.1 *O* é um subespaço comum invariável de todas as matrizes G_{ij}.

Prova:

$$G_{ij} = S\begin{pmatrix} 0 & A \\ B_i & C_i \end{pmatrix} S'(S')^{-1} \begin{pmatrix} 0 & A_j \\ B_j & C_j \end{pmatrix}^{-1} S^{-1} =$$

$$= S\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} \begin{pmatrix} 0 & A_j \\ B_j & C_j \end{pmatrix}^{-1} S^{-1}$$

As duas matrizes internas têm a forma de *E* e *F* na proposição 1. Portanto, o subespaço óleo é um subespaço invariável do termo interno e *O* é um subespaço invariável de $G_i G_j^{-1}$. O problema de achar subespaço invariável comum de conjunto de matrizes é estudado em [10]. Aplicando os algoritmos em [10] nos dá *O*. Então pegamos *V* para ser um subespaço arbitrário de dimensão *n* tal que $V + O = K^{2n}$, e elas dão uma equivalente separação de óleo e vinagre. Quando temos tal separação, trazemos de volta os termos lineares que foram omitidos, pegamos valores randômicos para as variáveis vinagre e deixamos com um conjunto de *n* equações lineares com *n* variáveis óleo.

Nota: A Proposição 1 não é mais verdadeira quando $v > n$. O

vinagre. Entretanto F^{-1} não mapeia necessariamente a imagem por E do subespaço óleo de volta para dentro do subespaço óleo e isto é porque a cripto-análise do óleo e vinagre original não é válida para o caso desbalanceado.

4 Cripto-análise quando $v > n$ e $v \cong n$

Nesta seção, descreveremos uma modificação do ataque acima, que é aplicável enquanto $v - n$ é pequeno (mais precisamente a complexidade esperada do ataque é de aproximadamente $q^{(v-n)-1}n^4$).

Definição 4.1: Definimos nesta seção o subespaço óleo como sendo o subespaço linear de todos os vetores em K^{n+v} cujas últimas coordenadas v são apenas zeros.

Definição 4.2: Definimos nesta seção o subespaço vinagre como sendo o subespaço linear de todos os vetores K^{n+v} cujas primeiras n coordenadas são apenas zeros.

Aqui nesta seção, começamos com os termos quadráticas homogêneas das equações: omitimos os termos lineares por um tempo. As matrizes G_i têm a representação $G_i = S\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S^t$ onde a matriz superior esquerda é a matriz zero n x n, A_i é uma matriz n x v, B_i é uma matriz v x n, C_i é

uma matriz v x v e S é uma matriz linear invertível $(n+v)$ x $(n+v)$.

Definição 4.3: Defina E_i para ser $\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix}$.

Proposição 2: *Para qualquer matriz E que tem a forma* $\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$, o seguinte é válido:

a) E transforma o subespaço óleo no subespaço vinagre.

b) Se a matriz E^{-1} existe, então a imagem do subespaço vinagre por E^{-1} é um subespaço de dimensão v o qual contém nele o subespaço óleo n-dimensional.

Prova: *a)* segue diretamente da definição dos subespaços óleo e vinagre. Quando *a)* é dado então *b)* é imediato.

O algoritmo que propomos é probabilístico. Ele procura um subespaço invariante do subespaço óleo depois que ele é transformado por S. A probabilidade do algoritmo ter sucesso na primeira tentativa é pequena. Portanto necessitamos repetí-lo com entradas diferentes. Utilizamos a seguinte propriedade: qualquer combinação linear das matrizes E_1, ..., E_n é também da forma $\begin{pmatrix} 0 & A \\ B & C \end{pmatrix}$. O seguinte teorema explica porque um subespaço invariável pode existir com uma certa probabilidade.

Teorema 4.1 *Deixe F ser uma combinação linear invertível das matrizes* E_1, ..., E_n. *Então para qualquer k tal que* E_k^{-1} *exista, a matriz* FE_k^{-1} *tem um subespaço invariante não trivial o qual também é um subespaço do subespaço óleo, com probabilidade não inferior a* $\frac{q-1}{q^{2d}-1}$ *para* $d = v - n$.

Prova: Veja a versão estendida deste trabalho.

Observação: É possível obter um resultado melhor para o número esperado de auto-vetores e com muito menos esforço: I_1 é um subespaço com dimensão não menor que n-d e é mapeado por FE_k^{-1} em um subespaço com dimensão n. A probabilidade para um vetor não nulo ser mapeado a um múltiplo não nulo dele mesmo é $\frac{q-1}{q^n-1}$. Para obter o valor esperado, multiplicamos pelo número de vetores não nulos em I_1. Resulta um valor que não é menor do que $\frac{(q-1)(q^{n-d}-1)}{q^n-1}$. Uma vez que cada auto-vetor é computado q-1 vezes, então o número esperado de subespaços não variáveis de dimensão 1 não é menor que $\frac{q^{n-d}-1}{q^n-1} \approx q^{-d}$.

Definimos O como na seção 3 e obtemos o seguinte resultado para O:

Teorema 4.2: *Seja F uma combinação linear com inversão das matrizes G_1, ..., G_n. Então para cada k tal que G_k^{-1} exista, a matriz FG_k^{-1} tem um subespaço não trivial invariável, que é também um subespaço de O com probabilidade não menor que $\frac{q-1}{q^{2d}-1}$ para d=v-n.*

Prova:

$$FG_k^{-1} = (\alpha_1 G_1 + \cdots + \alpha_n G_n) G_k^{-1}$$

$$= S(\alpha_1 E_1 + \cdots + \alpha_n E_n) S' (S')^{-1} E_k^{-1} S^{-1} = S(\alpha_1 E_1 + \cdots + \alpha_n E_n) E_k^{-1} S^{-1}.$$

O termo interno é um subespaço não variável do subespaço óleo com a probabilidade requerida. Portanto, o mesmo vale para FG_k^{-1}, mas ao invés de um subespaço do subespaço óleo, obtemos um subespaço de *O*.

Como encontrar *O* ?

Tomamos uma combinação linear randômica de G_1, ..., G_n e a multiplicamos por um inverso de uma das matrizes G_k. Depois nós calculamos todos os mínimos subespaços invariante desta matriz (um subespaço mínimo invariante de uma matriz *A* não contém subespaços não triviais invariáveis da matriz *A* – estes subespaços correspondem a fatores irredutíveis da característica polinomial de *A*). Isto pode ser feito em tempo probabilístico polinomial utilizando técnicas de álgebra linear

convencional. Esta matriz pode ter um subespaço invariável o qual é um subespaço de O.

A proposição seguinte nos possibilita distinguir entre subespaços que estão contidos em O e subespaços randômicos.

Proposição 3: *Se H é um subespaço linear e $H \subset O$, então para cada x, y em H e cada i, $G_i(x,y) = 0$ (aqui consideramos G_i como uma forma bilinear).*

Prova: Existem x' e y' no subespaço óleo de maneira que $x' = xS$ e $y' = yS$.

$$G_i(x,y) = xS\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} S' y' = x'\begin{pmatrix} 0 & A_i \\ B_i & C_i \end{pmatrix} (y')' = 0$$

O último termo é nulo porque x' e y' estão no subespaço óleo.

A Proposição 3 dá um teste polinomial para distinguir entre subespaços de O e subespaços aleatórios. Se a matriz que utilizamos não possui subespaço mínimo que também é um subespaço de O, então pegamos outra combinação linear de G_1, ..., G_n, a multiplicamos por um inverso de uma das matrizes G_k e tentamos de novo. Após a repetição deste processo aproximadamente q^{d-1} vezes, encontramos com boa probabilidade ao menos um vetor nulo de O. Continuamos o processo até conseguirmos n vetores independentes de O. Estes vetores ultrapassam O. A complexidade esperada do processo é proporcional a $q^{d-1}.n^4$. Utilizamos aqui o número esperado de

tentativas até que encontramos um subespaço não variante não trivial e o termo n^4 cubra as operações computacionais de álgebra linear que necessitamos executar para cada tentativa.

5. Os casos $v \cong \frac{n^2}{2}$ (ou $v \geq \frac{n^2}{2}$)

5 Propriedade

Deixe (A) ser um conjunto randômico de n equações quadráticas em $(n+v)$ variáveis $x_1, \ldots, x_{n+v}$. (Por "randômico" entendemos que os coeficientes destas equações são escolhidos uniforme e aleatoriamente). Quando $v \cong \frac{n^2}{2}$ (e mais genericamente quando $v \geq \frac{n^2}{2}$), existe provavelmente – para a maioria de tal (A) – uma troca linear de variáveis $(x_1,\ldots,x_{n+v}) \mapsto (x_1' \cdots, x_{n+v}')$ tal que o conjunto (A') de equações (A) escritas em $(x_1',\ldots,x_{n+v}')$ seja um sistema "Óleo e Vinagre" (*i.e.* na existem termos em $x_i' x_j'$ com $i \leq n$ e $j \leq n$).

Um argumento para justificar a propriedade

Seja
$$\begin{cases} x_1 = \alpha_{1,1}x_1' + \alpha_{1,2}x_2' + \ldots + \alpha_{1,n+v}x_{n+v}' \\ \vdots \\ x_{n+v} = \alpha_{n+v,1}x_1' + \alpha_{n+v,2}x_2' + \ldots + \alpha_{n+v,n+v}x_{n+v}' \end{cases}$$

Escrevendo que os coeficientse em todas as n equações de (A) de todos os $x_i' x_j'$ $(i \leq n \ \ e \ \ j \geq n)$ são nulos, obtemos um sistema

de $n.n.\frac{n+1}{2}$ equações quadráticas nas $(n+v).n$ variáveis $a_{i,j}$ $\left(1 \le i \le n+v, 1 \le j \le n\right)$.

Por isto, quando $v \geq$ aproximadamente $\frac{n^2}{2}$, podemos esperar ter uma solução para este sistema de equações para a maioria de (A).

Observações:

1. Este argumento é muito natural, mas isto não é uma prova matemática completa.

2. O sistema pode ter uma solução, mas encontrar a solução pode ser um problema difícil. Isto é porque um Esquema Óleo e Vinagre Desbalanceado pode ser seguro (para parâmetros bem escolhidos): existe sempre uma troca linear de variáveis que torna o problema fácil de resolver, mas achar tal troca de variáveis pode ser difícil.

3. Na seção 7, veremos que, a despeito do resultado desta seção, não é recomendável escolher $v \geq n^2$ (ao menos na característica 2).

6 Resolver um conjunto de n equações quadráticas em k incógnitas, $k > n$, tem dificuldade NP

(veja a versão estendida deste trabalho)

7 Um algoritmo geralmente eficiente (mas não sempre) para resolver um conjunto randômico de n equações quadráticas em n^2 (ou mais) incógnitas

Nesta seção, descrevemos um algoritmo que resolve um sistema de n equações quadráticas) randomicamente escolhidas em $n + v$ variáveis, quando $v \geq n^2$.

Seja (S) o seguinte sistema:

$$(S) \quad \begin{cases} \sum_{1 \leq i \leq j \leq n+v} a_{ij1} x_i x_j + \sum_{1 \leq i \leq n+v} b_{i1} x_i + \delta_1 = 0 \\ \vdots \\ \sum_{1 \leq i \leq j \leq n+v} a_{ijn} x_i x_j + \sum_{1 \leq i \leq n+v} b_{in} x_i + \delta_n = 0 \end{cases}$$

A principal idéia do algoritmo consiste na utilização de uma mudança de variáveis tal que:

$$\begin{cases} x_1 = \alpha_{1,1} y_1 + \alpha_{2,1} y_2 + \ldots + \alpha_{n+v,1} y_{n+v} \\ \vdots \\ x_{n+v} = \alpha_{1,n+v} y_1 + \alpha_{2,n+v} y_2 + \ldots + \alpha_{n+v,n+v} y_{n+v} \end{cases}$$

cujos coeficientes $\alpha_{i,j}$ (para $1 \leq i \leq n$, $1 \leq j \leq n+v$) são encontrados etapa por etapa, de maneira que o sistema resultante (S') (escrito com respeito a estas novas variáveis $y_1, \ldots, y_{n-v}$) seja fácil de resolver.

- Começamos por escolher randomicamente $\alpha_{1,1}$, ..., $\alpha_{1,n+v}$.

- Então calculamos $\alpha_{2,1}$, ..., $\alpha_{2,n+v}$ tal que (S') não contenha termos y_1y_2. Esta condição leva a um sistema de n equações lineares sobre as $(n+v)$ incógnitas $\alpha_{2,j}$ $(1 \le j \le n+v)$:

$$\sum_{1 \le i \le j \le n+v} a_{ijk}\alpha_{1,i}\alpha_{2,j} = 0 \qquad (1 \le k \le n).$$

- Depois calculamos $\alpha_{3,1}$, ..., $\alpha_{3,n+v}$ tal que (S') não contenha termos y_1y_3 ou y_2y_3. Esta condição é equivalente ao seguinte sistema de $2n$ equações lineares sobre as $(n+v)$ incógnitas $\alpha_{3,j}$ $(1 \le j \le n+v)$:

$$\begin{cases} \sum_{1 \le i \le j \le n+v} a_{ijk}\alpha_{1,i}\alpha_{3,j} = 0 & (1 \le k \le n) \\ \sum_{1 \le i \le j \le n+v} a_{ijk}\alpha_{2,i}\alpha_{3,j} = 0 & (1 \le k \le n) \end{cases}$$

- ...

- Finalmente, calculamos $\alpha_{n,1}$, ..., $\alpha_{n,n+v}$ tal que (S') não contenha termos y_1y_n, ou y_2y_n, ..., ou $y_{n-1}y_n$. Esta condição dá o seguinte sistema de $(n-1)n$ equações lineares em $(n+v)$ incógnitas $\alpha_{n,j}$ $(1 \le j \le n+v)$:

$$\begin{cases} \sum_{1 \le i \le j \le n+v} a_{ijk}\alpha_{1,i}\alpha_{n,j} = 0 & (1 \le k \le n) \\ \sum_{1 \le i \le j \le n+v} a_{ijk}\alpha_{n-1,i}\alpha_{3,j} = 0 & (1 \le k \le n) \end{cases}$$

Em geral, todas estas equações lineares fornecem ao menos uma solução (encontrada por redução Gaussiana). Em

particular, o último sistema de $n(n\text{-}1)$ equações e $(n+v)$ incógnitas geralmente dá uma solução, tão logo que

$n+v>n(n\text{-}1)$, *i.e.* $v>n(n\text{-}2)$, o que é verdadeiro por hipótese.

Além do mais, os n vetores $\begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{1,n+v} \end{pmatrix},\ldots,\begin{pmatrix} \alpha_{n,1} \\ \vdots \\ \alpha_{n,n+v} \end{pmatrix}$ muito provavelmente são linearmente independentes para um sistema randômico quadrático (S)

As constantes α_{ij} remanescentes (*i.e.*aquelas com $n+1\leq i\leq n+v$ e $1\leq j\leq n+1$) são randomicamente escolhidas, de modo a obter uma troca *bijetiva* de variáveis.

Reescrevendo o sistema (S) com respeito a estas novas variáveis y_i, somos levados ao seguinte sistema:

$$(S')\begin{cases} \sum_{i=1}^{n}\beta_{i,1}y_i^2+\sum_{i=1}^{n}y_iL_{i,1}(y_{n+1},\ldots,y_{n+v})+Q_1(y_{n+1},\ldots,y_{n+v})=0 \\ \qquad\vdots \\ \sum_{i=1}^{n}\beta_{i,n}y_i^2+\sum_{i=1}^{n}y_iL_{i,n}(y_{n+1},\ldots,y_{n+v})+Q_n(y_{n+1},\ldots,y_{n+v})=0 \end{cases}$$

onde cada L_{ij} é uma função afim e cada Q_i é uma função quadrática.

Então calculamos $y_{n+1}, \ldots, y_{n+v}$ tal que:

$$\forall i,\ 1\leq i\leq n,\ \forall j,\ 1\leq j\leq n+v,\ L_{ij}(y_{n+1},\ \ldots,\ y_{n+v})=0$$

Isto é possível porque temos que resolver um sistema linear de n^2 equações e v incógnitas, que geralmente dá ao menos uma solução, enquanto $v\geq n^2$. Tomamos uma dessas soluções.

Geralmente, isto dá o y_i^2 por redução Gaussiana.

Então, na característica 2, desde que $x \mapsto x^2$ é uma bijeção, então encontraremos facilmente uma solução para os y_i desta expressão dos y_i^2. Na característica $\neq 2$, também terá sucesso quando 2^n não é muito grande (*i.e.* quando $n \leq 40$ por exemplo). Quando n é grande, também existe um método para achar uma solução, baseado na teoria geral de formas quadráticas. Devido a falta de espaço, este método será encontrado na versão estendida deste trabalho.

8 Uma variação com assinaturas duas vezes menores

No UOV descrito na seção 2, a chave pública é um conjunto de n equações quadráticas $y_i = P_i(x_1, \ldots, x_{n+v})$, para $1 \leq i \leq n$, onde $y = (y_1, \ldots, y_n)$ é o valor de informação não significativa da mensagem a ser assinada. Se utilizamos uma função de informação não significativa livre de colisão, o valor de informação não significativa deve ter no mínimo 128 bits de comprimento. Portanto, q^n tem que ser no mínimo 2^{128}, de modo que o comprimento típico da assinatura, se $v = 2n$, é ao menos 3 x 128 = 384 bits.

Como vemos agora, é possível fazer uma pequena variação no projeto da assinatura para obter assinaturas duas vezes menores. A idéia é manter o mesmo polinômio P_i (com a mesma chave secreta associada), mas agora as equações públicas que verificamos são:

$$\forall i,\ P_i(x_i, \ldots, x_{n+v})+L_i(y_i, \ldots, y_n, x_1, \ldots, x_{n+v})=0,$$

onde L_i é uma função linear em $(x_i, \ldots, x_{n+v})$ e onde os coeficientes de L_i são gerados por uma função de informação não significativa em $(y_i, \ldots, y_n)$.

Por exemplo $L_i(y_i,\ldots, y_n, x_1,\ldots, x_{n+v})= \alpha_1 x_1+\alpha_2 x_2+ \ldots+ +\alpha_{n+v}x_{n+v}$, onde $(\alpha_1, \alpha_2, \ldots, \alpha_{n+v})$=Informação não significativa$(y_i, \ldots, y_n \| i)$. Agora, n pode ser escolhido tal que $q^n \geq 2^{64}$ (ao invés de $q^n \geq 2^{128}$). (Nota: q^n tem que ser $\geq 2^{64}$ para evitar a exaustiva busca de uma solução x). Se $v=2n$ e $q^n \cong 2^{64}$, o comprimento da assinatura será 3 x 64 = 192 bits.

9 Óleo e Vinagre de grau três

O esquema

Os esquemas quadráticos Óleo e Vinagre descritos na seção 2 podem facilmente ser estendidos para um grau mais alto. No caso de grau três, o conjunto (S) de equações ocultas são do seguinte tipo: para todos $i \leq n$,

$$y_i = \sum \gamma_{ijkl} a_j a_k a_l'' + \sum \mu_{ijkl} a_j' a_k' a_l' + \sum \lambda_{ijk} a_j' a_k' +$$

$$+ \sum \nu_{ijk} a_j' a_k' + \sum \xi_{ij} a_j + \sum \xi_{ij}' a_j' + \delta_i \qquad (S).$$

Os coeficientes γ_{ijk}, μ_{ijkl}, λ_{ijk}, ν_{ijk}, ξ_{ij}, ξ_{ij}' e δ_i são os coeficientes secretos destas n equações. Observe que estas equações (S) não contêm termos em $a_j a_k a_l$ ou em $a_j a_k$: as equações são afins nas a_j incógnitas quando as a_k' incógnitas são fixas.

A computação da chave pública, a computação da assinatura e a verificação de uma assinatura são feitas como anteriormente.

Primeira cripto-análise de Óleo e Vinagre de grau três quando $v \leq n$

Podemos olhar para a parte quadrática da chave pública e atacar exatamente como para a Óleo e Vinagre de grau 2. Isto deve funcionar quando $v \leq n$.

Nota: Se não existe parte quadrática (i.e. a chave pública é homogênea de grau três), ou se este ataque não funciona, então é sempre possível aplicar uma troca randômica afim de variáveis e tentar novamente.

Cripto-análise de Óleo e Vinagre de grau três quando $v \leq (1+\sqrt{3})n$ e K é de característica $\neq 2$ (de uma idéia de D. Coppersmith, cf [4])

A idéia chave é a de detectar a "linearidade" em algumas direções. Procuramos o conjunto V dos valores $d=(d_1, \ldots, d_{n+v})$ tal que:

$$\forall x, \forall i, 1 \leq i \leq n, P_i(x+d)+P_i(x-d)=2P_i(x) \qquad (\#)$$

Escrevendo que cada x_k indeterminado tem um coeficiente zero, obtemos $n.(n+v)$ equações quadráticas nas $(n+v)$ incógnitas d_j.

(Cada monômio $x_i x_j x_k$ resulta $(x_j+d_j)(x_k+d_k)(x_l+x_l)+(x_j-d_j)(x_k-d_k)(x_l-d_l)-2x_j x_k x_l$, *i.e.* $2(x_j d_k d_l+x_k d_j d_l+x_l d_j d_k)$.)

Além disso, o cripto-analista pode especificar cerca de n-1 das coordenadas d_k de d, uma vez que o espaço vetorial do d correto é de dimensão n. Fica para ser resolvido $n.(n-v)$ equações quadráticas em $(v+1)$ incógnitas d_j. Quando v não é muito grande (tipicamente quando $\frac{(v+1)^2}{2} \leq n(n+v)$, *i.e.* quando $v \leq (1+\sqrt{3})n$), isto é esperado ser fácil. Como um resultado quando $v\leq$ aproximadamente $(1+\sqrt{3})n$ e $|K|$ é impar, isto dá uma maneira simples de quebrar o esquema.

Nota 1: Quando v é sensivelmente maior que $(1+\sqrt{3})n$ (este é um limite mais desbalanceado do que tivemos no caso quadrático), não sabemos no presente como quebrar o esquema.

Nota 2: Bastante estranhamente, esta cripto-análise de esquemas Óleo e Vinagre de grau três não funciona em esquemas Óleo e Vinagre de grau dois. A razão é que – no grau dois – escrever

$$\forall x,\ \forall i,\ 1\leq i\leq n,\ P_i(x+d)+P_i(x-d)=2P_i(x)$$

somente dá n equações de grau dois sobre as $(n+v)d_j$ incógnitas (que não sabemos como resolver). (Cada monômial $x_i x_k$ resulta $(x_j+d_j)(x_k+d_k)(x_j-d_j)(x_k-d_k)-2x_j x_k$, *i.e.* $2d_j d_k$.)

Nota 3: No grau dois, vimos que chaves públicas Óleo e Vinagre não Balanceadas são esperadas cobrir quase todo o conjunto de n equações quadráticas quando $v=\frac{n^2}{2}$. No grau três, temos uma propriedade similar: as chaves públicas são esperadas cobrir quase todo o conjunto de n equações cúbicas quando $v\cong\frac{n^3}{6}$ (a prova é similar).

10 Outro esquema: HFEV

No esquema HFE "mais simples" (utilizamos as notações de [14], temos $b=f(a)$, onde:

$$f(a)=\sum_{i,j}\beta_{ij}a^{q^{\theta_{ij}}+q^{\varphi_{ij}}}+\sum_{i}\alpha_i a^{q^{\xi_i}}+\mu_0, \qquad (1)$$

onde β_{ij}, α_i e μ_0 são elementos do campo $\mathbf{F}_{q^n}$. Seja v um inteiro (v será o número de variáveis x_i extras, ou o número de variáveis "vinagre" que adicionamos no esquema). Seja $a'=(a_1',\ldots,a_v')$ um sobre-v de variáveis de K. Deixe agora cada α_i de (1) ser um elemento de $\mathbf{F}_{q^n}$ tal que cada dos n componentes de α_i em uma base é uma função linear randômica secreta das variáveis vinagre $a_1',\ldots,a_v'$. E em (1), seja agora μ_0 um elemento de $\mathbf{F}_{q^n}$ tal que cada um dos n componentes de μ_0 em uma base é uma função quadrática randômica secreta das variáveis $a_1',\ldots,a_v'$. Então as $n+v$ variáveis $a_1,\ldots,a_v,a_1',\ldots,a_v'$ serão misturadas na bijeção afim secreta s para obter as variáveis $x_1,\ldots,x_{n+v}$. E,

como anteriormente $t(b_1, \ldots, b_n)=(y_1, \ldots, y_n)$, onde t é uma bijeção afim secreta. Então a chave pública é dada como n equações $y_i=P_i(x_1, \ldots, x_{n+v})$. Para computar uma assinatura, os valores vinagre $a_1,\ldots,a_v$ serão simplesmente escolhidos randomicamente. Então, os valores de μ_0 e α_i serão computados. Então, as equações monovariáveis (1) serão resolvidas (em a) em $\mathbf{F}_{q^n}$.

Exemplo: Seja $K=\mathbf{F}_2$. Em HFEV, seja por exemplo o polinômio oculto:

$$f(a) = a^{17} + \beta_{16}a^{16} + a^{12} + a^{10} + a^9 + \beta_8 a^8 + a^6 + a^5 + \beta_4 a^4 + a^3 + \beta_2 a^2 + \\ + \beta_1 a + \beta_0$$

onde $a=(a_1, \ldots, a_n)$ ($a_1, \ldots, a_n$ são as variáveis "óleo"), β_1, β_2, β_4, β_8, e β_{16} são dados por n funções lineares secretas nas v variáveis vinagre e β_0 é dado por n funções quadráticas secretas nas v variáveis vinagre. Neste exemplo, computamos uma assinatura como segue: as variáveis vinagre são escolhidas randomicamente e a equação de grau 17 resultante é resolvida em a.

Nota: Diferentemente de UOV, em HFEV temos termos em óleo x óleo (tais como a^{17}, a^{12}, a^{10}, etc), óleo x vinagre (tais como $\beta_{16}a^{16}$, $\beta_8 a^8$, etc) e vinagre x vinagre (em β_0).

Simulações

Nicolas Courtois fez algumas simulações em HFEV e, em todas as suas simulações, quando o número de variáveis vinagre é ≥3, não existem equações múltiplas afins de pequeno grau (o que é muito bom). Veja a versão estendida deste trabalho para mais detalhes.

11 Exemplos concretos de parâmetros para UOV

No presente, parece possível escolher por exemplo n=64, v=128 (ou v=192) e K=$\mathbf{F}_2$. O esquema de assinatura é o da seção 8, e o comprimento da assinatura é somente 192 bits (ou 256) neste caso. Mais exemplos de possíveis parâmetros são dados na versão estendida deste trabalho.

Nota: Se escolhemos K=$\mathbf{F}_2$ então a chave pública é freqüentemente grande. Assim é freqüentemente mais prático escolher um K maior e um n menor: então o comprimento da chave pública pode ser bastante reduzido.

Entretanto, mesmo quando K e n são fixados, é sempre viável fazer alguma transformação fácil em uma chave pública de modo a obter a chave pública de maneira canônica tal que esta expressão canônica é algo menor que a expressão original.

Veja a versão estendida deste trabalho para detalhes.

12 Exemplo concreto de parâmetros para HFEV

No presente, parece possível escolher um pequeno valor para v (por exemplo v=3) e um pequeno valor para d (por exemplo n=77, v=3, d=33 e K=$\mathbf{F}_2$). O esquema de assinatura é descrito na versão estendida deste trabalho (para evitar o paradoxo de aniversário).

Aqui o comprimento da assinatura é apenas 80 bits! Mais exemplos de possíveis parâmetros são dados na versão estendida deste trabalho.

13 Estado da arte (em maio de 1999) em esquemas de Chave-Pública com Polinômios Multivariáveis sobre um campo finito pequeno

Recentemente, muitas novas idéias foram introduzidas para o projeto de esquemas melhores, tais como UOV ou HFEV descritos neste trabalho. Outra idéia é fixar algumas variáveis para ocultar algumas propriedades algébricas, e uma outra idéia é a de introduzir algumas equações randômicas quadráticas e mistura-las com as equações originais: veja a versão estendida deste trabalho. Entretanto, muitas novas idéias também foram introduzidas para projetar melhores ataques sobre esquemas anteriores, tais como os – ainda não publicados – trabalhos [1], [2], [3], [5]. Assim o campo está se desenvolvendo rapidamente e pode parecer um tanto confuso

de início. Ademais, alguns autores utilizam a palavra "cripto-análise" no sentido de "quebrar" (decifrar) e alguns autores utilizam esta palavra com o significado de 'uma análise sobre a segurança" o que não necessariamente significa "quebrar". Nesta seção descrevemos o que entendemos no presente sobre os principais esquemas.

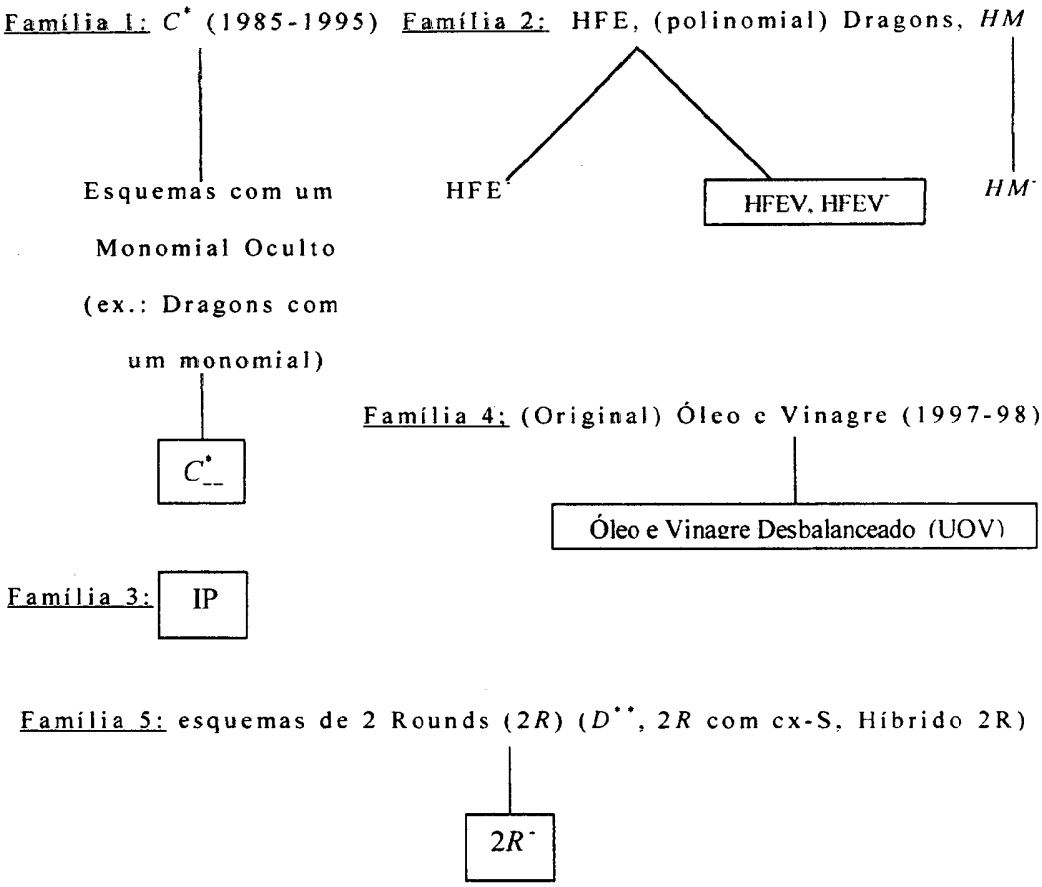
Nas grandes famílias da chave pública baseadas em polinomiais multivariáveis sobre um campo finito pequeno, podemos distinguir entre cinco famílias principais caracterizadas pelo modo que a porta de armadilha é introduzida ou pelo difícil problema sobre o qual depende a segurança. Na primeira família estão os esquemas "com um Monomial Oculto", *i.e.* a idéia chave e a de calcular uma exponenciação $x \mapsto x^d$ em um campo finito para o cálculo de chave secreta. Na segunda família estão os esquemas em que uma função polinomial (com mais de um monomial) é oculta. Na terceira família a segurança depende de um problema de isomorfismo.

Na quarta família, a segurança depende na dificuldade de achar a decomposição de dois polinômios multivariáveis quadráticos de toda ou parte de sua composição.

Finalmente, na quinta família, as computações de chave secreta são baseadas em computações Gaussianas.

Os principais esquemas nestas famílias são descritos na figura abaixo. O que pode ser o mais interessante

esquema em cada família está em um retângulo.



• C^* foi o primeiro esquema de todos, e pode ser visto como o ancestral de todos estes esquemas. Foi projetado em [12] e quebrado em [13].

• Esquemas com um Monomial Oculto (tais como alguns esquemas Dragon) foram estudados em [15], onde é mostrado que a maioria deles são inseguros. Entretanto, C^{*--} (estudado em[20] é (no presente) o mais eficiente esquema de assinatura (em tempo e RAM) em um cartão inteligente. O esquema não foi quebrado (mas pode parecer muito simples ou muito

próximo de C^* para ter uma grande confiança na sua segurança...).

• HFE foi projetado em [14]. Os resultados mais recentes sobre a sua segurança estão em [1] e [2]. Nestes trabalhos, ataques muito inteligentes são descritos. Entretanto, até o presente, parece que o esquema não foi quebrado desde que para parâmetros bem escolhidos e ainda parâmetros razoáveis os cálculos necessários para quebrá-lo ainda são muito grandes. Por exemplo, o primeiro desafio de US$ 500 oferecidos na versão estendida de [14] ainda não foram reclamados (é um puro HFE com n=80 e d=96 sobre $\mathbf{F}_2$).

• HFE$^-$ é apenas um HFE em que algumas das equações públicas não são publicadas. Devido a [1] e [2] pode ser recomendável fazer isto (a despeito do fato de que o HFE original poder ser seguro sem isto). Na versão estendida de [14] um segundo desafio de US$ 500 é descrito sobre um HFE$^-$.

• HEFV é descrito neste trabalho. HFEV e HFEV$^-$ parecem muito difíceis de serem quebrados. Ademais, HFEV é mais eficiente que o HFE original e pode dar assinaturas de chave pública de apenas 80 bits!

• *HM* e *HM*$^-$ foram projetados em [20]. Muito poucas análises foram feitas nestes esquemas (mas talvez possamos recomendar o uso de *HM*$^-$ ao invés de *HM*?).

• IP foi projetado em [14]. Esquemas IP tem a melhor prova de segurança até agora (veja [19]). IP é muito simples e pode

ser visto como uma bela generalização de Isomorfismo Gráfico.

- O Óleo e Vinagre original foi apresentado em [16] e quebrado em [10].
- UOV é descrito neste trabalho. Com o IP, são certamente os esquemas mais simples.
- $2R$ foi projetado em [17] e [18]. Devido a [3], é necessário ter no mínimo 128 bits na entrada, e devido a [5], pode ser prudente não publicar todas as (originais) equações públicas: isto dá aos algoritmos $2R^-$ (a eficiência dos algoritmos de decomposição dada em [5] sobre os esquemas $2R$ ainda não está completamente clara).

Observação 1: Estes esquemas são de interesse teórico mas (a exceção do IP) sua segurança não está diretamente relacionada a uma definição clara e é considerada um problema difícil. Assim será razoável implementá-los em produtos reais? Pensamos de fato ser algo arriscado depender toda segurança de aplicações sensitivas sobre tais esquemas. Entretanto, no presente, a maioria das aplicações de cartão inteligente utiliza algoritmos de chave secreta (por exemplo DES-triplo) por que cartões inteligentes RSA são mais caros. Assim pode ser razoável colocar em um cartão inteligente um dos esquemas prévios de chave pública em adição (não ao invés de) aos existentes esquemas de chave secreta. Então a segurança pode

apenas ser aumentada e o preço do cartão inteligente ainda seria baixo (coprocessador não necessário). A segurança dependeria então de uma chave mestra secreta para o algoritmo da chave secreta (com o risco de depender em uma chave mestre secreta) e em um esquema de baixo custo de chave pública (com o risco do esquema não ter prova de segurança).

Pode também ser percebido quando comprimento de assinatura extremamente curto (ou codificação de bloco curto) é necessário, não existe verdadeira opção: no presente apenas esquemas multivariáveis podem ter comprimento entre 64 e 256 bits.

Observação 2: Quando um novo esquema é encontrado com polinomiais multivariáveis, não necessariamente temos que explicar como a porta de armadilha foi introduzida. Então obtemos um tipo de "esquema de Chave Pública Secreta".

1 O esquema é claramente um esquema de Chave Pública uma vez que qualquer um pode verificar uma assinatura de uma chave pública (ou pode codificar de uma chave pública) e o esquema é secreto desde que o modo de calcular as computações da chave secreta (*i.e.* o modo que a porta de armadilha foi introduzida) não foi revelado e não pode ser adivinhada da chave pública. Por exemplo, poderíamos ter feito isto para HFEV (ao invés de publicá-lo).

13 Conclusão

Neste trabalho, apresentamos dois novos esquemas de chave pública com "variáveis vinagre": UOV e HFEV. O estudo de tais esquemas levou à análise de propriedades muito gerais sobre a solução de sistemas de formas gerais quadráticas. Ademais, da vista geral apresentada na seção 13, vemos que estes dois esquemas estão no presente entre os esquemas mais interessantes em duas das cinco famílias de esquemas baseadas em polinomiais multivariáveis sobre um campo finito pequeno. Será isto ainda verdade em alguns anos?

Referências

[1] Anônimo, *Cryptoanalisys of the HFE Public Key Cryptosystem*, ainda não publicado.

[2] Anônimo, *Practical cryptanalisys of Hidden Field Equations (HFE)*, ainda não publicado.

[3] Anônimo, *Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes*, not yet published.

[4] D. Coppersmith, *personal communication*, e-mail.

[5] Z. Dai, D. Ye, K. Y. Lam, *Factoring-attacks on Asymmetric Cryptography Based on Mapping-compositions*, not yet published.

[6] J. C. Faugere, *personal communication*.

[7] H. Fell, W. Diffie, *Analysis of a public key approach based on polynomial substitutions*, Anais da CRYPTO'85, Springer-Verlag, vol. 218, pp. 340-349.

[8] M. Garey, D. Johnson, *Computers and Intractability, a Guide to the Theory of NP-Completeness*, Freeman, p. 251.

[9] H. Imai, T. Matsumoto, *Algebraic Methods for Constructing Asymmetric Cryptosystems*, Algebrais Algorithms and Error Correcting Codes (AAECC-3), Grenoble, 1985, Springer-Verlag, LNCS n° 229.

[10] A. Kipnis, A. Shamir, *Cryptanalysis of the Oil and Vinegar Signature Scheme*, Anais do CRYPTO'98, Springer, LNCS n° 1462, pp. 257-266.

[11] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its applications, volume 20, Cambridge University Press.

[12] T. Matsumoto, H. Imai, *Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption*, Anais do EUROCRYPT'88, Springer-Verlag, pp. 419-453.

[13] Jacques Patarin, *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, Anais do CRYPTO'95, Springer-Verlag, pp. 248-261.

[14] J. Patarin, *Hidden Fields Equations(HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, Anais do EUROCRYPT'96, Springer,

pp.33-48.

[15] Jacques Patarin, *Asymmetric Cryptography with a Hidden Monomial*, Anais do CRYPTO'96, Springer, pp.45-60.

[16] J. Patarin, *The Oil and Vinegar Signature Scheme*, apresentado no Dagstuhl Workshop on Cryptography, setembro 1997 (transparencies).

[17] J. Patarin, L. Goubin, *Trapdoor One-way Permutations and Multivariate Polynomials*, Anais do ICICS'97 Springer, LNCS n° 1334, pp. 356-368.

[18] J. Patarin, L. Goubin, *Assymmetric Cryptography with S-Boxes*, Anais do ICICS'97, Springer, LNCS n° 1334, pp. 369-380.

[19] J. Patarin, L. Goubin, N. Courtois, *Improved Algorithms for Isomorphisms of Polynomials*, Anais do EUROCRYPT'98, Springer, pp. 184-200.

[20] J. Patarin, L. Goubin, N. Courtois, C^*_{-+} *and HM: Variations Around Two Schemes of T. Matsumoto and H Imai*, Anais do ASIACRYPT'98, Springer, pp.35-49.

[21] A. Shamir, *A simple scheme for encryption and its cryptanalysis found by D. Coppersmith and J. Stern*, apresentado no Luminy workshop em criptografia, setembro 1995.

REIVINDICAÇÕES

1) Método criptográfico de assinatura digital **caracterizado pelo** fato de que compreende:

suprir um conjunto S1 de k funções polinomiais como uma chave pública, o conjunto S1 incluindo as funções $P_1(x_1,..., x_{n+v}, y_1,..., y_k),..., P_k(x_1,..., x_{n+v}, y_1,..., y_k)$, onde k, v, e n são inteiros, $X_1,..., X_{n+v}$, são n+v variáveis de um primeiro tipo, $y_1, ... ,y_k$ são k variáveis de um segundo tipo, e o conjunto S1 é obtido pela aplicação de uma operação de chave secreta num conjunto S2 de k funções polinomiais $P'_1(a_1,..., a_{n+v}, y_1,..., y_k), ..., P'k(a_1,..., a_{n+v}, y_1,..., y_k)$, onde $a_1,..., a_{n+v}$ são n+v variáveis as quais incluem um conjunto de n variáveis "óleo" $a_1,..., a_n$, e um conjunto de v variáveis "vinagre" $a_{n+1},..., a_{n+v}$;

prover uma mensagem para ser assinada;

aplicar uma função de informação não significativa na mensagem para produzir uma série de k valores $b_1,..., b_k$;

substituir a série de k valores $b_1,..., b_k$ pelas variáveis $y_1,..., y_k$ do conjunto S2 respectivamente para produzir um conjunto S3 de k funções polinomiais $P''_1(a_1, ..., a_{n+v}),..., P''_k(a_1,..., a_{n+v})$;

selecionar v valores $a'_{n+1},..., a'_{n+v}$ para as v variáveis "vinagre" $a_{n+1},..., a_{n+v}$;

resolver um conjunto de equações $P''_1(a_1,..., a_n, a'_{n+1},..., a'_{n+v})= 0,...,P''_k(a_1,..., a_n, a'_{n+1},..., a'_{n+v})= 0$ para obter uma solução para $a'_1, ..., a'_n$; e

aplicar a operação de chave secreta para transformar $a'_1, ... ,a'_{n+v}$ para uma assinatura digital $e_1,..., e_{n+v}$.

2) Método, de acordo com a reivindicação 1, **caracterizado por** compreender a etapa de verificação da assinatura digital.

3) Método, de acordo com a reivindicação 2, **caracterizado por** a dita etapa de verificação compreende as etapas de:

obter a assinatura $e_1,..., e_{n+v}$, a mensagem, a função de informação não significativa e a chave pública;

aplicar a função de informação não significativa na mensagem para produzir a série de k valores $b_1,..., b_k$; e

verificar que as equações $P_1(e_1,..., e_{n+v}, b_1,..., b_k)= 0,..., P_k(e_1,..., e_{n+v}, b_1,..., b_k)= 0$ foram satisfeitas.

4) Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que o conjunto S2 compreende o conjunto f(a) de k funções polinomiais do esquema HFEV.

5) Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que o conjunto S2 compreende o conjunto S de k funções polinomiais do esquema UOV.

6) Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a dita etapa de suprimento compreende a etapa de selecionar o número v de variáveis "vinagre" para ser maior do que o numero n de variáveis "óleo".

7) Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que v é selecionado tal que q^v é maior do que 2^{32}, onde q é o número de elementos de um campo finito K.

8) Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a dita etapa de suprimento compreende a etapa de obter o conjunto S1 de um subconjunto S2' de k funções polinomiais do conjunto S2, o subconjunto S2' em que todos os coeficientes de componentes envolvendo quaisquer das variáveis $y_1,...,y_k$ nas k funções polinomiais $P'_1(a_1,..., a_{n+v}, y_1,..., y_k)$, ... , $P'_k(a_1,..., a_{n+v}, y_1,..., y_k)$ são zero, e o número v de variáveis "vinagre" e maior do que o número n de variáveis "óleo".

9) Método, de acordo com a reivindicação 8, **caracterizado pelo** fato de que o conjunto S2 compreende o conjunto S de k funções polinomiais do esquema UOV, e o número v de variáveis "vinagre" é selecionado de modo a satisfazer uma das seguintes condições:

(a) para cada característica p diferente de 2 de um campo K num esquema "Óleo e Vinagre" de grau 2, v satisfaz a desigualdade $q^{(v-n)-1} * n^4 > 2^{40}$,

(b) para p = 2 num esquema "Óleo e Vinagre" de grau 3, v é maior do que n*(1 + sqrt(3)) e menor do que ou igual a $n^3/6$, e

(c) para cada p diferente de 2 num esquema "Óleo e Vinagre" de grau 3, v é maior do que n e menor do que ou igual a n^4.

10) Método, de acordo com a reivindicação 8, **caracterizado pelo** fato de que o conjunto S2 compreende o conjunto S de k funções polinomiais do esquema UOV, e o número v de variáveis "vinagre" é selecionado de modo a satisfazer as desigualdades $v<n^2$ e $q^{(v-n)-1} * n^4 > 2^{40}$ para uma característica p=2 de um campo K num esquema "Óleo e Vinagre" de grau 2.

11) Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a dita operação de chave secreta compreende uma transformação s afim secreta nas n+v variáveis $a_1, \ldots, a^{n+v}$.

12) Método, de acordo com a reivindicação 4, **caracterizado pelo** fato de que o dito conjunto S2 compreende uma expressão que inclui k funções que são derivadas de um polinômio univariável.

13) Método, de acordo com a reivindicação 12, **caracterizado pelo** fato de que o polinômio univariável inclui um polinômio univariável de grau menor do que ou igual a 100.000.

14) Método criptográfico para verificação da assinatura digital, de acordo com a reivindicação 1, o método **caracterizado pelo** fato de que compreende:

obter a assinatura $e_1, \ldots, e_{n+v}$, a mensagem, a função de informação não significativa e a chave pública;

aplicar a função de informação não significativa na mensagem para produzir a série de k valores $b_1, \ldots, b_k$; e

verificar que as equações $P_1(e_1, \ldots, e_{n+v}, b_1, \ldots, b_k) = 0, \ldots, P_k(e_1, \ldots, e_{n+v}, b_1, \ldots, b_k) = 0$ foram satisfeitas.

15) Aperfeiçoamento num método de assinatura "Óleo e Vinagre" **caracterizado pelo** fato de que compreende a etapa de utilizar mais variáveis "vinagre" do que variáveis "óleo".

16) Método, de acordo com a reivindicação 15, **caracterizado pelo** fato de que o número v de variáveis "vinagre" é selecionado de modo a satisfazer uma das seguintes condições:

(a) para cada característica p diferente de 2 de um campo K e para um grau 2 do meto do de assinatura "Óleo e Vinagre", v satisfaz a desigualdade $q^{(v-n)-1} * n^4 > 2^{40}$,

(b) para p = 2 e para um grau 3 do método de assinatura "Óléo e Vinagre", v é maior do que n*(1 + sqrt(3)) e menor do que ou igual a $n^3/6$, e

(c) para cada p diferente de 2 e para um grau 3 do método de assinatura "Óleo e Vinagre", v é maior do que n e menor do que ou igual a n^4.

17) Método, de acordo com a reivindicação 15, **caracterizado pelo** fato de que o conjunto S2 compreende o conjunto S de k funções polinomiais do esquema DOV, e o número v de variáveis "vinagre" é selecionado de modo a satisfazer as desigualdades $v<n^2$ e $q^{(v-n)-1}* n^4 >2^{40}$ para uma característica p=2 de um campo K num esquema "Óleo e Vinagre" de grau 2.

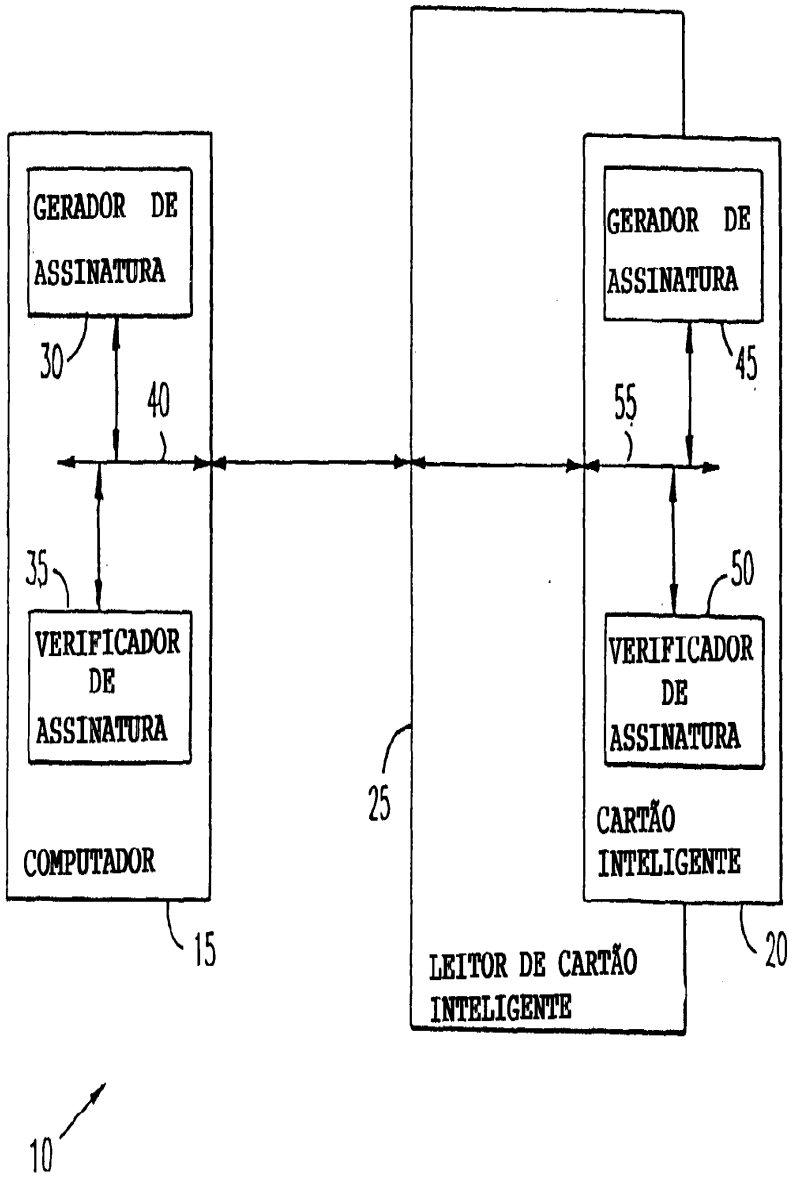

GERADOR DE ASSINATURA
30
40
35
VERIFICADOR DE ASSINATURA
COMPUTADOR
15
25
GERADOR DE ASSINATURA
45
55
50
VERIFICADOR DE ASSINATURA
CARTÃO INTELIGENTE
20
LEITOR DE CARTÃO INTELIGENTE
10

FIG. 1

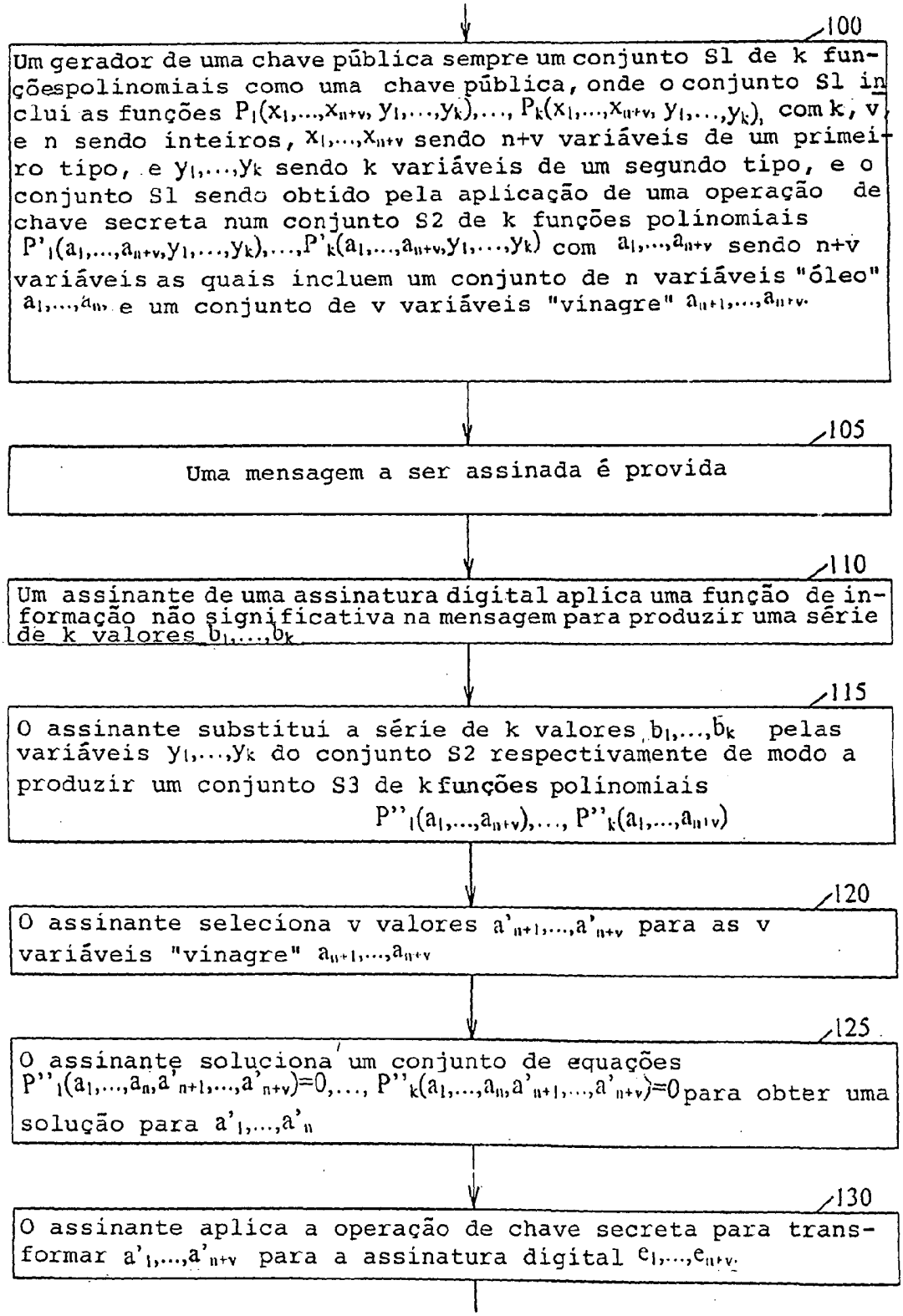

100
Um gerador de uma chave pública sempre um conjunto S1 de k funçõespolinomiais como uma chave pública, onde o conjunto S1 inclui as funções $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, com k, v, e n sendo inteiros, $x_1,...,x_{n+v}$ sendo n+v variáveis de um primeiro tipo, e $y_1,...,y_k$ sendo k variáveis de um segundo tipo, e o conjunto S1 sendo obtido pela aplicação de uma operação de chave secreta num conjunto S2 de k funções polinomiais $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ com $a_1,...,a_{n+v}$ sendo n+v variáveis as quais incluem um conjunto de n variáveis "óleo" $a_1,...,a_n$, e um conjunto de v variáveis "vinagre" $a_{n+1},...,a_{n+v}$.
105
Uma mensagem a ser assinada é provida
110
Um assinante de uma assinatura digital aplica uma função de informação não significativa na mensagem para produzir uma série de k valores $b_1,...,b_k$
115
O assinante substitui a série de k valores $b_1,...,b_k$ pelas variáveis $y_1,...,y_k$ do conjunto S2 respectivamente de modo a produzir um conjunto S3 de k funções polinomiais $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$
120
O assinante seleciona v valores $a'_{n+1},...,a'_{n+v}$ para as v variáveis "vinagre" $a_{n+1},...,a_{n+v}$
125
O assinante soluciona um conjunto de equações $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,..., P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ para obter uma solução para $a'_1,...,a'_n$
130
O assinante aplica a operação de chave secreta para transformar $a'_1,...,a'_{n+v}$ para a assinatura digital $e_1,...,e_{n+v}$.

FIG. 2A

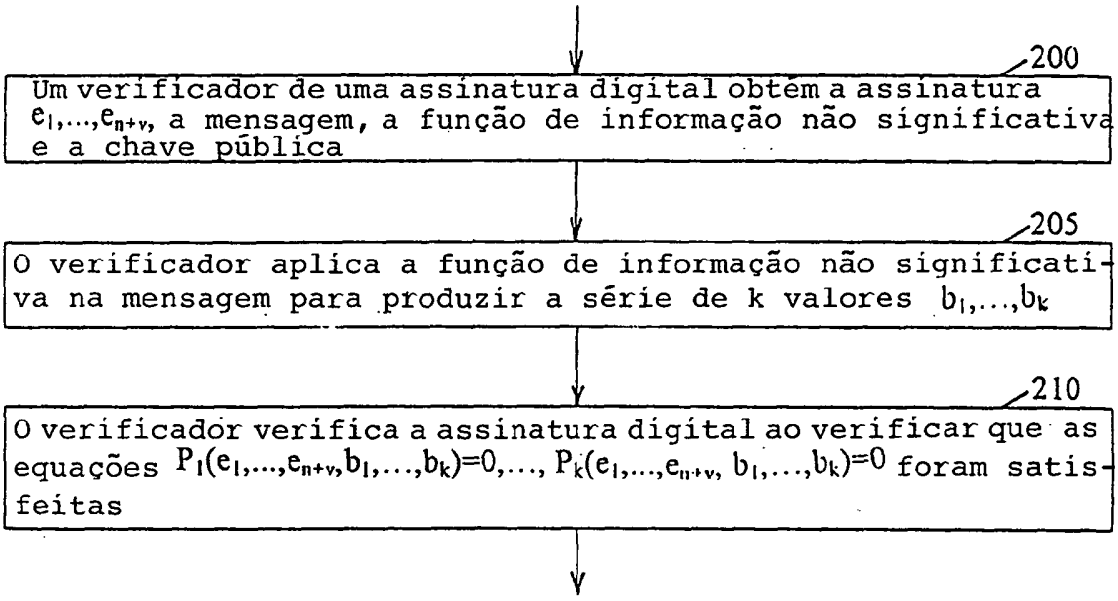

200
Um verificador de uma assinatura digital obtém a assinatura $e_1,\ldots,e_{n+v}$, a mensagem, a função de informação não significativa e a chave pública
205
O verificador aplica a função de informação não significativa na mensagem para produzir a série de k valores $b_1,\ldots,b_k$
210
O verificador verifica a assinatura digital ao verificar que as equações $P_1(e_1,\ldots,e_{n+v},b_1,\ldots,b_k)=0,\ldots, P_k(e_1,\ldots,e_{n+v}, b_1,\ldots,b_k)=0$ foram satisfeitas

FIG. 2B

RESUMO

SISTEMAS E MÉTODOS DE ASSINATURA DE CHAVE PÚBLICA

A invenção diz respeito a um método criptográfico para assinatura digital.

Um conjunto S1 de k funções polinomiais $P_k(x_1, ...,x_{n+v}, y_1, ...,y_k)$ são supridas como uma chave pública, onde k, v, e n são inteiros, $x_1, ...,x_{n+v}$ são n+v variáveis de um primeiro tipo, e $y_1, ..., y_k$ são k variáveis de um segundo tipo, o conjunto S1 sendo obtido pela aplicação de uma operação de chave secreta num dado conjunto S2 de k funções polinomiais $P'_k(a_1, ..., a_{n+v}, y_1, ..., y_k)$, $a_1, ..., a_{n+v}$ designando n+v variáveis que incluem um conjunto de n variáveis "óleo" e v "vinagre". Uma mensagem a ser assinada é provida e submetida a uma função de informação não significativa para produzir uma série de k valores $b_1, ..., b_k$. Estes k valores são substituídos pelas k variáveis $y_1, ..., y_k$ do conjunto S2 para produzir um conjunto S3 de k funções polinomiais $P''_k(a_1, ..., a_{n+v})$, e v valores $a'_{n+1}, ..., a'_{n+v}$ são selecionados para as v variáveis "vinagre". Um conjunto de equações $P''_k(a_1, ..., a'_{n+v})=0$ é resolvido para obter uma solução para $a'_1, ..., a'_n$ e a operação de chave secreta é aplicada para transformar a solução para a assinatura digital.