UNIVERSIDADE DE SÃO PAULO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

Sistemas Criptográficos Baseados em Identidades

Waldyr Dias Benits Júnior

Orientador: Prof. Dr. Routo Terada

Relatório apresentado ao Instituto de Matemática e Estatística da Universidade de São Paulo, como exigência da disciplina MAC 5701 - Tópicos em Ciência da Computação.
Área de Concentração: Criptografia.

São Paulo
2003

Sistemas Criptográficos baseados em Identidades

29 de maio de 2003

Resumo

O emprego de curvas elípticas em criptografia permitiu o aparecimento de uma criptografia assimétrica em que a chave pública de um usuário não é uma seqüência aleatória de *bits* e sim um identificador que caracteriza este usuário de forma única, como por exemplo seu número de CPF ou seu endereço eletrônico. Tal fato possibilitou que se estabeleça uma comunicação segura sem troca de segredos, sem troca de certificados digitais e sem a necessidade de se manter um diretório público de chaves. Este esquema de criptografia assimétrica, que será apresentado neste relatório, é hoje conhecido como criptografia baseada em identidades pessoais (ID-*based cryptosystems*) e será o tema de nossa pesquisa.

Palavras chaves: Sistemas baseados em identidades, Emparelhamento, Bilinearidade, Criptografia em curvas elípticas.

1 Introdução

O conceito de criptografia baseada em identidades pessoais surgiu em 1984, com Shamir, A. [SHA 84]. Neste artigo, o autor propôs um novo modelo de esquema criptográfico, que permitiria a qualquer par de usuários se comunicar de forma segura, sem que fosse necessária a troca de chaves secretas, como ocorre na criptografia simétrica, e sem que fosse preciso utilizar certificados digitais para autenticar chaves públicas, que é o caso da criptografia assimétrica tradicional.

Neste novo esquema, segundo Shamir, existe um Gerador de Chaves Particulares (PKG - *Private Key Generator*), cuja única função é gerar uma chave particular para um usuário solicitante e transmiti-la ao mesmo por um canal seguro. Naturalmente, antes de gerar e distribuir esta chave, o PKG fará uma cuidadosa investigação com o objetivo de autenticar o solicitante, da mesma forma que ocorre em uma verificação de identidade para emissão de certificados na criptografia assimétrica tradicional. Como "canal seguro", poderíamos imaginar que o solicitante compareça pessoalmente ao PKG, onde receberá sua chave particular gravada, por exemplo, em um cartão inteligente (*smart card*). Neste caso, antes de receber sua chave particular, este usuário deverá provar sua identidade. Diferentemente da criptografia assimétrica tradicional, após

gerar e distribuir as chaves particulares, o PKG não precisa mais participar da comunicação, permitindo que a rede funcione de forma totalmente descentralizada. Além disso, neste novo esquema não é preciso que os centros coordenem suas atividades e nem mantenham lista de seus usuários, como ocorre na infra-estrutura de chaves públicas. Ainda de acordo com Shamir, o esquema proposto é ideal para grupos fechados, como por exemplo em uma cadeia de lojas ou de bancos, onde a matriz pode fazer o papel de PKG.

O modelo proposto por Shamir baseia-se no esquema de criptografia assimétrica tradicional, sendo que, em vez de termos um par de chaves representadas por uma seqüência de *bits*, sendo uma aleatória, e a outra calculada em função da primeira, como no caso do RSA[1], teremos como chave pública um identificador, ou seja, uma característica que identifique o usuário de forma única, de modo que ele não tenha como negar que esta informação diz respeito a ele. Como exemplos de identificador, poderíamos citar o número do CPF ou o endereço eletrônico (*e-mail*).

A grande vantagem deste esquema é que, ao contrário da criptografia assimétrica tradicional, não há necessidade de se fazer um mapeamento entre uma chave pública e seu dono através de um certificado digital, haja vista que nesse caso, a chave pública identifica o dono. Sendo assim, evita-se um grande problema que ocorre na tradicional infra-estrutura de chaves públicas, pois se uma chave particular eventualmente for comprometida, a segurança da comunicação fica vulnerável durante o período de tempo que foi solicitada a revogação do certificado digital e a efetiva revogação do mesmo.

Uma outra vantagem é que, por não ser mais um número aleatório, um usuário Beto não precisa reservar espaço adicional para guardar as chaves públicas das pessoas com quem deseja se comunicar, pois pode usar sua própria lista de endereços eletrônicos. Estas características fazem com que a criptografia assimétrica baseada em identidades se assemelhe ao correio físico, ou seja, se você conhece o endereço de uma pessoa, você pode enviar-lhe uma mensagem, de modo que somente ela poderá ler. Com base no mesmo conceito, se Alice deseja enviar uma mensagem sigilosa para Beto, ela necessita apenas do endereço eletrônico de Beto, ou seja, não é preciso nem mesmo ter algum conhecimento sobre chaves ou protocolos de comunicação.

Neste mesmo artigo em que apresentou o modelo de sistema criptográfico baseado em identidade [SHA 84], Shamir propôs um esquema de assinatura, cuja segurança, assim como no RSA, se baseia na dificuldade de fatoração de números primos grandes, e considerou como um problema em aberto um modelo de criptografia baseado em identidade. Desde então, vários pesquisadores tentaram, sem sucesso, desenvolver um esquema de criptografia baseado em identidades, obedecendo a propriedade de não expor a chave particular do PKG. Algumas soluções propostas requeriam que os usuários não entrassem em conluio, em outras o PKG gastaria um tempo muito grande na geração de cada chave particular solicitada e em outras havia a necessidade de que o *hardware* fosse resistente a fraudes. Somente com o esquema proposto por Boneh & Franklin [BON 01],

[1] Algoritmo de criptografia assimétrica, proposto por Rivest, Shamir e Adleman [RIV 78].

baseado em propriedades de curvas elípticas, conseguiu-se uma solução satisfatória para criptografia com chaves baseadas em identidades.

Este relatório está organizado da seguinte forma: na seção 2 veremos as notações que serão utilizadas ao longo deste trabalho e os conceitos principais de criptografia com curvas elípticas; na seções 3 e 4, os conceitos de criptografia e assinatura baseados em identidades, respectivamente; na seção 5 comentaremos as principais vantagens e desvantagens de um esquema baseado em identidades, e finalmente, na seção 6 concluiremos este relatório e apresentaremos os assuntos que pretendemos estudar na segunda fase de nossa pesquisa, bem como um calendário de atividades que pretendemos seguir até a data da defesa da dissertação.

2 Definições e notações iniciais

Um sistema de criptografia baseado em identidade envolve uma série de notações e conceitos matemáticos, que nesta seção serão elucidados, para possibilitar um melhor entendimento do leitor.

2.1 Gerador de chaves particulares (PKG)

Definiremos Gerador de chaves particulares, também conhecido como Autoridade de confiança (TA) ou ainda como centro gerador de chaves (KGC), como uma entidade idônea que tem como principal objetivo gerar uma chave particular baseada em identidade, a partir do identificador de um usuário solicitante, e transmitir esta chave ao mesmo por um canal seguro. A fim de garantirmos o sucesso dos esquemas de criptografia e assinatura baseados em identidade que iremos apresentar, vamos considerar a hipótese de que a idoneidade deste PKG é inquestionável, ou seja, podemos confiar nele incondicionalmente. Vamos então nos referir ao PKG "totalmente idôneo" como Autoridade de confiança (TA).

2.2 Problema do Logaritmo Discreto (PLD)

Muitos sistemas criptográficos baseiam-se na dificuldade computacional do Problema do Logaritmo Discreto, que Terada, R.[TER 00] define como:

> Dados um número primo p e números inteiros g, t, tais que $0 < g, t < p$, calcular um inteiro s tal que
>
> $$t = g^s mod\ p$$

Para números pequenos, conseguimos calcular s atribuindo valores, até que o resultado desejado seja encontrado. Veja no exemplo ilustrativo a seguir:

Exemplo 1: Para $p = 13$, $g = 2$ e $t = 12$, calcular s tal que $12 = 2^s mod 13$.

s	$2^s mod 13$
0	1
1	2
2	4
3	8
4	3
5	6
6	**12**

Resposta: O valor de s é 6.

Entretanto, à medida que o valor de p aumenta, este método, conhecido como "força bruta" se torna inviável. Ainda não se conhece nenhum algoritmo de tempo polinomial, pelo menos até o momento em que foi escrito este trabalho, que resolva o problema do logaritmo discreto. Portanto, o PLD se enquadra na classe de problemas computacionalmente difíceis e devido a isto, é muito usado em sistemas criptográficos.

2.2.1 PLD em Curvas Elípticas (PLD - CE)

O PLD com aplicação em Curvas Elípticas é chamado de "Problema do Logaritmo Discreto em Curvas Elípticas", e é enunciado por Terada, R.[TER 00] da seguinte forma:

> Dados dois pontos R, P, de uma curva elíptica definida sobre um corpo finito, achar um inteiro s tal que[2]

$$R = sP \tag{1}$$

Em Silverman, J. [SIL 86] e Barreto, P. et al.[BAR 99] o leitor encontrará as principais operações utilizadas em curvas elípticas. Para prosseguir com o entendimento deste relatório, porém, basta apenas ter em mente que, da equação (1), o valor s está protegido pelo PLD - CE, ou seja, "é computacionalmente inviável se calcular s, dado que conhecemos os pontos R e P".

2.3 Bilinearidade

Quando trabalhamos com curvas elípticas em criptografia, uma propriedade que utilizaremos muito é a bilinearidade. Dizemos que um emparelhamento[3] de pontos de uma curva elíptica (denominado $e(P, Q)$) é bilinear quando podemos

[2] Podemos interpretar "sP" na equação (1) como sendo $\underbrace{P + P + P + \ldots + P}_{S \text{ vezes}}$

[3] No artigo de Boneh & Franklin [BON 01] o leitor poderá ver uma definição formal de emparelhamento, embora não seja necessária para o entendimento do restante deste relatório.

mover livremente os expoentes e multiplicadores sem alterar o resultado do emparelhamento, conforme podemos ver abaixo (P, Q são pontos da curva e $a, b, c \in \mathbb{Z}^*$):

$$\begin{array}{rcccccc} e(aP,bQ)^c & = & e(aP,cQ)^b & = & e(bP,cQ)^a & = & e(bP,aQ)^c \\ & = & e(abP,Q)^c & = & e(P,abQ)^c & = & e(cP,abQ) \\ & = & \cdots & & & & \\ & = & e(abcP,Q) & = & e(P,abcQ) & = & e(P,Q)^{abc} \end{array}$$

Resumindo a propriedade acima, temos:

$$e(aP,bQ)^c = e(P,Q)^{abc} \tag{2}$$

Além disso, a seguinte propriedade também se aplica a uma função bilinear:

$$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q) \tag{3}$$

cuja recíproca também vale:

$$e(P, Q_1)e(P, Q_2) = e(P, Q_1 + Q_2) \tag{4}$$

É importante ressaltar que, em termos computacionais, o cálculo de um emparelhamento tem ordem de grandeza maior do que uma exponenciação em $\mathbb{F}_q$, segundo Cha, J.C. e Cheon, J.H. [CHA 02], sendo portanto, a operação de `maior custo computacional` em sistemas criptográficos baseados em identidades, segundo Barreto, P., Lynn, B. e Scott, M. [BAR 02].

2.4 Nomenclatura básica

Tendo entendido as propriedades principais do PLD-CE e da bilinearidade, podemos prosseguir com as notações utilizadas. Considere que para os grupos $\mathbb{G}_1$ e $\mathbb{G}_2$ o problema do logaritmo discreto é assumidamente difícil e existe um mapeamento bilinear computável.
Sejam:
q: número primo longo[4]
$\mathbb{G}_1, \mathbb{G}_2$: grupos[5] de ordem prima q
$\mathbb{F}_q$: corpo finito de ordem q.
$t : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$: emparelhamento de *Tate*[6]

Se escrevermos $\mathbb{G}_1$ em notação aditiva e $\mathbb{G}_2$ em notação multiplicativa, podemos, na prática, considerar:
$\mathbb{G}_1$: subgrupo de um grupo aditivo de pontos de uma curva elíptica sobre $\mathbb{F}_q$
$\mathbb{G}_2$: subgrupo de um grupo multiplicativo de um corpo finito $\mathbb{F}^*_{q^k}$ para algum $k \in \mathbb{Z}^*$

[4] Em termos práticos, q é da ordem de 2^{160}.

[5] A definição algébrica de grupo, subgrupo, ordem e corpo finito pode ser vista em Terada, R.[TER 00]

[6] Um outro emparelhamento muito usado é o de *Weil*, mas Barreto, P.[BAR 99] e Galbraith, S. *et al.*[GAL 02] mostram que a implementação do emparelhamento de *Tate* é mais eficiente.

2.4.1 Funções de Espalhamento

Terada, R. [TER 00] define uma função de espalhamento (*Hash*) da seguinte forma:

> "Dado um valor x, de tamanho qualquer, uma função de espalhamento calcula um valor y de tamanho fixo, relativamente menor do que o tamanho de x. Por exemplo, x pode ser um texto da ordem de centenas de bytes e $|y|$ é da ordem de 128 *bits*. O valor y é chamado de resumo de x".

Uma importante característica das funções de espalhamento é que elas são não-inversíveis, *i.e.*, se H é uma função de espalhamento, é computacionalmente fácil calcular y tal que $H(x) = y$. Porém, é computacionalmente inviável, dado y, recuperar o valor de x.

Serão utilizadas as seguintes funções de espalhamento:

$$\begin{array}{lll} H_1: & \{0,1\}^* & \longrightarrow \mathbb{G}_1 \\ H_2: & \{0,1\}^* & \longrightarrow \mathbb{F}_q \\ H_3: & \mathbb{G}_2 & \longrightarrow \{0,1\}^* \end{array}$$

Em outras palavras, H_1 mapeia uma seqüência de *bits* de tamanho aleatório em um ponto da curva elíptica; H_2 mapeia uma seqüência de *bits* de tamanho aleatório em um corpo finito de ordem q e H_3 mapeia o resultado de um emparelhamento entre dois pontos da curva em uma seqüência de *bits* de tamanho aleatório.

2.5 Chaves utilizadas

Antes de darmos início ao esquema de criptografia baseada em identidade, vamos definir os tipos de chaves que serão utilizadas.

- Par de chaves pública/ particular padrão[7] (R,s)

Sejam $R \in \mathbb{G}_1$, $s \in \mathbb{F}_q$ e P um ponto fixo pertencente a $\mathbb{G}_1$ e de conhecimento público. Temos que:

$$R = sP \tag{5}$$

- Par de chaves baseadas em identidade(Q_{ID},S_{ID})

Sejam $Q_{ID}, S_{ID} \in \mathbb{G}_1$ e existe uma Autoridade de Confiança com um par de chaves padrão (R_{TA}, s) de modo que valem as seguintes relações:

$$S_{ID} = sQ_{ID} \tag{6}$$

$$Q_{ID} = H_1(ID) \tag{7}$$

[7] Este é um par de chaves assimétricas produzido por um algoritmo baseado em curvas elípticas. Quando nos referirmos a um par de chaves gerado por um algoritmo como o RSA, por exemplo, usaremos a denominação par de chaves tradicional.

Onde ID é o identificador (p. ex. um endereço eletrônico: alice@ime.usp.br).

Note pela equação (6) que, mesmo se Beto possui um par de chaves válido (Q_{beto}, S_{beto}), ele não consegue recuperar a chave particular s da Autoridade de confiança, pois esta chave está protegida pelo PLD-CE. O leitor mais atento deverá ter notado que neste tipo de sistema, diferentemente da criptografia assimétrica tradicional, a Autoridade de confiança tem conhecimento da chave particular de todos os seus usuários. Tal fato é chamado de custódia de chaves (*key escrow*) e será discutido mais adiante.

3 Criptografia em sistemas baseados em identidade

Vamos entrar agora, nos sistemas criptográficos baseados em identidade propriamente ditos, iniciando com a criptografia baseada em identidades (IBE - *Identity-Based Encryption*). Sejam (Q_{beto}, S_{beto}) o par de chaves baseadas em identidade de um usuário Beto; R_{TA} a chave pública padrão da Autoridade de confiança que gerou a chave particular de Beto; e m a mensagem que Alice deseja enviar para Beto.

Veremos a seguir o modelo proposto por Boneh & Franklin [BON 01] de criptografia baseada em identidade.

3.1 Criptografia

Alice escolhe um elemento aleatório r, tal que $r \in \mathbb{F}_q$ e calcula[8]:

$$\begin{cases} U &= rP \\ V &= m \oplus H_3(t(R_{TA}, rQ_{beto})) \end{cases} \tag{8}$$

E envia o texto criptografado (U, V) para Beto.
Boneh & Franklin, em seu artigo, não destacam a importância na escolha de r. É importante que o elemento aleatório r escolhido por Alice seja diferente para cada mensagem a ser criptografada (números com esta característica são conhecidos na literatura como "NONCE": *Number used ONCE.*); caso contrário, haverá uma falha de segurança que veremos mais adiante. Note que Alice utiliza a chave pública baseada em identidade de Beto para criptografar m. Para isto, basta que ela conheça o identificador de Beto (p. ex. beto@ime.usp.br).

3.2 Decriptografia

Beto, recebendo (U, V) de Alice, faz o seguinte cálculo para recuperar o legível m:

$$m = V \oplus H_3(t(U, S_{beto})) \tag{9}$$

[8] A operação $\oplus$ representa o ou-exclusivo *bit* a *bit*.

Vemos que Beto utiliza sua chave particular baseada em identidade para recuperar m.

3.3 Demonstração

Queremos demonstrar que Beto, através do cálculo efetuado na equação (9) consegue, de fato, recuperar m.

$$
\begin{aligned}
V \oplus H_3(t(U, S_{beto})) &= V \oplus H_3(t(rP, S_{beto})), && \text{pois } U = rP \text{ de (8)} \\
&= V \oplus H_3(t(rP, sQ_{beto})), && \text{pois } S_{beto} = sQ_{beto} \text{ de (6)} \\
&= V \oplus H_3(t(P, Q_{beto}))^{rs}, && \text{por bilinearidade} \\
&= V \oplus H_3(t(sP, rQ_{beto})), && \text{por bilinearidade} \\
&= V \oplus H_3(t(R_{TA}, rQ_{beto})), && \text{pois } R_{TA} = sP \text{ de (5)} \\
&= m, && \text{pois pela equação (8)} \\
& && V = m \oplus H_3(t(R_{TA}, rQ_{beto}))
\end{aligned}
$$

Boneh & Franklin [BON 01] definem este modelo de criptografia baseado em identidade através de quatro algoritmos, chamados de configuração (*setup*), extração (*extract*), criptografia (*encrypt*) e decriptografia (*decrypt*), que resumiremos a seguir:

Configuração

- Seleção dos parâmetros q, $\mathbb{G}_1$, $\mathbb{G}_2$, P e t;
- Escolha da chave particular s, tal que $s \in \mathbb{Z}_q^*$ e cálculo da chave pública R_{TA}, conforme equação (5);
- Escolha das funções de espalhamento H_1 e H_3.

Os parâmetros do sistema são os valores públicos $(q, \mathbb{G}_1, \mathbb{G}_2, t, P, R_{TA}, H_1, H_3)$. A chave particular s é também chamada de chave mestra.

Extração

- cálculo de Q_{ID}, para um dado ID, conforme equação (7);
- cálculo da chave particular S_{ID} baseada em identidade, conforme equação (6).

Criptografia

- cálculo de (U, V), conforme equação (8).

- recuperação do legível m, conforme equação (9).

Os algoritmos configuração e extração são executados pela Autoridade de confiança (TA) e os algoritmos criptografia e decriptografia pelos participantes da comunicação.

3.4 Importância da escolha do elemento aleatório r

Vimos na equação (8) que Alice deve escolher um r diferente para cada mensagem que deseja criptografar. O que aconteceria se ela escolhesse sempre o mesmo r ?

Suponha que Alice enviou as mensagens m_1 e m_2 para Beto e não teve a preocupação de selecionar dois r distintos. Pelas equações (8), vemos que o valor de U será o mesmo, tanto para m_1 quanto para m_2, apenas os valores de V serão diferentes para cada mensagem. Sejam então V_1 e V_2 os valores calculados por Alice, sobre m_1 e m_2, respectivamente. Da mesma forma, como r é o mesmo para m_1 e m_2, o valor de $H_3(t(R_{TA}, rQ_{beto}))$ permanece constante. Vamos chamar este valor de x. Desta forma, podemos reescrever a segunda equação de (8) como:

$$\begin{cases} V_1 &= m_1 \oplus x \\ V_2 &= m_2 \oplus x \end{cases}$$

Se um intruso Carlos interceptar os valores V_1 e V_2, ele pode calcular:

$$\begin{aligned} V &= V_1 \oplus V_2 \\ &= (m_1 \oplus x) \oplus (m_2 \oplus x) \\ &= m_1 \oplus m_2 \end{aligned}$$

Conhecendo o valor de V, se o intruso conseguir ter acesso a m_1 (s.p.g.)[9], pode realizar um ataque de "texto legível conhecido" e recuperar m_2.

4 Assinatura em sistemas baseados em identidade

Existem diversos sistemas de assinatura baseados em identidade, como Paterson, K.[PAT 02], Cha, J.C. e Cheon, J.H.[CHA 02], Hess, F.[HES 02] e outros. Vamos apresentar aqui o esquema de Hess, que é mais eficiente que os demais, segundo Chen, L. *et al.*[CHE 02].

[9] sem perda de generalidade

4.1 Assinatura

Alice, querendo assinar uma mensagem m, primeiramente escolhe um valor $k \in \mathbb{F}_q$ e um ponto aleatório $P_1 \in \mathbb{G}_1^*$ e calcula:

$$r = t(P_1, P)^k \tag{10}$$

Em seguida, calcula[10]

$$h = H_2(m||r) \tag{11}$$

E finalmente,

$$U = hS_{alice} + kP_1 \tag{12}$$

Onde a assinatura de m é (U, h).

Note em (12) que Alice usa sua chave particular S_{alice} para gerar a assinatura de m. Observe também que a "soma" na equação (12) representa uma soma de pontos, pois hS_{alice} e kP_1 são pontos de uma curva elíptica.

4.2 Verificação

Se Beto deseja verificar se a assinatura é realmente de Alice, faz o seguinte cálculo:

$$r = t(U, P).t(Q_{alice}, -R_{TA})^h \tag{13}$$

Onde $-R_{TA}$ é o ponto simétrico de R_{TA} em relação ao eixo das abscissas.
Após calcular r, Beto aceita a assinatura de Alice como válida se, e somente se:

$$h = H_2(m||r) \tag{14}$$

Note que somente valores públicos são utilizados na verificação de uma assinatura.

4.3 Demonstração

Vamos demonstrar que a equação (13) é satisfeita para uma assinatura válida. Observe que são empregadas as propriedades de bilinearidade, vistas nas equações (3) e (4).

[10] O termo || na equação (11) significa "concatenar".

$$
\begin{aligned}
t(U,P).t(Q_{alice},-R_{TA})^h &= t(hS_{alice}+kP_1,P).t(Q_{alice},-R_{TA})^h \\
&= t(hS_{alice}+kP_1,P).t(Q_{alice},-sP)^h \\
&= t(hS_{alice}+kP_1,P).t(Q_{alice},-P)^{sh} \\
&= t(hS_{alice}+kP_1,P).t(sQ_{alice},P)^{-h} \\
&= t(hS_{alice}+kP_1,P).t(S_{alice},P)^{-h} \\
&= t(hS_{alice}+kP_1,P).t(-hS_{alice},P) \\
&= t(hS_{alice}-hS_{alice}+kP_1,P) \\
&= t(kP_1,P) \\
&= t(P_1,P)^k \\
&= r \qquad \text{(pela equação (10))}
\end{aligned}
$$

Note que, como h é parte da assinatura de m, mesmo que ele tenha sido alterado por um ataque de modificação, a equação (13) será satisfeita. Para que Beto possa garantir que (U,h) é a assinatura da mensagem m, após calcular o valor de r, ele ainda deve verificar a condição da equação (14). Caso o h encontrado por Beto, com base no valor de r que ele acabou de calcular seja diferente do valor de h que ele recebeu na assinatura de Alice, Beto rejeita a assinatura.

5 Vantagens e desvantagens

Relacionaremos, a seguir, as principais vantagens e desvantagens dos sistemas criptográficos baseados em identidades.

- VANTAGENS

- NÃO É NECESSÁRIO UM DIRETÓRIO DE CHAVES PÚBLICAS.
  Como vimos, a chave pública baseada em identidades é alguma característica que identifique o usuário de forma única, chamada de identificador (na verdade, vimos que a chave é o resultado de uma função de espalhamento sobre este identificador, mas como esta função de espalhamento é de conhecimento público, podemos simplificar dizendo que a chave pública é o identificador). Desta forma, se pensarmos que o identificador é o endereço eletrônico de um usuário, uma vez conhecendo este endereço eletrônico (e, obviamente, precisamos conhecer, se quisermos enviar-lhe uma mensagem

via *web*), podemos enviar-lhe mensagens sigilosas, sem que seja necessário recorrermos a um diretório de chaves públicas.

- Qualquer entidade que possua um par de chaves padrão pode fazer o papel de PKG
  Vimos que o PKG tem conhecimento de todas as chaves particulares de seus usuários. Este fato, nem sempre, é desejável. Considere, por exemplo, uma empresa que trata de assuntos sensíveis. Se o PKG fosse uma entidade externa à empresa, ela teria acesso a todas as mensagens tramitadas na empresa, o que pode vir a se tornar um problema (suponha que este PKG foi subornado pela empresa concorrente). Com sistemas baseados em identidade, basta que uma entidade possua um par de chaves padrão, como vimos na seção 2.5 para que possa gerar as chaves baseadas em identidade. Portanto, o Presidente da empresa pode fazer o papel de Autoridade de confiança.

- O PKG tem conhecimento de todas as chaves particulares de seus usuários.
  Este fato é conhecido como custódia de chaves e embora nem sempre seja desejável (e por esta razão, também o incluímos nas desvantagens), em algumas situações, pode ser conveniente a possibilidade de recuperação de chaves particulares.
  Vamos aproveitar a situação descrita na vantagem anterior, onde o Presidente da empresa age como Autoridade de confiança. Neste caso, o conhecimento das chaves particulares é desejável. Imagine que um diretor da empresa sofreu um grave acidente e não tem condições de acessar seus arquivos nem confiar sua chave para uma terceira pessoa. Como o presidente gerou a chave particular deste diretor, ele conhece esta chave e, portanto, pode recuperar os arquivos de interesse da empresa que tenham sido criptografados com a chave pública baseada em identidade deste diretor.
  Uma outra situação em que o conhecimento das chaves particulares pode ser desejável é o assunto "Segurança Nacional", onde órgãos de inteligência do Governo podem desejar ter acesso a informações que possam vir a comprometer a soberania de uma Nação. Mas definirmos até que ponto deve ir a intervenção do Estado nos assuntos privados é um assunto delicado, e portanto, vamos deixar de lado estas discussões por não fazerem parte do escopo deste trabalho.

- Alice pode enviar mensagens criptografadas para Beto mesmo se ele ainda não obteve seu par de chaves do Gerador de Chaves Particulares (PKG).
  Diferentemente dos sistemas de chave pública tradicionais, em que a chave pública é uma seqüência aleatória de bits, e portanto deve ser previamente calculada, juntamente com seu par (chave particular), para que uma mensagem possa ser enviada, nos sistemas baseados em identidade Alice pode enviar uma mensagem sigilosa para Beto antes mesmo de ele ter obtido

seu par de chaves baseadas em identidade de um PKG.
Alice precisa apenas da chave pública padrão da Autoridade de confiança que irá gerar o par de chaves de Beto. Caso Alice tenha conhecimento desta Autoridade de confiança (por exemplo, digamos que a autoridade em questão é o presidente da empresa em que Alice trabalha e que Beto acabou de ser admitido nesta empresa, mas ainda não obteve seu par de chaves baseadas em identidade), ela envia uma mensagem criptografada, utilizando como identificador o endereço eletrônico de Beto. Beto, por sua vez, ao receber a mensagem criptografada, precisará apenas solicitar um par de chaves à Autoridade de confiança usando seu *e-mail* como identificador e então, decriptografar a mensagem.

- NÃO É NECESSÁRIO ALICE OBTER O CERTIFICADO DA CHAVE PÚBLICA DE BETO.
Diferentemente da criptografia assimétrica tradicional, onde não há nenhuma relação entre o usuário e sua chave pública, nos sistemas baseados em identidade a chave pública é uma característica que identifica o usuário de forma única e que ele não tem como negar que esta característica diz respeito a ele. Portanto, não há a necessidade de certificados digitais para autenticar chaves públicas e, conseqüentemente, não ocorre o problema de revogação de certificados e nem tampouco há necessidade de se estabelecer uma infra-estrutura de chaves públicas.

- **DESVANTAGENS**

- O PKG TEM CONHECIMENTO DE TODAS AS CHAVES PARTICULARES DE SEUS USUÁRIOS.
Resolvemos repetir este item, agora como desvantagem, pois dependendo da situação, o conhecimento de chaves particulares (custódia de chaves) por uma entidade externa pode causar sérios problemas de segurança (p. ex. como no caso de suborno do PKG, comentado anteriormente).

  Uma outra situação indesejável que poderá ocorrer, novamente desconsiderando a hipótese de que o PKG seja incondicionalmente confiável, é que este pode forjar a assinatura de qualquer um dos usuários para os quais gerou chaves baseadas em identidades, pois conhece as chaves particulares de cada um deles. Um esquema de assinatura proposto por [CHE 03], que iremos ver na segunda fase de nossa pesquisa, resolve este problema, garantindo ao usuário a possibilidade de provar que uma determinada assinatura foi forjada pelo PKG.

- DIFICULDADE DE IMPLEMENTAÇÃO DO EMPARELHAMENTO DE *TATE*.
Vimos que, em termos computacionais, o cálculo do emparelhamento em curvas elípticas é a operação de maior custo. Dependendo da forma como é implementado, um sistema criptográfico baseado em identidade pode se tornar inviável de ser utilizado em termos práticos, pois pode se tornar muito lento. Alguns pesquisadores como Galbraith, S. *et al.*[GAL 02],

Barreto, P. *et al.*[BAR 02] e Barreto, P., Lynn, B. e Scott, M. [BAR 03] já conseguiram uma implementação mais eficiente do emparelhamento de *Tate*, porém este ainda possui ordem de grandeza superior ao cálculo de exponenciação em um corpo finito.

6 Conclusão e expectativas

6.1 Assuntos estudados até o momento

Neste trabalho, apresentamos o conceito de sistemas criptográficos baseados em identidades, que permitem a qualquer par de usuários se comunicar de forma segura, sem que seja necessária a troca de chaves secretas, como ocorre na criptografia simétrica, e sem que seja preciso utilizar certificados digitais para autenticar chaves públicas, que é o caso da criptografia assimétrica tradicional.

O modelo, proposto por A. Shamir [SHA 84] em 1984, baseia-se no esquema de criptografia assimétrica tradicional, sendo que, em vez de termos um par de chaves representadas por uma seqüência de *bits*, sendo uma aleatória, e a outra calculada em função da primeira, como no caso do RSA, teremos como chave pública um identificador, ou seja, uma característica que identifique o usuário de forma única, de modo que ele não tenha como negar que esta informação diz respeito a ele. Como exemplos de identificador, poderíamos citar o número do CPF ou o endereço eletrônico (*e-mail*). A chave particular é então calculada por uma Autoridade de confiança e entregue ao usuário por um canal seguro.

A grande vantagem deste esquema é que, ao contrário da criptografia assimétrica tradicional, não há necessidade de se fazer um mapeamento entre uma chave pública e seu dono, haja vista que, nesse caso, a chave pública identifica o dono. Uma outra vantagem é que, por não ser mais um número aleatório, um usuário Beto não precisa reservar espaço adicional para guardar as chaves públicas das pessoas com quem deseja se comunicar, pois pode usar sua própria lista de endereços eletrônicos. Estas características fazem com que a criptografia assimétrica baseada em identidades se assemelhe ao correio físico, ou seja, se você conhece o endereço de uma pessoa, você pode enviar-lhe uma mensagem, de modo que somente ela poderá ler. Com base no mesmo conceito, se Alice deseja enviar uma mensagem sigilosa para Beto, ela necessita apenas do endereço eletrônico de Beto, ou seja, não é preciso nem mesmo ter algum conhecimento sobre chaves ou protocolos de comunicação.

Vimos também que foram propostos diversos esquemas de criptografia e assinatura que utilizavam este conceito, mas que somente em 2001, com o esquema de Boneh & Franklin [BON 01], foi encontrada uma solução satisfatória, baseado em propriedades de curvas elípticas.

Estes sistemas são ideais para grupos fechados, como por exemplo em uma cadeia de lojas ou de bancos, onde a matriz pode fazer o papel de uma Autoridade de confiança.

A grande motivação para estudarmos os sistemas criptográficos baseados

em identidade surgiu do levantamento dos principais problemas encontrados na infra-estrutura de chaves públicas (PKI) e suas possíveis vulnerabilidades. Somado a este fato, ao fazermos o levantamento bibliográfico, descobrimos que até o momento em que este trabalho foi escrito, só temos conhecimento de literatura sobre o assunto em língua estrangeira.

6.2 Assuntos em estudo

Estamos atualmente estudando o artigo *Signcryption scheme for Identity-based Cryptosystems* [NAL 02]. Este esquema de assinatura & criptografia em um único passo, baseado em identidade, foi proposto em 2002 por Malone-Lee [ML 02] e uma outra versão, mais eficiente, foi proposta por Nalla & Reddy [NAL 02] em 2003. Tem como principal característica garantir uma comunicação autenticada e sigilosa tanto na origem quanto no destino da comunicação, característica esta que um esquema de criptografia baseado em identidade por si só não consegue prover, a menos que opere em conjunto com um esquema de assinatura baseado em identidade, sendo neste caso, conhecido como "assinar-e-depois-criptografar". Esta solução, porém, é menos eficiente do que a proposta por Nalla & Reddy.

Estudaremos o esquema de assinatura & criptografia em um único passo detalhadamente, procurando fazer uma comparação em termos de consumo de tempo computacional entre os esquemas de Nalla & Reddy, Malone-Lee e o esquema tradicional "assinar-e-depois-criptografar". Pretendemos fazer também uma análise de segurança de um dos esquemas, visando a implementação de algum protótipo.

A primeira versão do artigo de Nalla & Reddy foi publicada no início de março de 2003 e uma nova versão, corrigida, foi publicada em 28 de março do mesmo ano. Nesta segunda versão também havia algumas incorreções, o que motivou o envio de um *e-mail* do autor deste trabalho a Divya Nalla, um dos autores do citado artigo, apontando as incorreções e sugerindo as alterações necessárias. O autor respondeu o *e-mail* concordando com as alterações sugeridas e republicou o artigo com as mesmas em 09 de abril de 2003.

6.3 Assuntos a serem estudados

Após termos completado o levantamento bibliográfico necessário para a nossa pesquisa, decidimos estudar os seguintes assuntos, que farão parte da fase final de nosso trabalho, juntamente com o esquema de assinatura & criptografia em um único passo, comentado acima. Ao lado do assunto a ser estudado, seguem as referências que serão utilizadas:

- **Aplicações de sistemas baseados em identidades** [CHE 02]
  Estudaremos as principais aplicações envolvendo sistemas criptográficos baseados em identidades. A maioria das aplicações que veremos também são possíveis em sistemas criptográficos que seguem o padrão PKI (e que,

neste trabalho, batizamos de criptografia assimétrica tradicional), mas nosso objetivo será mostrar que tais aplicações são perfeitamente viáveis de serem realizadas com sistemas baseados em identidades. As principais aplicações que veremos são:

- REVOGAÇÃO DE CHAVES PÚBLICAS - onde o prazo de validade de uma chave pública é acrescentado ao identificador, garantindo a validade daquela chave apenas durante o período desejado;

- DELEGAÇÃO PARA UM NOTEBOOK - onde um usuário pode gravar em seu *notebook* as chaves particulares baseadas em identidade correspondentes apenas aos dias de uma viagem, a fim de não haver risco de comprometimento de sua chave particular padrão;

- DELEGAÇÃO DE SERVIÇOS - em que cada Departamento de uma empresa possa decriptografar as mensagens de sua responsabilidade, sem contudo, conseguir decriptografar as mensagens dos outros Departamentos, sendo que o Presidente da empresa consegue decriptografar todas as mensagens;

- CRIAÇÃO DE GRUPOS - onde você pode enviar uma mensagem para um determinado grupo sem que saiba quem são os componentes deste grupo;

- ADIÇÃO DE ASSINATURAS - onde um grupo de pessoas pode assinar um mesmo documento, como por exemplo, um Tratado Internacional.

- **Variações em esquemas de assinaturas** [ZHA 02, CHE 03]
  Veremos esquemas de assinatura diferentes do que vimos na seção 4. Estes esquemas, embora sejam menos eficientes em termos computacionais do que o visto anteriormente, são utilizados para fins específicos, não atendidos pelo esquema de Hess [HES 02]. Os esquemas que serão estudados são:

  - ASSINATURA COM PKG NÃO-CONFIÁVEL - onde um usuário pode provar que sua assinatura foi forjada pelo PKG, considerando que este PKG não seja uma entidade totalmente idônea;

  - ASSINATURAS CEGAS - que preservam o anonimato do assinante, o que pode ser importante, como por exemplo, em votações eletrônicas;

  - ASSINATURA EM ANEL - em que você pode ter certeza de que determinada mensagem foi assinada por um grupo, mas não tem como saber quem do grupo assinou.

- **Hierarquia de sistemas baseados em identidades** [CHE 02, HOR 02]
  Exibiremos a hierarquia e certificação de sistemas baseados em identidades, apresentando um modelo híbrido de certificação PKI-IBE. Descreveremos como assinaturas curtas podem ser utilizadas para certificar autoridades de confiança e também como conseguir uma hierarquia de autoridades de confiança relacionadas com chaves baseadas em identidades.

Veremos também como transferir confiança e delegar direitos dentro da hierarquia baseada em identidades.

- **Implementação de um protótipo** [GAL 01, GAL 02, BAR 02, BAR 03] Para que uma implementação se torne viável, teremos que estudar detalhadamente a implementação das operações em curvas elípticas, utilizadas em sistemas criptográficos baseados em identidade, como soma de pontos em uma curva, multiplicação de um ponto da curva por um inteiro, cálculo do emparelhamento de *Tate* entre dois pontos de uma curva, potência de um emparelhamento de *Tate*, cálculo da funções de espalhamento (*hash*) H_1, H_2 e H_3.
  Obtendo sucesso na implementação dos itens descritos acima, sobretudo no cálculo do emparelhamento de *Tate* entre dois pontos, que é a operação mais complexa, teremos condições de implementar um esquema de assinatura & criptografia em um único passo, utilizando a linguagem de programação ANSI-C.

6.4 Cronograma-tentativa

Na tabela 1 apresentamos o cronograma que tentaremos seguir na fase final de nossa pesquisa.

Tabela 1: Cronograma-tentativa para a fase final

Assunto a ser estudado	ago 03	set 03	out 03	nov 03	dez 03
Assinatura & criptografia em um único passo	■				
Aplicações de sistemas baseados em identidades	■				
Variações em esquemas de assinaturas	■				
Hierarquia de sistemas baseados em identidades		■			
Implementação de um protótipo		■	■	■	
Redação do texto final			■	■	
Defesa da Dissertação					■

Referências

[BAR 99] BARRETO, P. **Curvas Elípticas e Criptografia: Conceitos e Algoritmos**. Disponível em <http://planeta.terra.com.br/informatica/paulobarreto>. Acesso em: 25 mar. 2003.

[BAR 02] BARRETO, P.; KIM, H.; LYNN, B. **Efficient Algorithms for Pairing-Based Cryptosystems**. In: Lecture Notes in Computer Science, v.2442, p.354–368. Springer-Verlag, 2002. Advances in Cryptology - Crypto'2002.

[BAR 03] BARRETO, P.; LYNN, B.; SCOTT, M. **On the selection of Pairing-Friendly Groups**. Disponível em <http://eprint.iacr.org/2003/086>. Acesso em: 04 mai. 2003.

[BON 01] BONEH, D.; FRANKLIN, M. **Identity Based Encryption from the Weil Pairing**. In: Lecture Notes in Computer Science, v.2139, p.213–229. Springer-Verlag, 2001. Advances in Cryptology - CRYPTO'2001.

[CHA 02] CHA, J. C.; CHEON, J. H. **An Identity-based Signature from gap Diffie-Hellman groups**. In: Lecture Notes in Computer Science, v.2567, p.18–30. Springer-Verlag, 2002.

[CHE 02] CHEN, L. et al. **Certification of Public Keys within an Identity-Based System**. In: Lecture Notes in Computer Science, v.2433, p.322–333. Springer-Verlag, 2002. 5th International Security Conference - ISC 2002.

[CHE 03] CHEN, X.; ZHANG, F.; KIM, K. **A New ID-based Group Signature Scheme from Bilinear Pairings**. Disponível em <http://eprint.iacr.org/2003/116>. Acesso em: 06 jun. 2003. Cryptology ePrint Archive, Report 2003/116.

[GAL 01] GALBRAITH, S. **Supersingular Curves in Cryptography**. In: Lecture Notes in Computer Science, v.2248, p.495–513. Springer-Verlag, 2001. ASIACRYPT 2001.

[GAL 02] GALBRAITH, S.; HASRRISON, K.; SOLDERA, D. **Implementing the Tate Pairing**. In: Lecture Notes in Computer Science, v.2369, p.324–337. Springer-Verlag, 2002. ANTS 2002.

[HES 02] HESS, F. **Efficient Identity Based Signature Schemes Based on Pairings**. In: Lecture Notes in Computer Science, v.2595, p.310–324. Springer-Verlag, 2002.

[HOR 02] HOROWITZ, J.; LYNN, B. **Hierarchical Identity-Based Encryption**. In: Lecture Notes in Computer Science, v.2332, p.466–481. Springer-Verlag, 2002. Advances in Cryptology - EUROCRYPT'2002.

[ML 02] MALONE-LEE, J. Signcryption with non-repudiation. Department of Computer Science, University of Bristol, jun., 2002. Relatório TécnicoCSTR 02-004.

[NAL 03] NALLA, D.; REDDY, K. **Signcryption scheme for Identity-based Cryptosystems**. Disponível em <http://eprint.iacr.org/2003/066/>. Acesso em: 22 abr. 2003.

[PAT 02] PATERSON, K. Id-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, jan., 2002. Relatório Técnico2002/004.

[RIV 78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public key cryptosystems. **Communications of the ACM**, [S.l.], v.1, n.2, p.120–126, fev, 1978.

[SHA 84] SHAMIR, A. **Identity Based Cryptosystems and Signature Schemes**. In: Lecture Notes in Computer Science, v.196, p.47–53. Springer-Verlag, 1984. Advances in Cryptology: Proceedings of CRYPTO 84.

[SIL 86] SILVERMAN, J. **The Arithmetic of Elliptic Curves**. In: GRADUATE TEXTS IN MATHMATICS N. 106. Springer Verlag, New York, 1. ed., 1986.

[TER 00] TERADA, R. **Segurança de Dados- Criptografia em Redes de Computador**. 1. ed. São Paulo: Edgard Blücher, 2000.

[ZHA 02] ZHANG, F.; KIM, K. **ID-based Blind Signature and Ring Signature from Pairings**. Disponível em <http://caislab.icu.ac.kr/paper/2002/zhang/paper177.pdf>. Acesso em: 12 mai. 2003.