UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO
CENTRO DE INFORMÁTICA

2009.1

ENCRIPTAÇÃO ESPAÇO-EFICIENTE BASEADA EM IDENTIDADE

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno Patrícia Lustosa Ventura Ribeiro (plvr@cin.ufpe.br)
Orientador Ruy J. Guerra B. de Queiroz (ruy@cin.ufpe.br)

03 de Março de 2009

Índice

1. Contexto

Em 1984, Shamir [1] propôs um esquema de encriptação de chave pública tal que a chave pública pode ser uma string arbitrária. Esse tipo de esquema é chamado *Identity-Based Enscryption* (IBE). A motivação original de Shamir para IBE era simplificar o gerenciamento de certificados em sistemas de email. Quando Alice manda um email para Bob no endereço bob@company.com, ela simplesmente encripta a sua mensagem usando a string "bob@company.com" como chave pública. Não há necessidade de Alice obter um certificado para a chave pública de Bob. Quando Bob recebe o email encriptado, ele entra em contato com uma terceira entidade, que é chamada de *Private Key Generator* (PKG). Bob se autentica no PKG da mesma maneira que ele se autenticaria para o *Certification Authority* (CA) e obtém sua chave privada do PKG. Bob pode então ler seu email. Note que, ao contrário da infra-estrutura de email existente, Alice pode mandar email encriptado para Bob mesmo se Bob ainda não criou seu certificado de chave pública.

Em um esquema IBE, existem quatro algoritmos que são usados para criar e usar o par de chaves pública-privada. Eles são tradicionalmente chamados de configuração, extração, encriptação e decriptação. Configuração é o algoritmo que inicializa os parâmetros necessários para os cálculos do IBE. Extração é o algoritmo para calcular uma chave privada IBE a partir da identidade do usuário e dos parâmetros estabelecidos na etapa de configuração. Encriptação é o algoritmo que gera o cifro-texto usando uma chave pública IBE, que é calculada a partir dos parâmetros da configuração e da identidade do usuário. Decriptação é o algoritmo que recupera o puro-texto usando a chave privada IBE do usuário e o cifro-texto.

Desde que o problema foi lançado, houve várias propostas de esquemas IBE. Contudo, nenhuma dessas propostas era totalmente satisfatória. Algumas soluções requeriam que os usuários não colidissem. Outras soluções requeriam que o PKG gastasse muito tempo para cada requisição de chave privada. Algumas soluções requeriam um hardware resistente a falsificações. Até 2001, construir um sistema IBE usável era um problema em aberto.

Em 2001, Dan Boneh e Matt Franklin [2] propuseram o primeiro esquema IBE totalmente funcional. Ele é baseado em curvas elípticas, em particular, nos chamados pareamentos de Weil. A performance desse sistema é similar a performance da encriptação ElGamal. A segurança do sistema é baseada na analogia natural da hipótese computacional de Diffie-Hellman em curvas elípticas.

Existem duas abordagens para a construção de sistemas IBE. A primeira delas, na qual o esquema Boneh-Franklin é baseada, constrói sistemas IBE usando pareamentos bilineares [2, 3, 4, 5]. Os sistemas resultantes são eficientes tanto em performance quanto em tamanho do cifro-texto. A rica estrutura de mapas bilineares possibilita o desenvolvimento de várias extensões, como IBE hierárquico [6], IBE anônimo [7] e muitos outros.

A segunda abordagem, utilizada por Cocks [8], constrói um sistema IBE elegante baseado no problema padrão da residuosidade quadrática [9, p.99] módulo um RSA composto N. Os cifro-textos nesse sistema contém dois elementos de Z/NZ para cada bit do puro-texto. Assim, a encriptação de uma mensagem de ℓ bits possui tamanho $2\ell \cdot \log 2\ N$. Por exemplo, encriptando uma mensagem de 128 bits usando um módulo de 1024 bits, o cifro-texto gerado possui 32678 bytes de tamanho. Em comparação, métodos baseados em pareamentos produzem um cifro-texto de 36 bytes para o mesmo nível de segurança.

Um problema em aberto desde o sistema de Cocks era a construção de um sistema IBE eficiente em espaço sem recorrer a pareamentos, ou seja, um sistema com cifro-texto curto. Em 2007, Boneh, Gentry e Hamburg [10] construíram um sistema com essas condições – a encriptação de uma mensagem de ℓ bits consiste em um único elemento em Z/NZ mais (ℓ +1) bits adicionais. Assim, o cifro-texto possui tamanho $\ell + \log 2\ N$. Encriptando uma mensagem de 128 bits, o resultado é um cifro-exto de tamanho 1024 + 129 = 1153 bits ou 145 bytes. O sistema faz uso extensivo da teoria das formas quadráticas [11]. Em particular, encriptação e decriptação são baseadas em uma versão do teorema dos três quadrados de Legendre.

O tempo de encriptação nesse sistema não é ideal. O tempo de encriptação na maior parte dos sistemas práticos de chave pública e nos sistemas IBE existentes [2, 8] é cúbico no parâmetro de segurança. O tempo de encriptação nesse sistema de Boneh é quadrático no parâmetro de segurança por bit da mensagem. O tempo de decriptação, contudo, é cúbico como nos outros sistemas. O gargalo durante a encriptação se deve a necessidade de gerar primos da ordem de N.

2. Objetivos

Este trabalho de graduação tem como objetivo entender o funcionamento do esquema de Boneh, Gentry e Hamburg. Para isso, faz-se necessário o entendimento do conceito de Identity-Based Encryption (IBE) e das soluções anteriores ao esquema em questão. Na área matemática, serão estudados a teoria das formas quadráticas e o problema da residuosidade quadrática. Em seguida, será realizado um estudo teórico de cada um dos quatro algoritmos da proposta de Boneh et al. Por fim, espera-se investigar os requisitos e as devidas conseqüências do esquema mencionado no desenvolvimento de IBEs aplicáveis ao mundo real.

3. Cronograma

O cronograma abaixo demonstra algumas datas para as atividades principais do processo de desenvolvimento do trabalho de graduação. Os prazos podem ser alterados conforme o estudo e aprofundamento do trabalho ou o acontecimento de imprevistos.

	Fevereiro				Março				Abril					Maio				Junho			
Levantamento do material bibliográfico				■	■																
Estudo sobre IBE						■	■														
Estudo sobre formas quadráticas								■	■	■											
Estudo sobre os algoritmos do esquema de Boneh-Gentry-Hamburg										■	■	■	■								
Estudo sobre conseqüências e requisitos do esquema de Boneh-Gentry-Hamburg												■	■	■							
Elaboração do Relatório												■	■	■	■	■	■				
Elaboração da Apresentação																	■	■	■		

4. Referências

[1] A Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology. Crypto 84, LNCS 196, Springer, 47-53, 1984.

[2] D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing", Advances in Cryptology. Crypto 2001, LNCS 2139, Springer, 213-229, 2001. (Versão estendida em SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.)

[3] Dan Boneh and Xavier Boyen. Efficient selective-ID identity based encryption without random oracles. In Proceedings of Eurocrypt 2004, LNCS, pages 223–238. Springer-Verlag, 2004.

[4] R. Sakai and M. Kasahara. ID based cryptosystems with pairing over elliptic curve. http://eprint.iacr.org/2003/054, 2003.

[5] B. Waters. Efficient identity-based encryption without random oracles. In Proceedings of Eurocrypt 2005, LNCS, 2005.

[6] Jeremy Horwitz and Ben Lynn. Towards hierarchical identity-based encryption. In Lars Knudsen, editor, Proceedings of Eurocrypt 2002, volume 2332 of LNCS, pages 466–81. Springer,2002.

[7] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In CRYPTO, pages 205–222, 2005.

[8] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Proceedings of the 8th IMA International Conference on Cryptography and Coding, pages 26–8, 2001.

[9] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[10] D. Boneh, C. Gentry, and M. Hamburg. Space-Efficient Identity Based Encryption Without Pairings. In proceedings of FOCS 2007, pp. 647-657, 2007

[11] J. W. S. Cassels. Rational quadratic forms, volume 13 of London Mathematical Society Monographs. Academic Press, 1978.

5. Possíveis Avaliadores

Anjolina Grisi de Oliveira

6. Assinaturas

Ruy J. Guerra B. de Queiroz
Orientador

Patrícia Lustosa Ventura Ribeiro
Aluno