Projeto de Pesquisa

Título: **Criptografia de Chave Pública sem Certificado**

Proponentes:

Denise Hideko Goya

Routo Terada (orientador)

Instituição:

Departamento de Ciência da Computação

Instituto de Matemática e Estatística

Universidade de São Paulo

São Paulo, julho de 2008

1 Resumo

O modelo de criptografia de chave pública sem certificado é uma alternativa ao modelo convencional que requer a manutenção de uma infra-estrutura de chaves públicas. Também é uma opção para a eliminação da custódia de chaves do modelo de criptografia assimétrica baseada em identidades.

Vários pesquisadores têm demonstrado interesse em estudar esse modelo. Citamos aqui alguns pontos que podem ser melhorados e que desejamos desenvolver: modelos de segurança para protocolos de assinatura, cifragem e cifrassinatura, além de propostas de protocolos sob modelos robustos de segurança, com eficiência computacional viável.

2 Introdução

O modelo convencional de criptografia de chave pública requer uma infra-estrutura de chaves públicas (ICP), para certificar a legitimidade dessas chaves. A manutenção de uma ICP, entretanto, implica custos e confere maior complexidade aos sistemas. O modelo de criptografia de chave pública baseada em identidade, proposto em [Shamir 1984], dispensa a necessidade da ICP, uma vez que a chave pública de um usuário é sua própria identificação (ou seja, dados pessoais, como nome, número do CPF ou telefone celular, etc). Em [Boneh, Franklin 2001] foi apresentado o primeiro esquema eficiente de cifragem baseado em identidade, que foi demonstrado seguro no modelo de oráculos aleatórios.

Uma característica inerente ao modelo de criptografia de chave pública baseada em identidade é a de custódia de chaves, em que uma entidade conhece as chaves secretas de todos seus usuários. A custódia de chaves é indesejável em vários tipos de aplicações; em particular, impossibilita a garantia de irretratabilidade.

Em [Al-Riyami, Paterson 2003], foi introduzido o paradigma de criptografia de chave pública sem certificado, que une propriedades do modelo convencional com o baseado em identidade. Nesse paradigma, ICP e certificados digitais se fazem desnecessários, pois a identidade de um usuário fica parcialmente relacionada com a chave secreta. E não há custódia de chaves, pois o usuário é o único conhecedor de sua chave criptográfica secreta. Ademais, para uso interno a uma dada instituição (por exemplo, uma empresa ou órgão do governo) este paradigma é apropriado, uma vez que a entidade geradora das chaves (chamada *Key Generating Centre*, KGC) pode ser um membro idôneo desta instituição.

A similaridade entre os protocolos de [Al-Riyami, Paterson 2003] e [Boneh, Franklin 2001] indica que aplicações desenvolvidas sobre identidades podem ser convertidas para o modelo sem certificado, ao custo da necessidade de divulgação das chaves públicas (ou da manutenção de um diretório de chaves). O modelo sem certificado poderia ser uma ponte entre sistemas baseados em identidade com os que requerem ICP, em particular, a ICP-Brasil.

3 Tópicos em Desenvolvimento

A proposta de [Al-Riyami, Paterson 2003] tem sido amplamente estudada e estendida nos últimos anos, na busca de melhores resultados nos quesitos segurança, eficiência computacional e derivação de protocolos, descritos a seguir.

3.1 Aspectos de Segurança

Classificaremos os aspectos de segurança em dois grandes grupos, relacionados entre si: criptanálise e análise formal de segurança.

A respeito do primeiro, criptanálise, podemos citar alguns tipos de ataque relatados. O modelo sem certificado requer uma entidade conhecida por KGC, que é responsável por gerar os parâmetros

gerais do sistema e as chaves secretas parciais para os usuários, após validar suas identidades. Um KGC desonesto pode gerar os parâmetros e as chaves parciais sem respeitar os protocolos, de modo que as chaves secretas dos usuários possam ser corrompidas e sem que os usuários tomem ciência (ver [Au et al. 2007]). Muitos dos esquemas já desenvolvidos são sujeitos a esse tipo de ataque; dentre as exceções podemos citar [Hwang et al. 2008] e [Zhang, Wang 2008].

O ataque de substituição de chave pública talvez seja o que compromete maior número de protocolos já propostos. Como exemplo, citamos [Terada, Goya 2007], cujo esquema foi estudado em [Castro, Dahab 2007]. Em muitos casos, protocolos sujeitos a esse ataque foram inicialmente demonstrados seguros usando determinadas hipóteses (que foram posteriormente exploradas culminando em quebra). Esse tipo de ataque está intimamente relacionado com o aspecto análise formal de segurança, adiante.

O ataque DoD (*Denial-of-Decryption*) também substitui chaves públicas, porém de modo a simplesmente impedir que um usuário decifre uma mensagem ou verifique uma assinatura, caso uma chave pública ilegítima tenha sido mal-intencionadamente divulgada. Em [Liu et al. 2007], por exemplo, há tratamento deste caso.

Em análise formal de segurança, há várias questões a serem consideradas durante o projeto de protocolos e algoritmos, como modelo de segurança para esquemas sem certificado, modelo de demonstração (padrão ou por oráculos aleatórios) e problemas envolvidos nas reduções.

Especialmente dentre os protocolos com maior eficiência computacional, é comum encontrarmos demonstrações sustentadas em hipóteses bastante fortes (talvez questionáveis), como a dificuldade de problemas matemáticos pouco conhecidos (por exemplo, p-*BDHI* em [Libert, Quisquater 2006] ou q-*BSDH* em [Zhang, Wang 2008]). Reduções polinomiais pouco eficientes, com folgas relativamente grandes (como em [Barbosa, Farshim 2008]) devem ser evitadas.

O controverso modelo de oráculos aleatórios para segurança demonstrável tem sido dominante entre as propostas de esquemas sem certificados, sob a justificativa de que os protocolos são mais viáveis para implementações práticas. Mas há estudos como o de [Dent et al. 2008] que usam o modelo padrão e forte modelo de adversários, ao custo de menor desempenho computacional.

Em [Dent 2006], há um levantamento dos modelos de segurança dos esquemas de cifragem desenvolvidos até então. Desconhecemos trabalho equivalente para esquemas de assinatura e seria importante uma discussão detalhada em torno do assunto, para que possamos melhor avaliar cada protocolo.

3.2 Eficiência Computacional

Foi sugerido em parágrafos anteriores que esquemas mais rápidos costumam apresentar inferioridade em algum aspecto de segurança. É desejável o bom equilíbrio entre eficiência computacional e eficiência teórica da segurança.

Embora a grande maioria dos trabalhos para o modelo sem certificado considere emparelhamentos bilineares sobre curvas elípticas, em [Sun et al. 2007] há um exemplo de que é possível um caminho mais convencional (exponenciações em $\mathbb{Z}_p$). Certamente o grupo algébrico e suas operações influenciam fortemente na velocidade dos algoritmos.

3.3 Derivação de Protocolos

Protocolos de cifragem e de assinatura são os mais elementares em criptografia de chave pública. A partir deles, outros esquemas podem ser derivados, como o de cifrassinatura, que tem por objetivo a gararantia simultânea de confidencialidade e autenticidade. Existem modelos robustos de segurança para cifrassinatura, como os de [An et al. 2002] e [Baek et al. 2002], que podem ser adaptados para o modelo sem certificado (ver [Barreto et al. 2008] e [Barbosa, Farshim 2008]).

Cifra autenticada também une confidencialidade e autenticidade, porém com características de segurança menos fortes que as da cifrassinatura. Outros protocolos variantes dos básicos, como com múltiplos usuários ou hierárquicos, não serão foco de nossos estudos.

4 Objetivos

O objetivo primário de nosso trabalho é o desenvolvimento de protocolos de cifragem e de assinatura, no modelo de criptografia de chave pública sem certificado. Os protocolos devem ser demonstrados seguros em fortes modelos de segurança e devem despertar interesse prático, isto é, eficiência computacional é um dos critérios a serem ponderados. As construções poderão ser genéricas, criadas a partir de subprotocolos considerados seguros, ou concretas, para implementação direta. Objetivam-se, ainda, aprimoramentos em cifrassinatura sem certificado, projetados a partir de protocolos de cifragem e de assinatura.

Eventualmente, outros resultados podem ser alcançados, como conseqüência dos esforços sobre os alvos anteriores. A saber:

- Melhoria em demonstrações de segurança de protocolos existentes (reduções mais eficientes ou para problemas melhor estudados);
- Descoberta de falhas em demonstrações de segurança sobre protocolos existentes;
- Quebra de protocolos existentes;
- Modelos de segurança alternativos;
- Nova forma de ataque ao modelo sem certificado;

Basicamente, os objetivos descritos refletem o interesse em dar continuidade ao trabalho apresentado na dissertação de mestrado, em [Goya 2006].

5 Plano de Trabalho

Nosso plano de trabalho consiste na realização das principais tarefas a seguir:

1. Levantamento dos modelos de segurança para assinatura usados em trabalhos existentes;
2. Levantamento dos modelos de segurança para cifragem usados em trabalhos existentes;
3. Levantamento dos modelos de segurança para cifrassinatura usados em trabalhos existentes;
4. Estudos para elaboração de proposta de assinatura;
5. Proposta de esquema de assinatura sem certificado;
6. Atualizações dos modelos de segurança;
7. Estudos para elaboração de proposta de cifragem;
8. Proposta de esquema de cifragem sem certificado;
9. Estudos para elaboração de proposta de cifrassinatura;
10. Proposta de esquema de cifrassinatura sem certificado;
11. Revisão e melhoria das propostas;
12. Texto final da tese e defesa;

Nos itens 1, 2 e 3, serão avaliados os modelos de adversários e interações com oráculos, usados em propostas no modelo sem certificado. O objetivo é mapear pontos fortes e fracos de cada alternativa. Nesse momento, também serão estudadas as técnicas de provas de segurança aplicadas em cada trabalho. No item 2, basicamente será completada uma atualização sobre a pesquisa de [Dent 2006].

As tarefas 4, 7 e 9 refletem as tentativas de elaboração de protocolos e respectivas demonstrações de segurança. Já as tarefas 5, 8 e 10 referem-se à redação dos resultados obtidos a partir dos estudos anteriores.

Atualizações dos modelos de segurança e revisão das propostas serão realizadas sempre que necessário ou conveniente, até a redação final da tese.

Uma proposta de cronograma para execução desse plano de trabalho é apresentada na tabela 1, em que cada coluna refere-se a um semestre. Os momentos para apresentação das propostas de esquemas de assinatura, cifragem e cifrassinatura são meramente metas temporais.

Tarefas		2008	2009		2010		2011	
		2º	1º	2º	1º	2º	1º	2º
1	Modelos de segurança para assinatura	x						
2	Modelos de segurança para cifragem		x					
3	Modelos de segurança para cifrassinatura		x					
4	Estudos para proposta de assinatura	x	x	x				
5	Proposta de assinatura sem certificado			x				
6	Atualizações dos modelos de segurança			x	x	x	x	
7	Estudos para proposta de cifragem		x	x	x			
8	Proposta de cifragem sem certificado				x			
9	Estudos para proposta de cifrassinatura			x	x	x		
10	Proposta de cifrassinatura sem certificado					x		
11	Revisão e melhoria das propostas				x	x	x	x
12	Texto final da Tese e defesa						x	x

Tabela 1: Cronograma

6 Análise dos Resultados

As três primeiras tarefas descritas na seção anterior, levantamento de modelos de segurança, serão inicialmente uma compilação dos resultados existentes. Acreditamos que essa compilação para assi-

natura e cifrassinatura é inédita. O resultado será tanto melhor se for possível sugerirmos melhorias sobre os modelos existentes.

Para avaliação das propostas de esquemas, os critérios a serem considerados são divididos em dois grupos, aspectos de segurança e eficiência computacional, conforme discussão na seção 3.

Aspectos de segurança. Bons protocolos contemplam:

- Robustez do modelo de segurança;
- Problemas usados nas reduções são conhecidos e estudados;
- Eficiência das reduções;
- Resistência a ataques conhecidos.
- Demonstrações de segurança bem fundamentadas;

Eficiência computacional. Análise grosseira, contando as quantidades de operações mais caras; são potencialmente mais eficientes os protocolos que minimizam tais operações:

- Número de emparelhamentos bilineares, se for o caso;
- Número de exponenciações;
- Outras operações, se for o caso;

Construções genéricas tendem a ser menos eficientes do ponto de vista computacional quando comparadas com construções concretas, porém são de grande interesse, pois mostram caminhos para combinação de outras soluções prontas.

7 Conclusão

Expusemos motivações para o estudo do modelo de criptografia de chave púbica sem certificado, bem como um plano de trabalho para a criação de protocolos sob fortes modelos de segurança.

Referências

[Al-Riyami, Paterson 2003] Al-Riyami, S. S., Paterson, K. G. (2003). Certificateless public key cryptography. In *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security*, volume 2894 of *Lecture Notes in Computer Science*, Taipei, Taiwan. Springer.

[An et al. 2002] An, J. H., Dodis, Y.,, Rabin, T. (2002). On the security of joint signature and encryption. In *EUROCRYPT*, volume 2332 of *Lecture Notes in Computer Science*, pages 83–107. Springer.

[Au et al. 2007] Au, M. H., Mu, Y., Chen, J., Wong, D. S., Liu, J. K.,, Yang, G. (2007). Malicious kgc attacks in certificateless cryptography. In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pages 302–311, New York, NY, USA. ACM.

[Baek et al. 2002] Baek, J., Steinfeld, R.,, Zheng, Y. (2002). Formal proofs for the security of signcryption. In *PKC 2002*, volume 2274 of *Lecture Notes in Computer Science*, pages 80–98. Springer.

[Barbosa, Farshim 2008] Barbosa, M., Farshim, P. (2008). Certificateless signcryption. In *ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pages 369–372, New York, NY, USA. ACM.

[Barreto et al. 2008] Barreto, P. S. L. M., Deusajute, A. M., de Souza Cruz, E., Pereira, G. C. F.,, da Silva, R. R. (2008). Toward efficient certificateless signcryption from (and without) bilinear pairings. Submetido para *"VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais"* (SBSeg 2008).

[Boneh, Franklin 2001] Boneh, D., Franklin, M. K. (2001). Identity-based encryption from the weil pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229, London, UK. Springer-Verlag.

[Castro, Dahab 2007] Castro, R., Dahab, R. (2007). Two notes on the security of certificateless signatures. In *Provable Security*, volume 4784 of *Lecture Notes in Computer Science*, pages 85–102, Berlin/Heidelberg. Springer.

[Dent 2006] Dent, A. W. (2006). A survey of certificateless encryption schemes and security models. Cryptology ePrint Archive, Report 2006/211. http://eprint.iacr.org/.

[Dent et al. 2008] Dent, A. W., Libert, B.,, Paterson, K. G. (2008). Certificateless encryption schemes strongly secure in the standard model. In *Public Key Cryptography - PKC 2008*, volume 4939 of *Lecture Notes in Computer Science*, pages 344–359, Berlin/Heidelberg. Springer.

[Goya 2006] Goya, D. H. (2006). Proposta de esquemas de criptografia e de assinatura sob modelo de criptografia de chave pública sem certificado. Mestrado, Instituto de Matemática e Estatística, Universidade de São Paulo. 1º Lugar na categoria Mestrado do concurso de Teses, Dissertações e TCCs, no SSI 2006, Instituto Tecnológico de Aeronáutica - ITA. Disponível em http://www.teses.usp.br/teses/disponiveis/45/45134/tde-28072006-142410/.

[Hwang et al. 2008] Hwang, Y. H., Liu, J. K.,, Chow, S. S. (2008). Certificateless public key encryption secure against malicious kgc attacks in the standard model. *Journal of Universal Computer Science*, 14(3):463–480.

[Libert, Quisquater 2006] Libert, B., Quisquater, J.-J. (2006). On constructing certificateless cryptosystems from identity based encryption. In *Public Key Cryptography 2006 (PKC'06)*, volume 3958 of *Lecture Notes in Computer Science*, pages 474–490, New York, NY, USA. Springer-Verlag.

[Liu et al. 2007] Liu, J. K., Au, M. H.,, Susilo, W. (2007). Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pages 273–283, New York, NY, USA. ACM.

[Shamir 1984] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, volume 196/1985 of *Lecture Notes in Computer Science*, pages 47–53, New York, NY, USA. Springer-Verlag New York, Inc.

[Sun et al. 2007] Sun, Y., Zhang, F.,, Baek, J. (2007). Strongly secure certificateless public key encryption without pairing. In *CANS*, volume 4856 of *Lecture Notes in Computer Science*, pages 194–208. Springer.

[Terada, Goya 2007] Terada, R., Goya, D. H. (2007). A certificateless signature scheme based on bilinear pairing functions. In *Symposium on Computer and Information Security 2007*, volume 2C4-5 of *Information, and Communication Engineers*, pages 1–7, Tokyo, Japão. IEICE Institute of Electronics.

[Zhang, Wang 2008] Zhang, G., Wang, S. (2008). A certificateless signature and group signature schemes against malicious pkg. In *22nd International Conference on Advanced Information Networking and Applications, AINA 2008*, pages 334–341. IEEE Computer Society.