Relatório do Plano de Estudos

Modelos de Segurança em Assinatura sem Certificado

MAC5801 - Tópicos Especiais em Ciência da Computação

aluna: Denise Hideko Goya

orientador: Routo Terada

Instituição:

Departamento de Ciência da Computação

Instituto de Matemática e Estatística

Universidade de São Paulo

São Paulo, novembro 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.

Neste relatório listamos propriedades de alguns modelos de segurança para protocolos de assinatura sob o modelo sem certificado. Elegemos um que apresentou as melhores características até o momento e relacionamos possíveis extensões para ele. Ao final, colocamos alguns questionamentos que devem ser melhor estudados, pois podem levar a outros trabalhos.

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 (CL-PKC), 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.

Estudos em criptanálise revelaram vários tipos de ataque sobre o modelo. 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 2007b]. 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, que

foi o alvo principal do plano de estudos que gerou o presente relatório.

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.

4 Plano de Estudos Original

Nosso plano de estudos original envolvia a investigação dos modelos de segurança descritos nos vários esquemas de assinatura já propostos. Foram estudados prioritariamente os seguintes trabalhos:

- Certificateless signature: a new security model and an improved generic construction [Hu et al. 2007];

- A certificateless signature and group signature schemes against malicious PKG [Zhang, Wang 2008];
- Certificateless public key signature: security model and efficient construction [Zhang et al. 2006];
- Security analysis of two signature schemes and their improved schemes [Zhang, Mao 2007];
- Two notes on the security of certificateless signatures [Castro, Dahab 2007b];
- Generic transformation from weakly to strongly unforgeable signatures [Huang et al. 2008];

Adicionalmente, pretendíamos olhar os modelos de segurança nas seguintes variantes sobre assinaturas:

- Security mediated certificateless signatures [Yap et al. 2007];
- Simulatability and security of certificateless threshold signatures [Wang et al. 2007];
- Efficient certificateless signatures suitable for aggregation [Castro, Dahab 2007a];
- A provably secure ring signature scheme in certificateless cryptography [Zhang et al. 2007];
- Certificateless universal designated verifier signature schemes [Ming et al. 2007];

5 Objetivos do Trabalho

O objetivo principal é a compilação dos modelos de segurança existentes para assinatura sem certificado, incluindo as técnicas de tratamento dos ataques conhecidos.

6 Resultados Alcançados e Organização do Trabalho

Conseguimos relacionar os principais trabalhos e descrever os resultados mais significativos da cada um, fornecendo um panorama geral em modelos de segurança para CLS.

Eventualmente poderíamos ter alcançado os itens abaixo, mas ainda não temos:

- 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;

Este relatório está organizado como segue: na Seção 7, são resumidos os pontos mais importantes dos modelos existentes, que justificam nossa escolha para o modelo básico, descrito na Seção 8. Na Seção 9, são relatadas as extensões que elevam o grau de seguraça do modelo básico, os ataques conhecidos e as técnicas básicas usadas para tratar cada ataque. Por fim, seguem as conclusões e propostas de trabalho futuro.

7 Breve Histórico de Modelos de Segurança para CLS

Em [Al-Riyami, Paterson 2003] foi apresentado o primeiro esquema de assinatura sob o modelo sem certificado. Naquela ocasião, os autores não apresentaram modelo de segurança e nem demonstração de que o esquema era seguro. Mas lá foram identificados dois tipos de adversários ao modelo sem certificado:

Tipo I. Um terceiro que pode substituir chaves públicas, porém não conhece a chave-mestra.

Tipo II. Simula um ataque por parte do KGC, que conhece a chave-mestra, mas não pode substituir chaves públicas.

Um modelo formal de segurança para CLS foi primeiramente descrito em [Yum, Lee 2004], amplamente baseado no modelo de segurança para o esquema de cifragem de [Al-Riyami, Paterson 2003]. Nesse trabalho foi apresentada uma construção genérica de esquema CLS a partir de uma assinatura no modelo baseado em identidade (IBS) combinada com assinatura no modelo convencional (PKS). Os autores afirmaram que com o CLS resultante é seguro se tanto o IBS quanto o PKS forem seguros. Posteriormente, como veremos adiante, foram apontadas falhas nessa construção, invalidando os resultados obtidos.

Em [Huang et al. 2005] foi demonstrado que o esquema de assinatura de [Al-Riyami, Paterson 2003] era falsificável, sujeito a ataque de substituição de chave pública. Os autores propuseram correções e usaram um modelo de segurança igual ao de [Yum, Lee 2004] para demonstrar a segurança dessa correção.

O modelo de segurança para CLS de [Yum, Lee 2004] e de [Huang et al. 2005] foi usado por [Zhang et al. 2006], na proposta de um novo esquema de assinatura. Porém, uma pequena (mas significativa) modificação no modelo de segurança foi adicionada: na substituição de uma chave pública, o adversário Tipo I não precisava fornecer o valor secreto correspondente. Como mostrado em [Castro, Dahab 2007b], muitos dos esquemas CLS que seguiram o modelo de segurança de [Yum, Lee 2004] (que exigia que o adversário Tipo I conhecesse o valor secreto correspondente à chave pública substituída) foram quebrados.

O trabalho de [Zhang et al. 2006] foi melhorado em [Hu et al. 2007]. Acreditamos que o modelo de segurança proposto nesse trabalho é o que reúne as melhores características. Na Seção 8,

detalharemos os pontos fortes desse modelo.

Em [Huang et al. 2007], os adversários Tipo I e II foram subdivididos em três subtipos cada um: **Normal** Type I/II, **Strong** Type I/II e **Super** Type I/II, em ordem do mais fraco para o mais forte. A definição desses subtipos aparentemente foi inspirada parcialmente em [Dent 2006]. Os adversários de [Hu et al. 2007] equivalem ao Super Type, de maior poder. Os adversários de, por exemplo, [Al-Riyami, Paterson 2003] e de [Yum, Lee 2004] (cujos esquemas propostos foram ambos quebrados) equivalem ao Normal Type.

[Huang et al. 2007] justificam a apresentação de três níveis para que seja possível a criação de esquemas de assinatura mais velozes, com segurança inferior (ou, alternativamente, menor velocidade com maior nível de segurança). Os próprios autores propuseram dois esquemas CLS, um cujo Tipo I era Normal e outro de Tipo Super. Embora ambos esquemas foram anunciados demonstravelmente seguro (as demonstrações foram prometidas para a versão completa do artigo), a proposta de CLS de Tipo I Normal foi quebrada por [Shim 2009].

De acordo com as afirmações de [Huang et al. 2007], um esquema que seja seguro no Strong Type, também o será em Normal Type; se o CLS for seguro em Super Type, então será nos tipos Normal e Strong. Embora essas afirmações possam parecer válidas à primeira vista, acreditamos que não estejam corretas. [Castro, Dahab 2007b] relacionam vários esquemas CLS de tipo Normal e a maioria já foi quebrada; aqueles que não foram talvez não sejam seguros. Desse modo, acreditamos que um esquema seguro no tipo Super não poderia ter condições relaxadas ao tipo Normal e continuar seguro. Não conseguimos avaliar, ainda, se um esquema seguro em Strong Type pode ser seguro na prática. De qualquer forma, achamos prudente considerar apenas o Super Type, que também é adotado no modelo de segurança da seção a seguir.

8 Modelo Básico para Assinatura sem Certificado

Sugerimos como modelo básico de segurança para CLS o definido em [Hu et al. 2007].

A definição de esquema de assinatura sem certificado de [Hu et al. 2007] tem as seguintes diferenças em relação às anteriores:

- Apenas **cinco algoritmos** capturam os mesmos comportamentos dos sete anteriores. Em particular, é mantida a característica de se gerar chaves públicas antes mesmo do KGC gerar a secreta parcial.
- O algoritmo de geração de **chave pública pode ser probabilístico** e vários valores de chave pública podem existir para um mesmo valor secreto.
- O algoritmo de geração de **chave parcial secreta pode ser probabilístico**. Na definição antiga, uma única chave parcial poderia ser gerada a partir do ID e da chave-mestra.

O modelo de segurança para CLS de [Hu et al. 2007] tem as seguintes alterações importantes sobre os modelos anteriores:

- Na consulta ao oráculo de substituição de chave pública, o adversário Tipo I pode fornecer, como valor secreto correspondente, uma **string vazia ou inválida** (isto é, a nova chave pública não tem associação com o valor secreto fornecido). Isso simula o caso em que o adversário não conhece a chave secreta, mas tenta mudar arbitrariamente o valor da chave pública.
- O adversário **Tipo II pode substituir chaves públicas** de identidades que não são alvo do ataque principal. Nos modelos anteriores, a substituição de chaves pelo adversário Tipo II não era permitida em momento algum.

- Para simplificar as demonstrações, é considerado apenas o caso em que o adversário Tipo I compromete o valor secreto ou substitui a chave pública. Nos modelos anteriores, paralelamente a essa condição, é tratada a restrição de que o adversário Tipo I não pode ter obtido a chave parcial secreta. Essa simplificação não enfraquece o modelo, uma vez que, se a chave parcial secreta for obtida, será simulado o adversário Tipo II.

9 Extensões do Modelo Básico para CLS

Nesta Seção, listamos as extensões que podem ser aplicadas ao modelo básico de segurança para CLS de [Hu et al. 2007].

9.1 Nível 3 de Confiança de Girault

A primeira extensão do modelo de segurança para CLS de [Hu et al. 2007] é proposta originalmente em [Yum, Lee 2004]: a construção genérica de CLS a partir de IBS e PKS seguros pode ser levada ao nível 3 de confiança, segundo [Girault 1991].

Girault define os seguintes três níveis de confiança, do mais fraco para o mais forte:

Nível 1. O KGC conhece a chave secreta de todos usuários.

Nível 2. O KGC não conhece chaves secretas, mas pode personificar usuários gerando falsas chaves públicas (ou certificados), contraditórias com as verdadeiras.

Nível 3. O KGC não conhece chaves secretas, pode personificar usuários gerando falsas chaves públicas, mas é detectado nessa ação, pois é o único que pode gerar chaves públicas válidas (ou certificados).

Sob o modelo baseado em identidade, o PKG atinge nível 1, pois conhece todas as chaves secretas. O KGC do modelo sem certificado alcança nível 2. No modelo convencional de criptografia de chave

pública com infra-estrutura de chaves públicas chega-se ao nível 3, pois a autoridade certificadora pode ser delatada se emitir dois certificados diferentes para a mesma identidade.

Em [Hu et al. 2007] é descrito um ataque de substituição de chave-e-mensagem em [Yum, Lee 2004]. Para corrigir a falha, [Hu et al. 2007] apresentam nova construção genérica de CLS a partir de IBS e PKS, usando o novo modelo de segurança. Os próprios autores propõem uma extensão para que o CLS chegue ao nível 3, com base na sugestão de [Yum, Lee 2004]. Para tanto, acrescenta-se a chave pública no cálculo da chave parcial privada. Adicionalmente, é proposto um jogo adicional para garantir que o KGC seja o **único** capaz de gerar chaves parciais.

9.2 Contra Ataque DoD – *Denial of Decryption*

O conceito de *Denial of Decryption* (DoD, em referência ao DoS, *Denial of Service*), foi introduzido por [Liu et al. 2007]. Trata-se de um ataque em que o adversário substitui chaves públicas e induz remetentes a cifrarem mensagens com falsas chaves públicas. Se o destinatário (dono da verdadeira chave pública) não conseguir decifrar ou obter uma mensagem diferente da original, o ataque é bem sucedido. No contexto de assinatura, usuários não conseguem validar assinaturas legítimas.

A solução proposta para se evitar o DoD envolve o cálculo da chave pública dependentemente da chave parcial secreta. Isso, entretanto, elimina uma das características peculiares do modelo sem certificado, que é a possibilidade de se gerar chaves públicas antes da interação com o KGC (tal propriedade viabiliza fluxos criptográficos, conforme descrito em [Al-Riyami, Paterson 2003]).

A proposta de [Liu et al. 2007] combina CLE (cifragem no modelo sem certificado) e CLS, criando **duas** chaves parciais secretas, uma para CLE e outra para CLS. Portanto, há também duas chaves secretas completas, uma para decifrar e outra para assinar. A chave pública passa a ser um par $< pk, \sigma >$ onde σ é a assinatura do usuário sobre sua própria chave pública pk. Um remetente verifica σ antes de cifrar com pk e, assim, DoD é evitado.

Os autores chamaram essa solução de *self-generated certificate PKC*; ela se assemelha a certificados auto-assinados em ICPs. Também apresentaram o modelo de segurança.

Um questionamento que fica em aberto é se não seria possível outro tipo de solução para CL-PKC, pois, na verdade, os autores inseriram uma espécie de certificado (a assinatura, que deve ser verificada e que só pode existir depois de uma interação com o KGC) em um modelo que deveria ser sem certificados.

9.3 Contra KCG Mal Intencionado

O adversário Tipo II, definido originalmente em [Al-Riyami, Paterson 2003], presume que o KGC é honesto e segue os protocolos conforme especificados. Em [Au et al. 2007], no entanto, é apresentada a possibilidade de que o KGC gere parâmetros desonestamente, de modo que ele consiga decifrar textos, sem o conhecimento dos usuários. À exceção de [Libert, Quisquater 2006, Hu et al. 2006], todos os esquemas propostos até o trabalho de [Au et al. 2007], são vulneráveis a esse KGC mal intencionado, e mesmo os trabalhos mais recentes também o são em grande parte. O artigo de [Hu et al. 2006] é uma prévia de [Hu et al. 2007], cujo modelo discutimos na Seção 8; ele já apresentava praticamente todos os elementos essenciais deste último.

Para que o esquema de [Hu et al. 2006] (e de [Hu et al. 2007]) seja demonstrado seguro contra o KGC mal intencionado, basta acrescentar ao modelo de segurança Tipo II a criação da chave-mestra pelo adversário (e não pelo desafiante). As demonstrações são apresentadas em [Au et al. 2007].

Vale citar o trabalho de [Zhang, Wang 2008] que, embora tenha usado adversários mais fracos que o de [Hu et al. 2007], apresentou CLS seguro contra KGC mal intencionado, não vulnerável a ataque DoD, que alcança nível 3 de Girault e todas as demonstrações são feitas sob o modelo padrão, sem oráculos aleatórios. Os autores se valem de uma técnica menos usual em CLS: é adotado um protocolo de conhecimento-zero na geração da chave parcial secreta, que (aparentemente) garante a

segurança contra KGC mal intencionado e leva ao nível 3 de Girault.

9.4 Assinaturas Fortemente Não-Falsificáveis

Todos os esquemas CLS propostos que foram demonstrados seguros seguem a noção de segurança EUF-CMA (*Existentially UnForgeable against Chosen-Message Attacks*), de [Goldwasser et al. 1988].

Em [Huang et al. 2008] é apresentada uma interessante transformação genérica de esquemas de assinatura EUF-CMA (e qualquer outro tipo não-falsificável) para sUF-CMA (*Strong UnForgeable against Chosen-Message Attacks*), que pode ser aplicada também a esquemas de assinatura sem certificado.

A noção sUF-CMA é mais forte que EUF-CMA, pois garante que não ocorrem falsificações de assinaturas sobre mensagens **que já tenham sido assinadas** anteriormente. A noção EUF-CMA trata de impedir apenas falsificações de assinaturas sobre **novas** mensagens que ainda não tenham sido assinadas.

10 Conclusões e Trabalhos Futuros

Apresentamos, neste trabalho, um levantamento de modelos de segurança relativos a esquema de assinatura no modelo de criptografia de chave púbica sem certificado. Fizemos comentários sobre o modelo que nos parece melhor elaborado e sobre como estendê-lo para tratar alguns tipos de ataque.

Listamos abaixo o que pretendemos (ou sugerimos) estudar melhor:

- Na apresentação de [Paterson 2007] são feitos questionamentos importantes a respeito de CLS. Para que aplicações, de fato, precisamos de esquema de assinatura sem certificado? Se para assinarmos no modelo sem certificado é necessária antes uma interação com o KGC (para se obter a chave parcial secreta), o CLS poderia ser substituído por um PKS (com o KGC emitindo

um certificado em vez de uma chave parcial). Talvez a vantagem de CLS seja que a chave parcial não depende do par <*chave pública, valor secreto*>, mas para que aplicações isso é importante?

- Explorar melhor a proposta de [Zhang, Wang 2008], que pode ter erros ou pode ser um caminho muito bom.

- Normal Type I é viável? Isto é, é possível que um CLS demonstrado seguro nesse tipo seja confiável?

- Strong Type é viável? Isto é, é possível criar um esquema CLS seguro em Strong Type I/II, que tenha melhor desempenho que um Super Type I/II (melhor velocidade ou menor tamanho de assinatura)?

- Verificar se o esquema de criptoassinatura de [Barbosa, Farshim 2008] é realmente sUF-CMA, como afirmam os autores. À primeira vista, pareceu EUF-CMA.

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.

[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.

[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.

[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 2007a] Castro, R., Dahab, R. (2007a). Efficient certificateless signatures suitable for aggregation. Cryptology ePrint Archive, Report 2007/454. http://eprint.iacr.org/.

[Castro, Dahab 2007b] Castro, R., Dahab, R. (2007b). 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. Também disponível em Cryptology ePrint Archive, Report 2007/121.

[Girault 1991] Girault, M. (1991). Self-certified public keys. In *EuroCrypt91*, pages 490–497, Brighton, UK. Springer. LCNS vol.547.

[Goldwasser et al. 1988] Goldwasser, S., Micali, S.,, Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17:281–308.

[Hu et al. 2007] Hu, B., Wong, D., Zhang, Z.,, Deng, X. (2007). Certificateless signature: a new security model and an improved generic construction. *Designs, Codes and Cryptography*, 42(2):109–126.

[Hu et al. 2006] Hu, B. C., Wong, D. S., Zhang, Z.,, Deng, X. (2006). Key replacement attack against a generic construction of certificateless signature. In *Information Security and Privacy, 11th Australasian Conference, ACISP 2006*, volume 4058 of *Lecture Notes in Computer Science*, pages 235–246. Springer.

[Huang et al. 2008] Huang, Q., Wong, D., Li, J.,, Zhao, Y.-M. (2008). Generic transformation from weakly to strongly unforgeable signatures. *Journal of Computer Science and Technology*, 23(2):240–252.

[Huang et al. 2007] Huang, X., Mu, Y., Susilo, W., Wong, D. S.,, Wu, W. (2007). Certificateless signature revisited. In *Information Security and Privacy, 12th Australasian Conference, ACISP 2007*, volume 4586 of *Lecture Notes in Computer Science*, pages 308–322. Springer.

[Huang et al. 2005] Huang, X., Susilo, W., Mu, Y.,, Zhang, F. (2005). On the security of certificateless signature schemes from asiacrypt 2003. In *Cryptology and Network Security, 4th International Conference, CANS 2005*, volume 3810 of *Lecture Notes in Computer Science*, pages 13–25, Xiamen, China. Springer.

[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.

[Ming et al. 2007] Ming, Y., qin Shen, X.,, Wang, Y.-M. (2007). Certificateless universal designated verifier signature schemes. *The Journal of China Universities of Posts and Telecommunications*, 14(3):85–94.

[Paterson 2007] Paterson, K. G. (2007). Certificateless cryptography. Invited talks at ICE-EM RNSA 2007 Workshop on Pairing Based Cryptography, Queensland University of Technology, June 2007. Disponível em http://www.isg.rhul.ac.uk/∼kp/certlessII.pdf. Acesso em novembro/08.

[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.

[Shim 2009] Shim, K.-A. (2009). Breaking the short certificateless signature scheme. *Information Sciences*, 179(3):303–306. Disponível em http://www.sciencedirect.com desde setembro de 2008.

[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.

[Wang et al. 2007] Wang, L., Cao, Z., Li, X.,, Qian, H. (2007). Simulatability and security of certificateless threshold signatures. *Information Sciences*, 177(6):1382–1394.

[Yap et al. 2007] Yap, W.-S., Chow, S., Heng, S.-H.,, Goi, B.-M. (2007). Security mediated certificateless signatures. In *Applied Cryptography and Network Security - ACNS 2007*, volume 4521 of *Lecture Notes in Computer Science*, pages 459–477. Springer.

[Yum, Lee 2004] Yum, D. H., Lee, P. J. (2004). Generic construction of certificateless signature. In *ACISP 2004*, volume 3108 of *Lecture Notes in Computer Science*, pages 200–211, Sydney, Australia. Springer-Verlag.

[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.

[Zhang, Mao 2007] Zhang, J., Mao, J. (2007). Security analysis of two signature schemes and their improved schemes. In *Computational Science and Its Applications ICCSA 2007*, volume 4705 of *Lecture Notes in Computer Science*, pages 589–602. Springer Berlin.

[Zhang et al. 2007] Zhang, L., Zhang, F.,, Wu, W. (2007). A provably secure ring signature scheme in certificateless cryptography. In *Provable Security*, volume 4784 of *Lecture Notes in Computer Science*, pages 103–121. Springer.

[Zhang et al. 2006] Zhang, Z., Wong, D. S., XU, J.,, FENG, D. (2006). Certificateless public key signature: Security model and efficient construction. In *4th. International Conference on Applied Cryptography and Network Security, ACNS'06*, volume 3989 of *Lecture Notes in Computer Science*, Singapore. Springer.