Protocolo de Assinatura Rabin, sem Randomização, e com Prova Eficiente de Segurança

Exame de Qualificação de Mestrado

Bernardo C. Magri

Universidade de São Paulo - Instituto de Matemática e Estatística

4 de agosto de 2011

Visão Geral

Objetivos

Desenvolver um protocolo de Assinatura que:

- Utilize a função Rabin (equivalente a fatoração).
- Tenha uma prova eficiente de segurança, no modelo do oráculo aleatório.
- Não necessita de randomização na entrada.
- Utilize a raiz quadrada principal da mensagem.
- Seja eficiente para ser usado na prática.

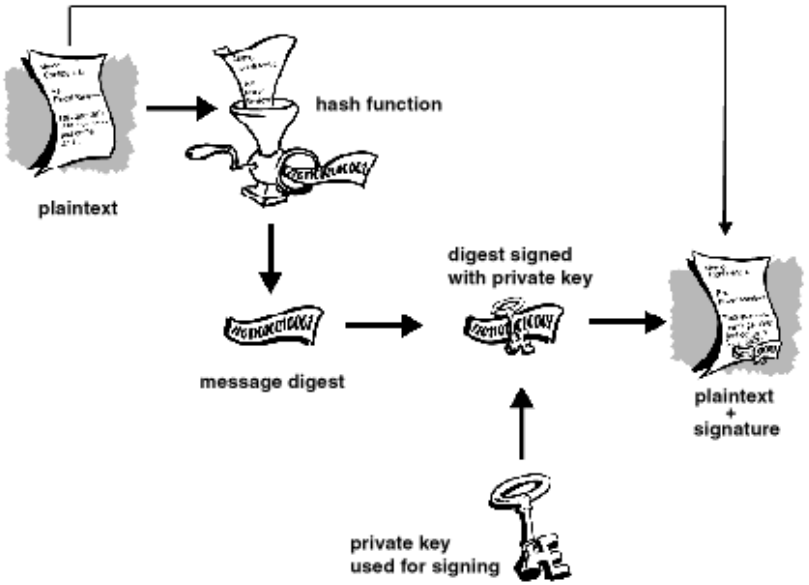
Motivação

Estender o trabalho de [Bernstein, 2008] para o caso da raiz quadrada principal.

Introdução

Assinaturas digitais são semelhantes às assinaturas convencionais em papel. Ambas buscam os mesmos objetivos:

- Não-repudiação.
- Autenticação do remetente.
- Garantia da integridade da mensagem.



Introdução

O PSS-RSA foi o primeiro protocolo eficiente de assinatura digital com uma prova eficiente de segurança.
Muitos trabalhos posteriores tentaram de alguma forma *melhorar* o desempenho do protocolo, tanto em eficiência, quanto em segurança.

Estado da Arte

	B, número de bits aleatórios na entrada do hash		
	B grande	B =1	B=0: sem randomização na entrada do hash
Não-Estruturado Variável Rabin/Williams	redução eficiente (1996 Bellare/Rogaway)	sem segurança (ataque fácil)	sem segurança (ataque fácil)
Principal Variável Rabin/Williams	redução eficiente (2008 Bernstein)	redução ineficiente	redução ineficiente
RSA Variável	redução eficiente (1996 Bellare/Rogaway)	redução ineficiente (1993 Bellare/Rogaway)	redução ineficiente (1993 Bellare/Rogaway)
RSA Fixo	redução eficiente (1996 Bellare/Rogaway)	redução eficiente (2003 Katz/Wang)	redução ineficiente (1993 Bellare/Rogaway)
Principal Fixo Rabin/Williams	redução eficiente (2008 Bernstein)	redução eficiente (2008 Bernstein)	redução ineficiente
Não-Estruturado Fixo Rabin/Williams	redução eficiente (1996 Bellare/Rogaway)	redução eficiente (2008 Bernstein)	redução eficiente (2008 Bernstein)

Tipos de Ataque a Assinaturas

- Ataque de chave pública (*Key-Only attack*).
- Ataque com assinatura conhecida (*Known signature attack*).
- Ataque de mensagem escolhida (*(Adaptive) Chosen message attack.*).

Objetivos do Adversário

- Falsificação existente (*Existential forgery*)
- Falsificação selecionada (*Selective forgery*).
- Falsificação universal (*Universal forgery*).
- Quebra total (*Total break*).

Modelo do Oráculo Aleatório

- Foi introduzido por [Bellare and Rogaway, 1993].
- Assume-se que todas as partes envolvidas no protocolo tem acesso a um "oráculo" aleatório e uniforme.

Modelo do Oráculo Aleatório

1. Assuma que existe um problema Π.
2. Encontre uma definição formal para Π no modelo em que todos os participantes compartilhem um oráculo aleatório R.
3. Desenvolva um protocolo P para Π nesse modelo do oráculo aleatório.
4. Prove que P satisfaz a definição de Π.
5. Substitua os acessos ao oráculo R por uma função de hash H.

Críticas ao Modelo do Oráculo Aleatório

1. Não retrata a realidade das aplicações atuais.
2. [Canetti et al., 2004] é um artigo que explora algumas fraquezas do modelo.

Protocolo Simples de Assinatura RSA

- $n = p \cdot q$
- $\Phi(n) = (p-1)(q-1)$
- $e \cdot d \equiv 1 \mod \Phi(n)$
- Para assinar M: $\sigma(M) = M^d \mod n$
- Para verificar a assinatura: $M \stackrel{?}{=} \sigma(M)^e \mod n$

Fácil de obter FALSIFICAÇÕES!

Protocolo Simples de Assinatura RSA

- $n = p \cdot q$
- $\Phi(n) = (p-1)(q-1)$
- $e \cdot d \equiv 1 \mod \Phi(n)$
- Para assinar M: $\sigma(M) = M^d \mod n$
- Para verificar a assinatura: $M \stackrel{?}{=} \sigma(M)^e \mod n$

Fácil de obter FALSIFICAÇÕES!

Ataque de Davida

1. Seja m a mensagem que se quer falsificar uma assinatura.
2. Seja $m_1, ..., m_t$ os fatores de m. Note que a fatoração não precisa ser completa.
3. Seja $sig = S(m')$ a assinatura da mensagem m'.
4. Suponha que o adversário consiga obter as assinaturas $sig_1, ..., sig_t$ das mensagens $m'.m_1, ..., m'.m_t$.
5. Então ele consegue calcular a assinatura s da mensagem m:

$$s = (\prod_{i=1}^{t} sig_i) sig^{-t} \mod n$$

Ataque de Moore

1. Seja m a mensagem que se quer falsificar a assinatura s.
2. Seja s_1 um valor aleatório.
3. Calcule m_1, tal que, (m_1, s_1) seja um par $(\textit{mensagem}, \textit{assinatura})$ válido:

$$m_1 = s_1^e \mod n$$

4. Obtenha (com a cooperação da vítima) a assinatura de $m_1 m$.

$$s_2 = S(m_1 m) = (m_1 m)^d \mod n$$

5. Calcule $s_1^{-1} s_2$[1] para obter a assinatura s da mensagem m:

$$s = s_1^{-1} s_2 = s_1^{-1} (m_1 m)^d = s_1^{-1} s_1 m^d = m^d \mod n$$

[1] Se s_1^{-1} não existir, então s_1 é um múltiplo de n, logo $s_1 = p$ ou $s_1 = q$.

Protocolo de Assinatura RSA ISO/IEC 9796-2

- $\mu(m) = 6A_{16} \parallel m[1] \parallel HASH(m) \parallel BC_{16}$
- $\sigma = \mu(m)^d \mod n$

Não possui prova de segurança!

Protocolo de Assinatura RSA ISO/IEC 9796-2

- $\mu(m) = 6A_{16} \parallel m[1] \parallel HASH(m) \parallel BC_{16}$
- $\sigma = \mu(m)^d \mod n$

Não possui prova de segurança!

Ataque Prático à Assinatura RSA ISO/IEC 9796-2

1. Implementado por [Coron et al., 2009].
2. Escolha um limite B, e seja $\mathcal{B} = \{p_1, ..., p_\ell\}$ o conjunto de todos os números primos menores que B.
3. Escolha $\ell + 1$ mensagens, tal que todos os fatores de $\mu(m_i) \in \mathcal{B}$.
4. Represente um $\mu(m_j)$ como uma combinação multiplicativa dos outros $\mu(m_i)$ resolvendo um sistema linear representado pelo vetor de expoentes de $\mu(m_j)$ em relação aos primos em $\mathcal{B}$.
5. Obtenha as assinaturas de m_i para $i \neq j$ e falsifique a assinatura de m_j.

Probabilistic Signature Scheme (PSS)

- Prova eficiente de segurança (modelo do oráculo aleatório)
- Randomização (uma mensagem tem várias assinaturas)
- Duas funções de *hash* $h: \{0,1\}^* \rightarrow \{0,1\}^{k_1}$.
- $g: \{0,1\}^{k_1} \rightarrow \{0,1\}^{n-k_1-1}$, tal que $g_1 = k$ bits (mais à esquerda) , e g_2 os bits restantes.
- Dois parâmetros de segurança, k_0 e k_1.

$SignPSS(M)$

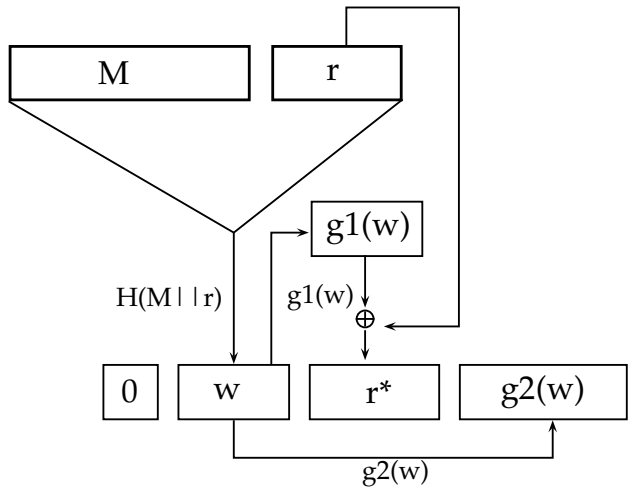
$r \xleftarrow{R} \{0,1\}^{k_0}$

$w \leftarrow h(M \parallel r)$

$r^* \leftarrow g_1(w) \oplus r$

$y \leftarrow 0 \parallel w \parallel r^* \parallel g_2(w)$

retorna $y^d \bmod N$



Segurança do PSS

Suponha que o problema do *RSA* seja (t', ϵ')-seguro. Então para qualquer quantidade de q_{sig}, q_{hash} o protocolo PSS$[k_0, k_1]$ é $(t, q_{sig}, q_{hash}, \epsilon)$-seguro, onde,

$$t = t' - [q_{sig} + q_{hash} + 1] \cdot k_0 \cdot \Theta(k^3)$$

$$\epsilon = \epsilon' + [3(q_{sig} + q_{hash})^2] \cdot (2^{-k_0} + 2^{-k_1})$$

Segurança do PSS (cont.)

- Para uma redução eficiente, é necessário que $\epsilon \simeq \epsilon'$.
- Logo, $(q_{sig} + q_{hash})^2 \cdot (2^{-k_0} + 2^{-k_1}) < \epsilon'$.
- Precisamos que $k_0 \geq k_{min}$ e $k_1 \geq k_{min}$
- $k_{min} = 2 \cdot \log_2(q_{hash} + q_{sig}) + \log_2 \frac{1}{\epsilon'}$
- Se $q_{sig} = 2^{30}$, $q_{hash} = 2^{60}$ e $\epsilon' = 2^{-60}$
- k_0 e $k_1 > 180$ bits.

Nova Prova de Segurança do PSS

- [Coron, 2002] melhorou a redução de segurança.
- $t = t' - q_{sig} + q_{hash} \cdot k_1 \cdot \mathcal{O}(k^3)$
- $\epsilon = \epsilon' \cdot (1 + 6 \cdot q_{sig} \cdot 2^{-k_0}) + 2 \cdot (q_{sig} + q_{hash})^2 \cdot 2^{-k_1}$
- $k_0 = \log_2 q_{sig}$

Uma Variante do PSS

- Criado por [Katz and Wang, 2003].
- Prova eficiente de segurança.
- Assinatura determinística (cada mensagem gera uma única assinatura).
- Necessita de 1 bit de randomização.
- Não é necessário manter estado.
- Baseado em permutações *Claw-Free*.

Permutação Claw-Free

- [Dodis and Reyzin, 2003]alegaram que essa é a suposição que torna as reduções eficientes.
- Um par de funções de permutação (f_0, f_1) sob o mesmo domínio.
- É difícil encontrar um par (x, y), tal que $f_0(x) = f_1(y)$.

Permutação Claw-Free (cont.)

Definition (Permutações Claw-Free)

Uma família de permutações *claw-free* é uma tupla de algorítmos probabilísticos de tempo polinomial (cf-Gen, F, G, F^{-1}, G^{-1}) tal que:

- cf-Gen gera um índice aleatório i e um número *trapdoor* td.
- $F(i, \cdot)$ e $G(i, \cdot)$ são permutações sob o mesmo domínio D_i.
- Existe um algoritmo que recebe como entrada o índice i e retorna um valor em D_i, distribuído uniformemente.
- se (i, td) for o resultado de cf-Gen, então $F^{-1}(td, \cdot)$ é o inverso de $F(i, \cdot)$, e $G^{-1}(td, \cdot)$ é o inverso de $G(i, \cdot)$.

Descrição do Protocolo

Geração das chaves:

- Executa cf-Gen para obter (f, g) e a informação *trapdoor* td.
- A chave pública $PK = f$ e a chave secreta é a *trapdoor* td.

Descrição do Protocolo (cont.)

Assinatura de m:

- verifica se a mensagem m já foi assinada anteriormente
- se sim, **retorna** a assinatura gerada anteriormente
- senão, escolhe um bit aleatório b e **retorna** $\sigma = f^{-1}(H(b \parallel m))$

Descrição do Protocolo (cont.)

Verificação da assinatura (m, σ):

- Se $f(\sigma) = H(0 \parallel m)$ ou $f(\sigma) = H(1 \parallel m)$ **retorna** 1
- Senão **retorna** 0

Prova Eficiente de Segurança

Theorem (Katz e Wang, 2003)

Se a permutação claw-free do protocolo é (t', ϵ')-segura, e o tempo para se computar f ou g é, no máximo, t_f, então o protocolo acima é $(t, q_{hash}, q_{sig}, \epsilon)$-seguro (no modelo do oráculo aleatório), onde:

$$t \leq t' - (q_{hash} + q_{sig}) \cdot t_f$$

$$\epsilon \geq 2\epsilon'$$

Protocolo Simples de Assinatura Rabin

- [Rabin, 1979] estendeu o artigo do RSA [Rivest et al., 1978] e criou uma função de permutação *trapdoor* mais simples e mais *eficiente* do que o RSA.
- A verificação da assinatura pode ser centenas de vezes mais rápida.
- É uma função 1 para 4, e não uma permutação.

Descrição do Protocolo

1. Escolher dois primos grandes p e q, e calcular $n = p \cdot q$.
2. A chave pública é n, e a chave secreta é (p, q).
3. Seja $H : \{0,1\}^* \rightarrow \{0,1\}^n$ uma função de *hash* resistente à colisão.
4. Para assinar uma mensagem m, escolher um número aleatório r, e calcular $h = H(m \parallel r)$.
5. Se $h \notin Q_n$ voltar ao passo anterior. (número de Jacobi)
6. $\sigma \stackrel{R}{=} \sqrt{h} \mod n$.
7. Para verificar se a tupla (m, r, σ) é válida, calcular $H(m \parallel r) \stackrel{?}{=} \sigma^2 \mod n$. Se a igualdade for verdadeira a assinatura é válida, caso contrário, a assinatura é falsa.

Raiz Quadrada Principal

- Escolher p e q tal que $p \equiv q \equiv 3 \mod 4$.
- Transforma a função em uma permutação. $Rabin : Q_n \longrightarrow Q_n$
- A raiz quadrada principal de $h \mod n$ é a *única* raiz quadrada de h, que também é um *resíduo quadrático* de n.

Protocolo de Assinatura Rabin-Williams

- $p \equiv 3 \mod 8$ e $q \equiv 7 \mod 8$
- A assinatura de uma mensagem m é a tupla (e, f, r, s).
- $e \in \{1, -1\}$
- $f \in \{1, 2\}$
- $efs^2 \equiv H(m \parallel r) \mod n$
- Permutação $\mathbb{Z}_n \to \mathbb{Z}_n$.

Prova Eficiente de Segurança para Assinaturas Rabin/Williams

- Criada por [Bernstein, 2008].
- Não necessita de randomização.
- Não utiliza a raiz quadrada principal.
- Nova estrutura para provas de segurança.

Prova Eficiente de Segurança para Assinaturas Rabin/Williams (cont.)

	B, número de bits aleatórios na entrada do hash		
	B grande	B =1	B=0: sem randomização na entrada do hash
Não-Estruturado Variável Rabin/Williams	redução eficiente (1996 Bellare/Rogaway)	sem segurança (ataque fácil)	sem segurança (ataque fácil)
Principal Variável Rabin/Williams	redução eficiente (2008 Bernstein)	redução ineficiente	redução ineficiente
RSA Variável	redução eficiente (1996 Bellare/Rogaway)	redução ineficiente (1993 Bellare/Rogaway)	redução ineficiente (1993 Bellare/Rogaway)
RSA Fixo	redução eficiente (1996 Bellare/Rogaway)	redução eficiente (2003 Katz/Wang)	redução ineficiente (1993 Bellare/Rogaway)
Principal Fixo Rabin/Williams	redução eficiente (2008 Bernstein)	redução eficiente (2008 Bernstein)	redução ineficiente
Não-Estruturado Fixo Rabin/Williams	redução eficiente (1996 Bellare/Rogaway)	redução eficiente (2008 Bernstein)	redução eficiente (2008 Bernstein)

Algumas Definições

- Toda mensagem m possui 2^{r+1} assinaturas distintas módulo pq, sendo 2^r escolhas da variável aleatória r, e 4 escolhas de raízes quadradas.
- Qual assinatura que o assinante deverá retornar?

Existem três propostas:

1. Não-Estruturado.
2. Principal.
3. |Principal|.

Algumas Definições (cont.)

Outro ponto importante, é a diferença entre assinatura *fixa*, e *variável*.

- Fixa: se o protocolo recebe mais de uma vez a mesma mensagem para ser assinada, ele escolhe a mesma assinatura em todas as vezes.
- Variável: se o protocolo recebe mais de uma vez a mesma mensagem para ser assinada, ele gera uma nova assinatura, que é baseada em escolhas aleatórias e independentes das escolhas anteriores.

Nova Estrutura para Provas

- Estrutura em camadas.
- Tenta capturar a intuição de um criptánalista analisando o protocolo.
- permite enxergar com mais *clareza* os detalhes da redução.
- Considera 5 problemas básicos.

5 Problemas Básicos

1. Inversão da função (*Generic blind inversion*).
2. Inversão selecionada com uma assinatura (*Generic selective inversion with one signature*).
3. Inversão selecionada com várias assinaturas (*Generic selective inversion with many signatures*).
4. Inversão existencial (*Generic existential inversion*).
5. Ataques genéricos (*Generic attacks*).

Prova de Segurança

- A prova de segurança é feita através da nova *estrutura* criada.
- A intuição é assumir 5 algoritmos $(\mathcal{A}_1, ..., \mathcal{A}_5)$, que resolvam cada problema básico descrito.
- Depois, faça uma redução (polinomial) do problema da fatoração para o algoritmo $\mathcal{A}_1$.
- Faça redução do $\mathcal{A}_1$ para o $\mathcal{A}_2$, e assim sucessivamente, para todos os algoritmos restantes.

Contribuição Pretendida

Estender o trabalho de [Bernstein, 2008], e tentar encontrar uma prova eficiente de segurança para o protocolo*Rabin-Williams Principal Fixo* $B = 0$.
Isso iria melhorar o estado da arte atual [Bernstein, 2008], tornando desnecessário o uso de uma função secreta adicional para tornar fixa a escolha das raízes quadradas.
Em [Bernstein, 2008] é citado que "Uma prova para o caso da raiz quadrada principal parece ser mais difícil de encontrar, e em alguns casos parecem não existir...".

Contribuição Pretendida (cont.)

O protocolo pretendido (*Rabin-Williams Principal Fixo B = 0*) não viola a restrição imposta em [Coron, 2002], que diz que protocolos de assinatura *hash-and-sign* com assinatura única não podem ter uma redução eficiente de segurança.

Cronograma de Atividades

Atividade	Ago	Set	Out	Nov	Dez
Desenvolver a prova	X	X	X		
Implementar		X	X		
Escrever dissertação		X	X	X	
Defesa					X


Bellare, M. and Rogaway, P. (1993).
Random oracles are practical: a paradigm for designing efficient protocols.
In *Proceedings of the 1st ACM conference on Computer and communications security*, CCS '93, pages 62–73, New York, NY, USA. ACM.


Bernstein, D. J. (2008).
Proving tight security for rabin/williams signatures.
In *In EUROCRYPT*.


Canetti, R., Goldreich, O., and Halevi, S. (2004).
The random oracle methodology, revisited.
J. ACM, 51:557–594.


Coron, J.-S. (2002).
Optimal security proofs for pss and other signature schemes.

In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '02, pages 272–287, London, UK, UK. Springer-Verlag.

Coron, J.-S., Naccache, D., Tibouchi, M., and Weinmann, R.-P. (2009).
Practical cryptanalysis of iso/iec 9796-2 and emv signatures.
In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, pages 428–444, Berlin, Heidelberg. Springer-Verlag.

Dodis, Y. and Reyzin, L. (2003).
On the power of claw-free permutations.
In *Proceedings of the 3rd international conference on Security in communication networks*, SCN'02, pages 55–73, Berlin, Heidelberg. Springer-Verlag.


Katz, J. and Wang, N. (2003).
Efficiency improvements for signature schemes with tight security reductions.
In *Proceedings of the 10th ACM conference on Computer and communications security*, CCS '03, pages 155–164, New York, NY, USA. ACM.


Rabin, M. O. (1979).
Digitalized signatures and public-key functions as intractable as factorization.
Technical report, Cambridge, MA, USA.


Rivest, R. L., Shamir, A., and Adleman, L. (1978).
A method for obtaining digital signatures and public-key cryptosystems.
Commun. ACM, 21:120–126.