

Proposta de aprimoramento para o protocolo de assinatura digital Quartz

Ewerton Rodrigues Andrade

ewe@ime.usp.br

Instituto de Matemática e Estatística - IME
Universidade de São Paulo - USP

Agência de fomento:

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES

Defesa de Dissertação de Mestrado

27 de agosto de 2013

Banca Examinadora:

Prof Dr Routo Terada – IME/USP

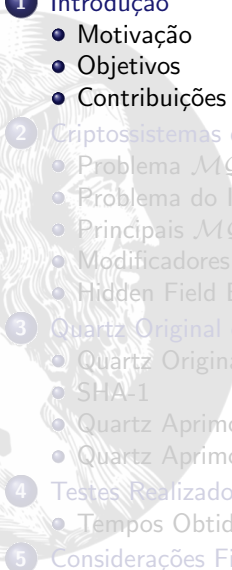
Prof Dr Marco Dimas Gubitoso – IME/USP

Prof^a Dr^a Denise Hideko Goya – CMCC/UFABC

Sumário

- 1 Introdução
 - Motivação
 - Objetivos
 - Contribuições
- 2 Criptosistemas de Chave Pública Multivariada
 - Problema MQ
 - Problema do Isomorfismo de Polinômios
 - Principais MQ -Trapdoors
 - Modificadores Genéricos
 - Hidden Field Equations - HFE
- 3 Quartz Original e Quartz Aprimorado
 - Quartz Original
 - SHA-1
 - Quartz Aprimorado
 - Quartz Aprimorado x Outros Protocolos
- 4 Testes Realizados
 - Tempos Obtidos
- 5 Considerações Finais

Sumário

- 
- 1 Introdução
 - Motivação
 - Objetivos
 - Contribuições
 - 2 Criptosistemas de Chave Pública Multivariada
 - Problema MQ
 - Problema do Isomorfismo de Polinômios
 - Principais MQ -*Trapdoors*
 - Modificadores Genéricos
 - Hidden Field Equations - HFE
 - 3 Quartz Original e Quartz Aprimorado
 - Quartz Original
 - SHA-1
 - Quartz Aprimorado
 - Quartz Aprimorado x Outros Protocolos
 - 4 Testes Realizados
 - Tempos Obtidos
 - 5 Considerações Finais

Motivação

Criptossistemas Clássicos (*Quânticos*)

- Diffie e Hellman (1976) propõem “solução” para troca segura de informações sobre canal inseguro (cript. pública) [DH76];
- São criptossistemas baseados na **teoria dos números**;
- Estes sistemas criptográficos são os “adotados” até hoje.
 - **Fatoração de Inteiros** (RSA)
 - **Logaritmo Discreto** (ElGamal / Curvas Elípticas)

Motivação

Criptossistemas Clássicos (*Quânticos*)

- Diffie e Hellman (1976) propõem “solução” para troca segura de informações sobre canal inseguro (cript. pública) [DH76];
- São criptossistemas baseados na **teoria dos números**;
- Estes sistemas criptográficos são os “adotados” até hoje.
 - **Fatoração de Inteiros** (RSA)
 - **Logaritmo Discreto** (ElGamal / Curvas Elípticas)

Origem dos Criptossistemas Modernos (*Pós-Quânticos*)

- Deutsch (1985) propõe opção mais poderosa que a máquina universal de Turing: **O computador quântico** [Deu85];
- Shor (1997) formula **algoritmo polinomial quântico** para fatoração de inteiros e cálculo do logaritmo discreto [Sho97].

Motivação

Criptossistemas Clássicos (*Quânticos*)

- Diffie e Hellman (1976) propõem “solução” para troca segura de informações sobre canal inseguro (cript. pública) [DH76];
- São criptossistemas baseados na **teoria dos números**;
- Estes sistemas criptográficos são os “adotados” até hoje.
 - **Fatoração de Inteiros** (RSA)
 - **Logaritmo Discreto** (ElGamal / Curvas Elípticas)

Origem dos Criptossistemas Modernos (*Pós-Quânticos*)

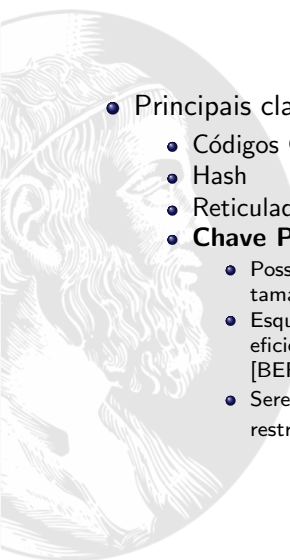
- Deutsch (1985) propõe opção mais poderosa que a máquina universal de Turing: **O computador quântico** [Deu85];
 - Shor (1997) formula **algoritmo polinomial quântico** para fatoração de inteiros e cálculo do logaritmo discreto [Sho97].
- Evolução natural do poder computacional e das criptoanálises.

Criptografia Pós-Quântica (CPQ)

Possíveis Abordagens da CPQ

- **Desenvolver/Aprimorar sistemas criptográficos baseados em problemas intratáveis em computadores quânticos;**
- Determinar a complexidade quântica das hipóteses de intratabilidade;
- Avaliar a segurança e a usabilidade de tais sistemas.

Criptografia Pós-Quântica (CPQ)

- 
- Principais classes de criptosistemas Pós-Quânticos:
 - Códigos Corretores de Erros
 - Hash
 - Reticulados
 - **Chave Pública Multivariada (MPKC)**
 - Possibilitam a criação de esquemas de assinatura digital com tamanho assinaturas reduzidos [Cou04];
 - Esquemas derivados desta primitiva tem se mostrado rápidas e eficientes, tanto em software, quanto em hardware [BERW08, CCC+09];
 - Serem indicados como uma opção para sistemas embarcados com restrição de processamento [BBD09, DGS06, Hei09].

Motivação (Cont.)

Porque estudar o Quartz?

- O Quartz é baseado no HFEv-;
- HFE (*Hidden Field Equations*) é um criptossistema proposto por Patarin na EUROCRYPT de 96 que baseia-se nos **Problemas \mathcal{MQ}** e IP (Isomorfismo de Polinômios);
- O problema \mathcal{MQ} é **NP-completo** [PG97].

Objetivos

Os objetivos principais deste trabalho são:

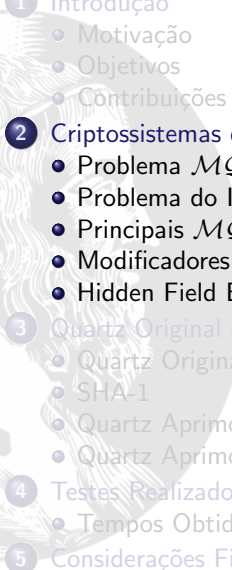
- **análise** do esquema de assinatura digital **Quartz**, proposto por Patarin, Courtois e Goubin, idealizado para gerar assinaturas extremamente curtas;
- a apresentação de um novo protocolo de assinatura digital **Quartz Aprimorado**, com foco no aumento da segurança;
- o desenvolvimento de uma **implementação do Quartz**, tanto em seu modelo original quanto aprimorado;
- **análise de nossa proposta de aprimoramento**, através da estimativa de segurança e apreciação dos tempos obtidos durante os testes realizados a partir de nossa implementação.

Contribuições

As principais contribuições deste trabalho são:

- a **apresentação de um novo protocolo** de assinatura digital baseado no Quartz, logo, com assinaturas extremamente curtas e fundamentado em um problema intratável até mesmo em computadores quânticos;
- obtenção de um criptossistema resistente a ataques adaptativos que realizem chamadas ao oráculo aleatório, com um **nível de segurança** estimado em 2^{112} , contra os 2^{50} do protocolo original;
- demonstração de que nosso aprimoramento irá **testar até 4.096 vezes menos** hipóteses de utilização da chave pública durante a verificação de assinatura, quando comparado com o Quartz Original;
- **implementação** do Quartz Original e do Quartz Aprimorado em uma linguagem de programação altamente portátil.

Sumário

- 
- 1 Introdução
 - Motivação
 - Objetivos
 - Contribuições
 - 2 Criptosistemas de Chave Pública Multivariada
 - Problema MQ
 - Problema do Isomorfismo de Polinômios
 - Principais MQ -Trapdoors
 - Modificadores Genéricos
 - Hidden Field Equations - HFE
 - 3 Quartz Original e Quartz Aprimorado
 - Quartz Original
 - SHA-1
 - Quartz Aprimorado
 - Quartz Aprimorado x Outros Protocolos
 - 4 Testes Realizados
 - Tempos Obtidos
 - 5 Considerações Finais

Sistema de Equações Multivariadas Quadráticas Simultâneas

Sejam:

- $n \in \mathbb{N}$, onde n é a quantidade de variáveis da equação;
- $m \in \mathbb{N}$, onde m é a quantidade de equações do sistema;
- $d \in \mathbb{N}$, onde d é o grau do sistema de equações;
- \mathbb{F} um corpo finito (*Corpo de Galois*);
- $q := |\mathbb{F}|$, ou seja, q é a quantidade de elementos de \mathbb{F} ;
- $\mathcal{P} = (p_1, \dots, p_m)$, onde \mathcal{P} é um sistema sobre \mathbb{F} com m polinômios de grau d com n variáveis;
- $y = (y_1, \dots, y_m) \in \mathbb{F}^m$, onde y é um vetor.

- Então o problema do Sistema de Equações Polinomiais Multivariadas Simultâneas **consiste em encontrar** $x = (x_1, \dots, x_n) \in \mathbb{F}^n$ tal que:

$$\begin{cases} p_1(x_1, \dots, x_n) = y_1 \\ p_2(x_1, \dots, x_n) = y_2 \\ \vdots \\ p_m(x_1, \dots, x_n) = y_m \end{cases}$$

Sistema de Equações Multivariadas Quadráticas Simultâneas

Sejam:

- $n \in \mathbb{N}$, onde n é a quantidade de variáveis da equação;
- $m \in \mathbb{N}$, onde m é a quantidade de equações do sistema;
- $d \in \mathbb{N}$, onde d é o grau do sistema de equações;
- \mathbb{F} um corpo finito (*Corpo de Galois*);
- $q := |\mathbb{F}|$, ou seja, q é a quantidade de elementos de \mathbb{F} ;
- $\mathcal{P} = (p_1, \dots, p_m)$, onde \mathcal{P} é um sistema sobre \mathbb{F} com m polinômios de grau d com n variáveis;
- $y = (y_1, \dots, y_m) \in \mathbb{F}^m$, onde y é um vetor.

$$d \geq 2 \Rightarrow \text{MQ}$$

- Então o problema do Sistema de Equações Polinomiais Multivariadas Simultâneas **consiste em encontrar** $x = (x_1, \dots, x_n) \in \mathbb{F}^n$ tal que:

$$\begin{cases} p_1(x_1, \dots, x_n) = y_1 \\ p_2(x_1, \dots, x_n) = y_2 \\ \vdots \\ p_m(x_1, \dots, x_n) = y_m \end{cases}$$

Sistema de Equações Multivariadas Quadráticas Simultâneas

Sejam:

- $n \in \mathbb{N}$, onde n é a quantidade de variáveis da equação;
 - $m \in \mathbb{N}$, onde m é a quantidade de equações do sistema;
 - $d \in \mathbb{N}$, onde d é o grau do sistema de equações; $d \geq 2 \Rightarrow MQ$
 - \mathbb{F} um corpo finito (*Corpo de Galois*);
 - $q := |\mathbb{F}|$, ou seja, q é a quantidade de elementos de \mathbb{F} ; $\mathbb{F} = GF(2)$ ou $GF(2^k)$
 - $\mathcal{P} = (p_1, \dots, p_m)$, onde \mathcal{P} é um sistema sobre \mathbb{F} com m polinômios de grau d com n variáveis;
 - $y = (y_1, \dots, y_m) \in \mathbb{F}^m$, onde y é um vetor.
- Então o problema do Sistema de Equações Polinomiais Multivariadas Simultâneas **consiste em encontrar** $x = (x_1, \dots, x_n) \in \mathbb{F}^n$ tal que:

$$\begin{cases} p_1(x_1, \dots, x_n) = y_1 \\ p_2(x_1, \dots, x_n) = y_2 \\ \vdots \\ p_m(x_1, \dots, x_n) = y_m \end{cases}$$

Problema MQ

- Para qualquer q e d (normalmente igual a 2) nós chamamos então de Problema de equações *M*ultivariadas *Q*uadráticas e designamos o correspondente vetor \mathcal{P} como $MQ(n, m, \mathbb{F})$.

Formato genérico da função MQ

$$p_1(x_1, \dots, x_n) := \sum_{1 \leq i < j \leq n} \alpha_{1,i,j} x_i x_j + \sum_{i=1}^n \beta_{1,i} x_i + \delta_1$$

$$\vdots$$

$$p_l(x_1, \dots, x_n) := \sum_{1 \leq i < j \leq n} \alpha_{l,i,j} x_i x_j + \sum_{i=1}^n \beta_{l,i} x_i + \delta_l$$

$$\vdots$$

$$p_m(x_1, \dots, x_n) := \sum_{1 \leq i < j \leq n} \alpha_{m,i,j} x_i x_j + \sum_{i=1}^n \beta_{m,i} x_i + \delta_m$$

Função *Trapdoor*

Segundo Patarin e Goubin (1997):

Função de mão única (*one-way function*)

Seja $f : \mathcal{D} \mapsto \mathcal{I}$ uma função. f é dita de mão única se:

- Dado $x \in \mathcal{D}$, seja fácil calcular $y = f(x)$;
- Dado $y \in_R \mathcal{I}$, seja difícil calcular $x \in \mathcal{D}$ tal que $f(x) = y$.

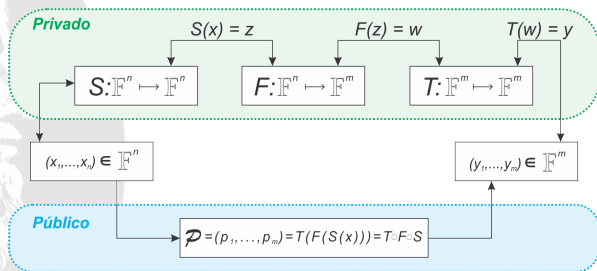
Função Alçapão (*trapdoor*)

Seja $f : \mathcal{D} \mapsto \mathcal{I}$ uma função. f é dita uma função *trapdoor* se:

- f seja uma função de mão única;
- Existe uma informação secreta t tal que, dado $y \in_R \mathcal{I}$ e t , seja fácil calcular $x \in \mathcal{D}$ tal que $f(x) = y$.

Função MQ-Trapdoor

- Partindo de um conjunto de equações polinomiais “fáceis” utiliza-se duas transformações afins “criar” uma aparente instância aleatória de uma função MQ.



- A Chave Pública \mathcal{P} é a composição de duas transformações afins inversíveis $S: \mathbb{F}^n \mapsto \mathbb{F}^n$ e $T: \mathbb{F}^m \mapsto \mathbb{F}^m$, e um mapeamento central $F: \mathbb{F}^n \mapsto \mathbb{F}^m$, tal que F seja um vetor de polinômios $F = (p'_1, \dots, p'_m)$, onde $\mathcal{P} = T \circ F \circ S$.

Isomorfismo de Polinômios (IP)

- Baseado na dificuldade de **decompor** \mathcal{P} em (S, F, T) ;
- A tripla (S, F, T) obtida na solução do problema do IP permitiu, inicialmente, a implementação de autenticação (*zero knowlegde*) e assinatura [Pat96];

Isomorfismo de Polinômios (IP)

- Baseado na dificuldade de **decompor** \mathcal{P} em (S, F, T) ;
- A tripla (S, F, T) obtida na solução do problema do IP permitiu, inicialmente, a implementação de autenticação (*zero knowlegde*) e assinatura [Pat96];
- IP para instâncias aleatórias é supostamente difícil, porém quando F possui uma “estrutura especial” é possível que o correspondente problema IP se torne fácil e possibilite a **quebra** do sistema devido esta fraqueza.

Principais MQ -Trapdoors

- A principal diferença entre as atuais MQ -trapdoors está no **mapeamento central F** ;
- As duas transformações afins (S e T) funcionam praticamente da mesma forma em todas *trapdoors*.

2 Classes Genéricas que agrupam as 5 principais MQ -trapdoors

Big Field	Matsumoto-Imai scheme A (MIA) [MI88] Hidden Field Equations (HFE) [Pat96]
Single Field	Unbalanced Oil and Vinegar (UOV) [KPG99] Step-wise Triangular Systems (STS) [WBP04] ℓ -Invertible Cycles (ℓ -IC) [DWY07]

Modificações Genéricas em esquemas MQ

- **Versões básicas** de todas MQ-Trapdoors **foram quebradas!**
- Aplicar modificadores pode contribuir para a **obtenção de criptosistemas mais seguros.**

Símbolo	Nome	Segurança	Ideia Básica
-	Menos	seguro	remove alguns polinômios
+	Mais	maioria sem efeito	adiciona polinômios
p	Pré-fixo ou Pós-fixo	em aberto	força algum $p_i = 0$
v	Vinagre	pouco mais seguro	variáveis extras são definidas
i	Perturbação Interna	em aberto	equivalente a $p + v$
f	Fixador	em aberto	fixa algumas variáveis forma aleatória
m	Mascaramento	em aberto	descarta algumas variáveis
s	Esparso	em aberto	usa polinômios esparsos

- Assim como as Versões Básicas, alguns modificadores já foram considerados inseguros ou sem efeito:

Ramificação (\perp), Sub-Corpo($/$), Homogeneização(h), Incorporação(\nearrow)

Modificações Genéricas em esquemas MQ

- Todavia, aplicar modificadores também acarreta a **perda de eficiência**.

Símbolo	Nome	Perda
-	Menos	Encriptação mais lenta
+	Mais	Assinatura mais lenta
p	Pré-fixo ou Pós-fixo	Assinatura mais lenta
v	Vinagre	Encriptação mais lenta
i	Pertubação Interna	Tudo mais lento
s	Esparso	<i>Speedup</i> geralmente mais lento

HFE - Esquemas *Big Field*

- Para esquemas *Big Field* são empregadas uma bijeção adicional $\varphi : \mathbb{E} \mapsto \mathbb{F}$ e sua inversa, onde \mathbb{E} é uma extensão do corpo \mathbb{F}_q (ou seja, \mathbb{E} é igual a \mathbb{F}_{q^n}).

Desta forma:

$$\mathbb{F}^n \xrightarrow{S} \mathbb{F}^n \xrightarrow{\varphi^{-1}} \mathbb{E}^n \xrightarrow{F} \mathbb{E}^n \xrightarrow{\varphi} \mathbb{F}^m \xrightarrow{T} \mathbb{F}^m$$

HFE - Visão Geral

- Proposto por Patarin em 1996;
- É uma **generalização do MIA** (C^*).

Sejam:

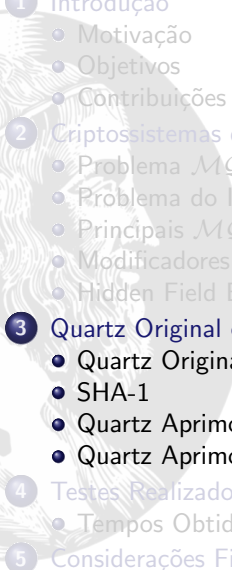
- $i, j, k, d \in \mathbb{N}$, onde d é o grau do sistema de equações;
- \mathbb{F} um corpo finito (*Corpo de Galois*);
- $q := |\mathbb{F}|$, ou seja, q é a quantidade de elementos de \mathbb{F} ;
- \mathbb{E}_{q^k} uma extensão de \mathbb{F}_q com grau k ;
- α_{ij}, β_i e δ elementos de \mathbb{E}_{q^k} ;
- θ_{ij}, σ_{ij} e γ_i pertencentes ao conjunto \mathbb{Z} .

Temos que,

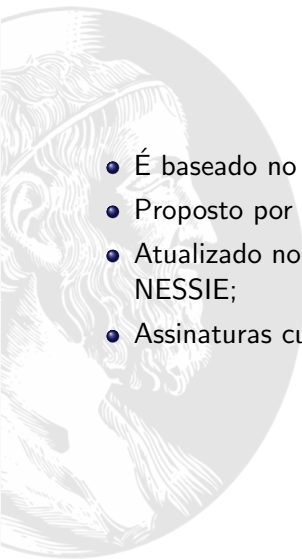
$$f(x) = \sum_{i,j}^d \alpha_{ij} x^{q^{\theta_{ij}} + q^{\sigma_{ij}}} + \sum_i^d \beta_i x^{q^{\gamma_i}} + \delta$$

onde $f(x)$ é um polinômio em x sobre \mathbb{E}_{q^k} com grau d , para os inteiros $0 \leq \theta_{ij}, \sigma_{ij}, \gamma_i \leq d$.

Sumário

- 
- 1 Introdução
 - Motivação
 - Objetivos
 - Contribuições
 - 2 Criptosistemas de Chave Pública Multivariada
 - Problema MQ
 - Problema do Isomorfismo de Polinômios
 - Principais MQ -Trapdoors
 - Modificadores Genéricos
 - Hidden Field Equations - HFE
 - 3 Quartz Original e Quartz Aprimorado
 - Quartz Original
 - SHA-1
 - Quartz Aprimorado
 - Quartz Aprimorado x Outros Protocolos
 - 4 Testes Realizados
 - Tempos Obtidos
 - 5 Considerações Finais

Quartz Original - Visão Geral



- É baseado no HFEv-;
- Proposto por Patarin, Courtois e Goubin em 2001;
- Atualizado no mesmo ano pelos mesmos autores durante o NESSIE;
- Assinaturas curtas (128 bits).

Quartz Original - Definições Básicas

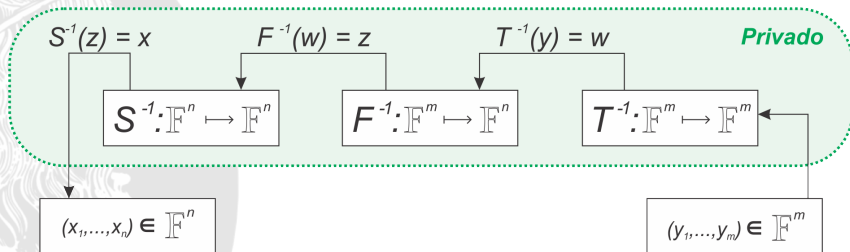
Sejam:

- $n \in \mathbb{N}$, onde n é a quantidade total de variáveis da equação;
- $v \in \mathbb{N}$, onde v é a quantidade de variáveis vinagre;
- $h \in \mathbb{N}$, onde $h = n - v$;
- $m \in \mathbb{N}$, onde m é a quantidade de polinômios do sistema;
- $r \in \mathbb{N}$, onde r é a quantidade de polinômios removidos;
- $d \in \mathbb{N}$, onde d é o grau do sistema de equações;
- \mathbb{F} um corpo finito (*Corpo de Galois*);
- $q := |\mathbb{F}|$, ou seja, q é a quantidade de elementos de \mathbb{F} .

No Quartz Original, temos que:

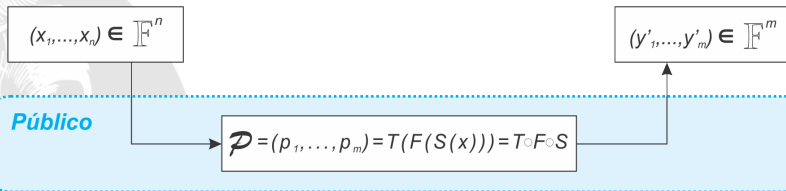
$$n = 107, \quad v = 4, \quad h = 103, \quad m = 100, \quad r = 3, \quad d = 129, \quad q = 2.$$

Quartz Original - Parâmetros Privados



- No QUARTZ, T , F e S são chamadas de t , F_V e s , respectivamente;
- Além disto, é gerada uma cadeia privada de 80 bits, denotada por Δ .

Quartz Original - Parâmetro Público



$$(y'_1, \dots, y'_m) \in \mathbb{F}^m \stackrel{?}{=} (y_1, \dots, y_m) \in \mathbb{F}^m$$

- No Quartz Original, \mathcal{P} é chamada de G .

Algoritmo de Assinatura

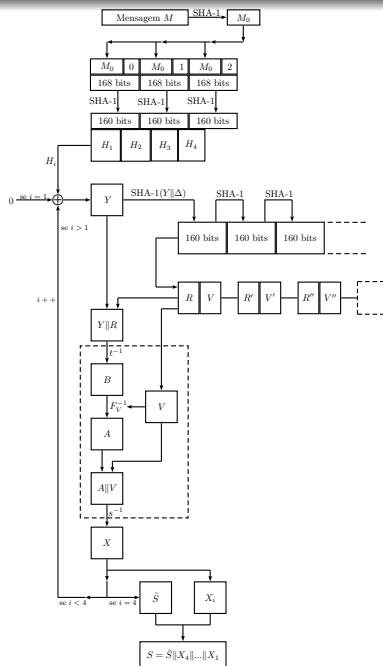
- Sejam M_0 , M_1 , M_2 e M_3 quatro cadeias de 160 bits definidas por:

$$\begin{aligned} M_0 &= \text{SHA-1}(M), \\ M_1 &= \text{SHA-1}(M_0\|0), \\ M_2 &= \text{SHA-1}(M_0\|1), \\ M_3 &= \text{SHA-1}(M_0\|2). \end{aligned}$$

- Sejam H_1 , H_2 , H_3 e H_4 quatro cadeias de 100 bits definidas por:

$$\begin{aligned} H_1 &= [M_1]_{0 \rightarrow 99}, \\ H_2 &= [M_1]_{100 \rightarrow 159} \parallel [M_2]_{0 \rightarrow 39}, \\ H_3 &= [M_2]_{40 \rightarrow 139}, \\ H_4 &= [M_2]_{140 \rightarrow 159} \parallel [M_3]_{0 \rightarrow 79}. \end{aligned}$$

- Seja \tilde{S} uma cadeia de 100 bits, tal que \tilde{S} seja inicializada com $00\dots 0$.



- Para $i = 1$ até 4, faça:
 - Calcule a cadeia de 100 bits Y definida por:

$$Y = H_i \oplus \tilde{S}.$$

- Calcule a cadeia de 160 bits W definida por:

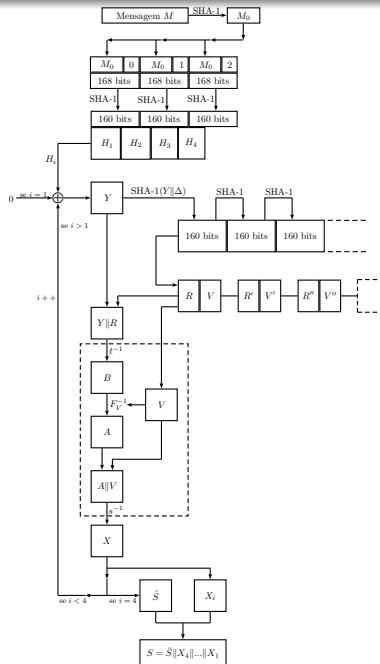
$$W = \text{SHA-1}(Y \parallel \Delta).$$

- Obtenha a cadeia de 3 bits R definida por:

$$R = [W]_{0 \rightarrow 2}.$$

- Obtenha a cadeia de 4 bits V definida por:

$$V = [W]_{3 \rightarrow 6}.$$

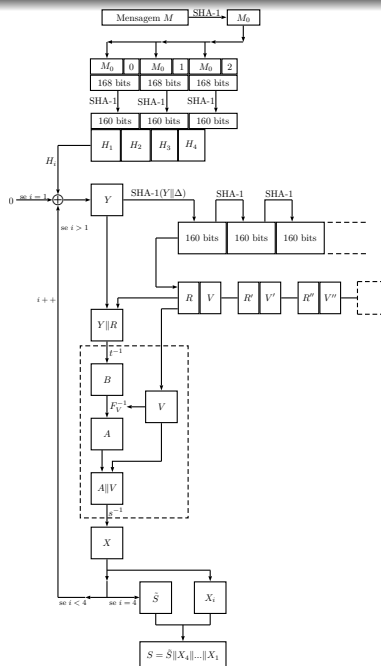


- Para $i = 1$ até 4, faça:
(Continuação)
 - Calcule B tal que ele seja um elemento de \mathbb{E} definido por:

$$B = \varphi(t^{-1}(Y\|R)).$$

- Solucione a seguinte equação polinomial em Z sobre \mathbb{E} :

$$F_V(Z) = B.$$



- Para $i = 1$ até 4, faça:
(Continuação)

- Calcule a cadeia de 107 bits X definida por:

$$X = s^{-1}(\varphi^{-1}((A)\|V)).$$

- Defina um novo valor para a cadeia de 100 bits \tilde{S} como sendo:

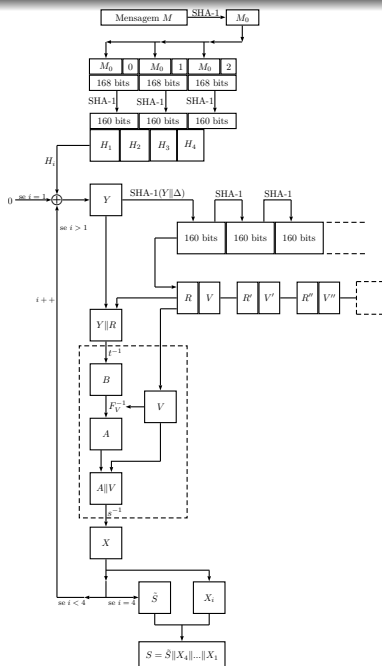
$$\tilde{S} = [X]_{0 \rightarrow 99}.$$

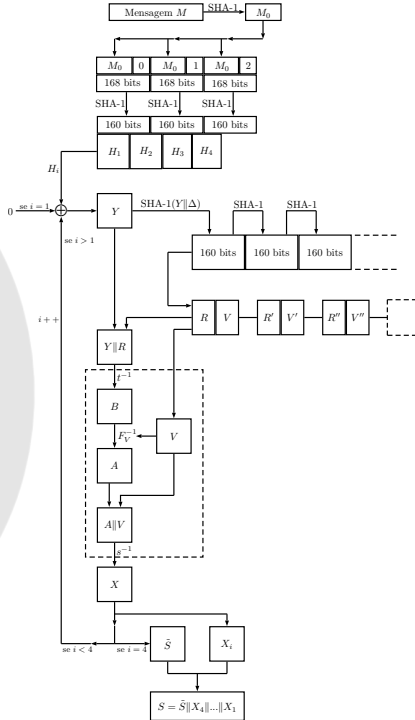
- Obtenha a cadeia de 7 bits X_i definida por:

$$X_i = [X]_{100 \rightarrow 106}.$$

- A assinatura S é a cadeia de 128 bits definida por:

$$S = \tilde{S}\|X_4\|X_3\|X_2\|X_1.$$





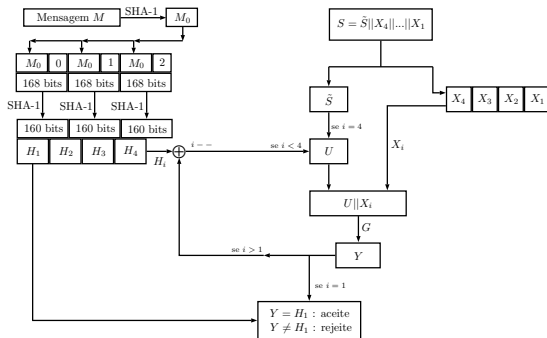
Algoritmo de Verificação

- Sejam M_0 , M_1 , M_2 e M_3 quatro cadeias de 160 bits definidas por:

$$\begin{aligned} M_0 &= \text{SHA-1}(M), \\ M_1 &= \text{SHA-1}(M_0 || 0), \\ M_2 &= \text{SHA-1}(M_0 || 1), \\ M_3 &= \text{SHA-1}(M_0 || 2). \end{aligned}$$

- Sejam H_1 , H_2 , H_3 e H_4 quatro cadeias de 100 bits definidas por:

$$\begin{aligned} H_1 &= [M_1]_{0 \rightarrow 99}, \\ H_2 &= [M_1]_{100 \rightarrow 159} || [M_2]_{0 \rightarrow 39}, \\ H_3 &= [M_2]_{40 \rightarrow 139}, \\ H_4 &= [M_2]_{140 \rightarrow 159} || [M_3]_{0 \rightarrow 79}. \end{aligned}$$



- Seja \tilde{S} uma cadeia de 100 bits definida por:

$$\tilde{S} = [S]_{0 \rightarrow 99}.$$

- Sejam X_4, X_3, X_2 e X_1 quatro cadeias de 7 bits definidas por:

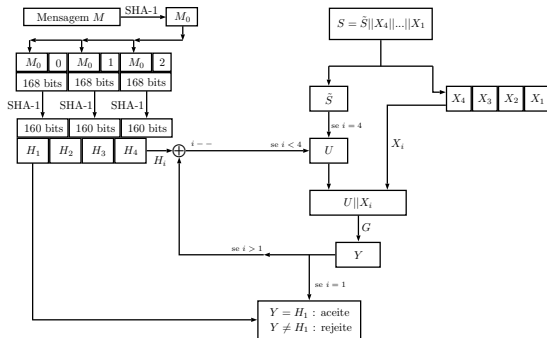
$$X_4 = [S]_{100 \rightarrow 106},$$

$$X_3 = [S]_{107 \rightarrow 113},$$

$$X_2 = [S]_{114 \rightarrow 120},$$

$$X_1 = [S]_{121 \rightarrow 127}.$$

- Seja U uma cadeia de 100 bits, tal que U seja inicializada com \tilde{S} .



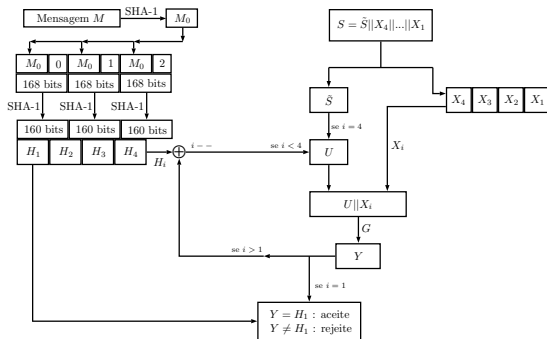
- Para $i = 4$ até 1, faça:
 - Calcule a cadeia de 100 bits Y definida por:

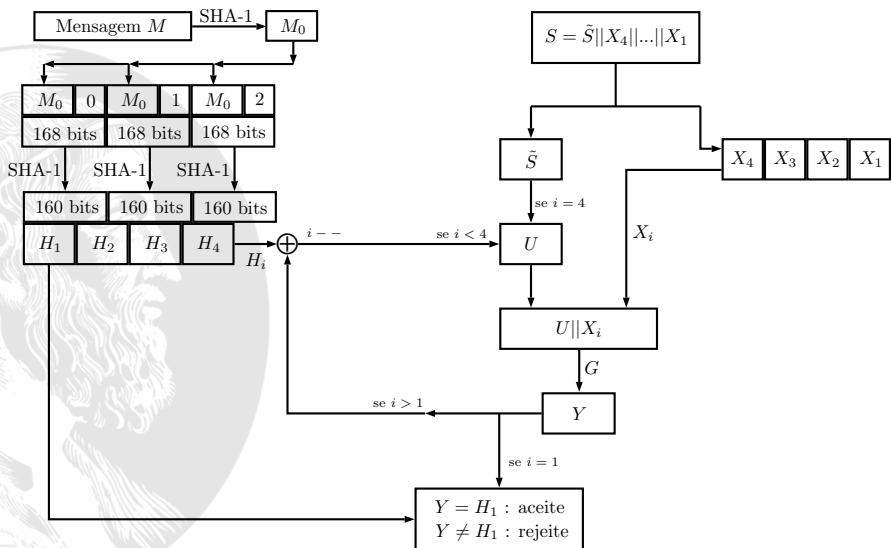
$$Y = G(U||X_i).$$

- Defina um novo valor para a cadeia de 100 bits U como sendo:

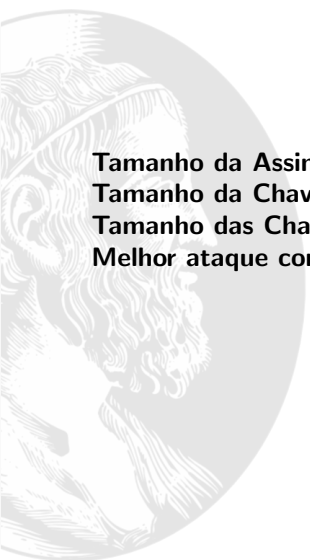
$$U = Y \oplus H_i.$$

- Se U é igual a cadeia 00...0, aceite a assinatura. Caso contrário, rejeite-a.





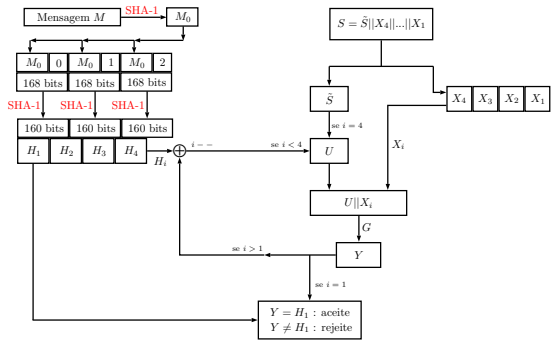
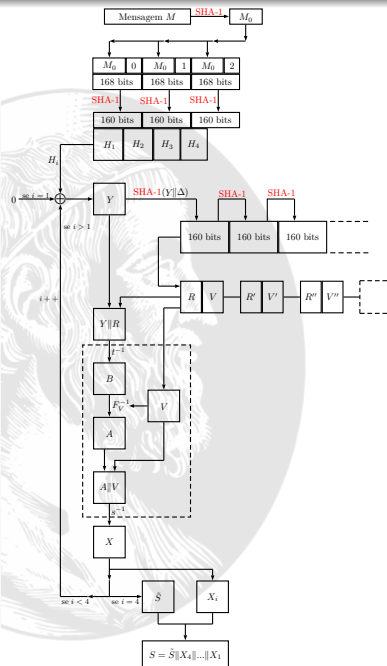
Quartz Original - Principais Características



Tamanho da Assinatura:	128 bits
Tamanho da Chave Pública:	71 Kbytes
Tamanho das Chaves Privadas:	3 Kbytes
Melhor ataque conhecido [JM03]:	2^{50} computações com 2^{50} chamadas ao oráculo aleatório

SHA-1

- O SHA-1 é empregado em diversos pontos do QUARTZ;
- Desde 2005 o SHA-1 é considerado inseguro já que apresenta colisões em 58 iterações com uma complexidade de 2^{33} [WYY05];
- Ano passado, o NIST publicou um Relatório Técnico “proibindo” a utilização do SHA-1 em esquemas de assinatura digital que requeiram uma segurança mínima de 2^{80} , nos EUA [Dan12];
- Além disto, Joux (2004) apresenta um trabalho afirmando que funções hash iteradas são **menos seguras do que esperava-se** [Jou04]. Ou seja, a resistência a colisões é de apenas $\mathcal{O}(n \cdot 2^{n/2})$ e não $\mathcal{O}(2^n)$ como se esperava.



Quartz Aprimorado - Definições Básicas

Sejam:

- $n \in \mathbb{N}$, onde n é a quantidade total de variáveis da equação;
- $v \in \mathbb{N}$, onde v é a quantidade de variáveis vinagre;
- $h \in \mathbb{N}$, onde $h = n - v$;
- $m \in \mathbb{N}$, onde m é a quantidade de polinômios do sistema;
- $r \in \mathbb{N}$, onde r é a quantidade de polinômios removidos;
- $d \in \mathbb{N}$, onde d é o grau do sistema de equações;
- \mathbb{F} um corpo finito (*Corpo de Galois*);
- $q := |\mathbb{F}|$, ou seja, q é a quantidade de elementos de \mathbb{F} .

No Quartz Original, temos que:

$$n = 231, \quad v = 2, \quad h = 229, \quad m = 224, \quad r = 5, \quad d = 129, \quad q = 2.$$

Algoritmo de Assinatura

- Seja Γ uma cadeia de 96 bits, tal que $\Gamma \in_R \{0, 1\}^{96}$;
- Seja M_0 uma cadeia de 512 bits definida por:

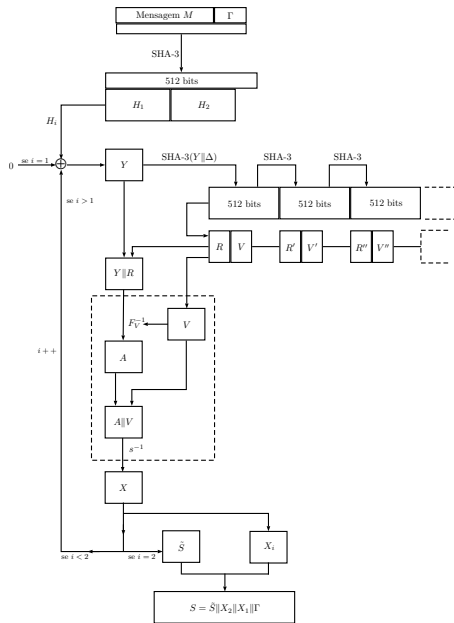
$$M_0 = \text{SHA-3}(M \parallel \Gamma).$$

- Sejam H_1 e H_2 duas cadeias de 224 bits definidas por:

$$H_1 = [M_0]_{0 \rightarrow 223},$$

$$H_2 = [M_0]_{224 \rightarrow 447}.$$

- Seja \tilde{S} uma cadeia de 224 bits, tal que \tilde{S} seja inicializada com $00\dots 0$.



- Para $i = 1$ até 2, faça:
 - Calcule a cadeia de 224 bits Y definida por:

$$Y = H_i \oplus \tilde{S}.$$

- Calcule a cadeia de 512 bits W definida por:

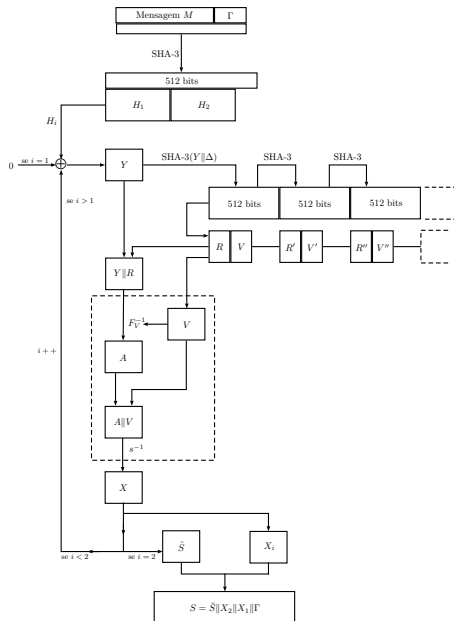
$$W = \text{SHA-3}(Y \parallel \Delta).$$

- Obtenha a cadeia de 5 bits R definida por:

$$R = [W]_{0 \rightarrow 4}.$$

- Obtenha a cadeia de 2 bits V definida por:

$$V = [W]_{5 \rightarrow 6}.$$



- Para $i = 1$ até 2, faça:
(Continuação)

- Solucione a seguinte equação polinomial em Z sobre \mathbb{E} :

$$F_V(Z) = (Y \parallel R).$$

- Calcule a cadeia de 231 bits X definida por:

$$X = s^{-1}(\varphi^{-1}(A) \parallel V).$$

- Defina um novo valor para a cadeia de 224 bits \tilde{S} como sendo:

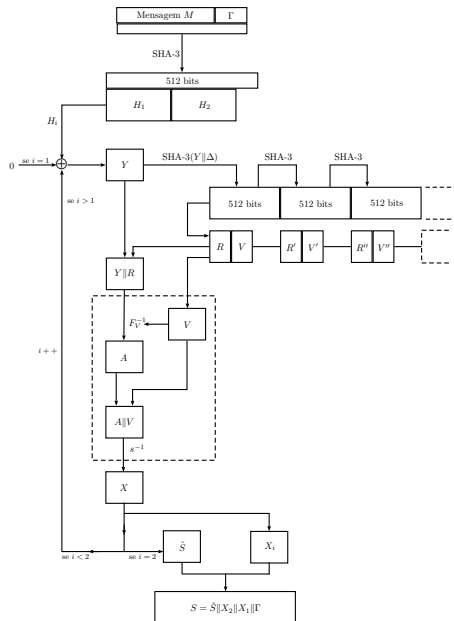
$$\tilde{S} = [X]_{0 \rightarrow 223}.$$

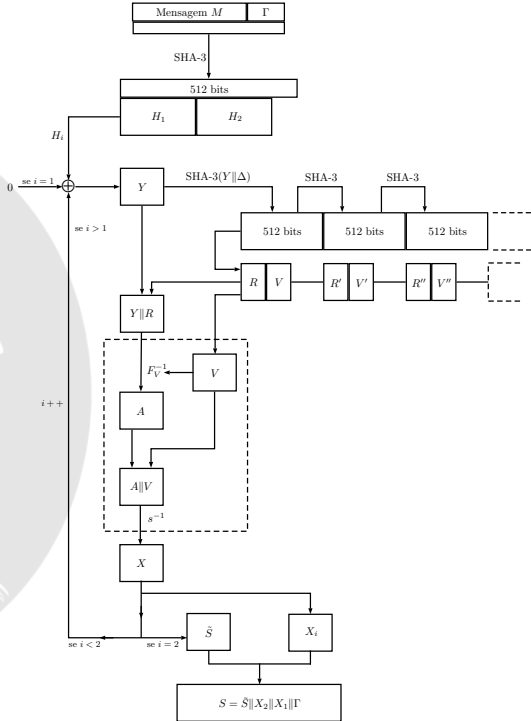
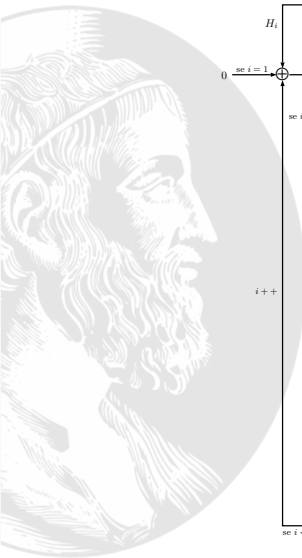
- Obtenha a cadeia de 7 bits X_i definida por:

$$X_i = [X]_{224 \rightarrow 230}.$$

- A assinatura S é a cadeia de 334 bits definida por:

$$S = \tilde{S} \parallel X_2 \parallel X_1 \parallel \Gamma.$$





Algoritmo de Verificação

- Seja \tilde{S} uma cadeia de 224 bits definida por:

$$\tilde{S} = [S]_{0 \rightarrow 223}.$$

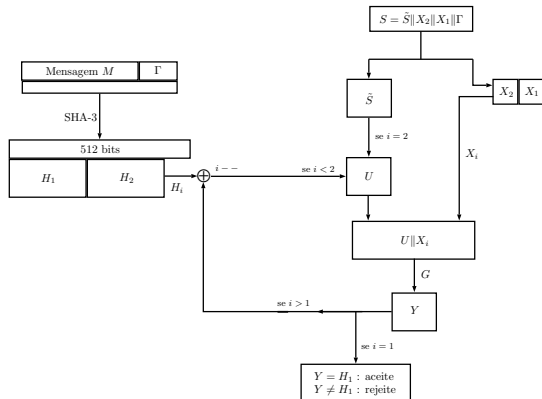
- Sejam X_2 e X_1 duas cadeias de 7 bits definidas por:

$$X_2 = [S]_{224 \rightarrow 230},$$

$$X_1 = [S]_{231 \rightarrow 237}.$$

- Seja Γ uma cadeia de 96 bits definida por:

$$\Gamma = [S]_{238 \rightarrow 334}.$$



- Seja M_0 uma cadeia de 512 bits definida por:

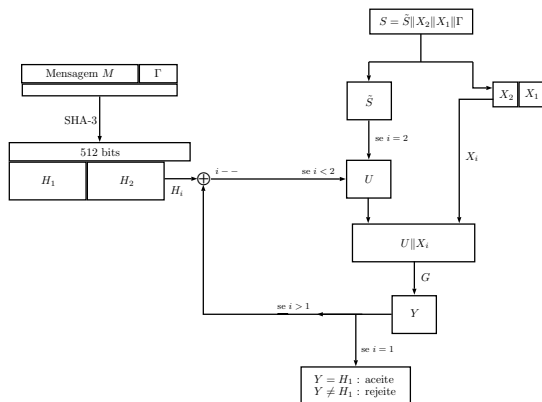
$$M_0 = \text{SHA-3}(M \parallel \Gamma).$$

- Sejam H_1 e H_2 duas cadeias de 224 bits definidas por:

$$H_1 = [M_0]_{0 \rightarrow 223},$$

$$H_2 = [M_0]_{224 \rightarrow 447}.$$

- Seja U uma cadeia de 224 bits, tal que U seja inicializada com \tilde{S} .



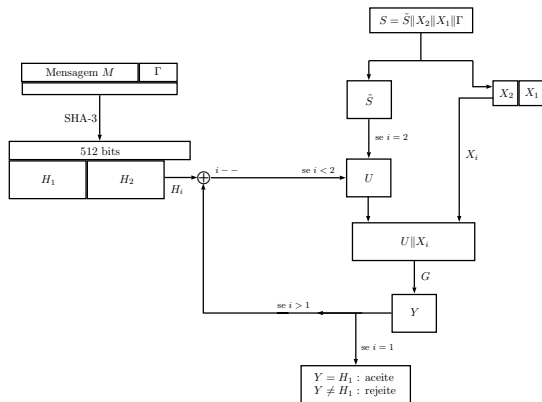
- Para $i = 2$ até 1, faça:
 - Calcule a cadeia de 224 bits Y definida por:

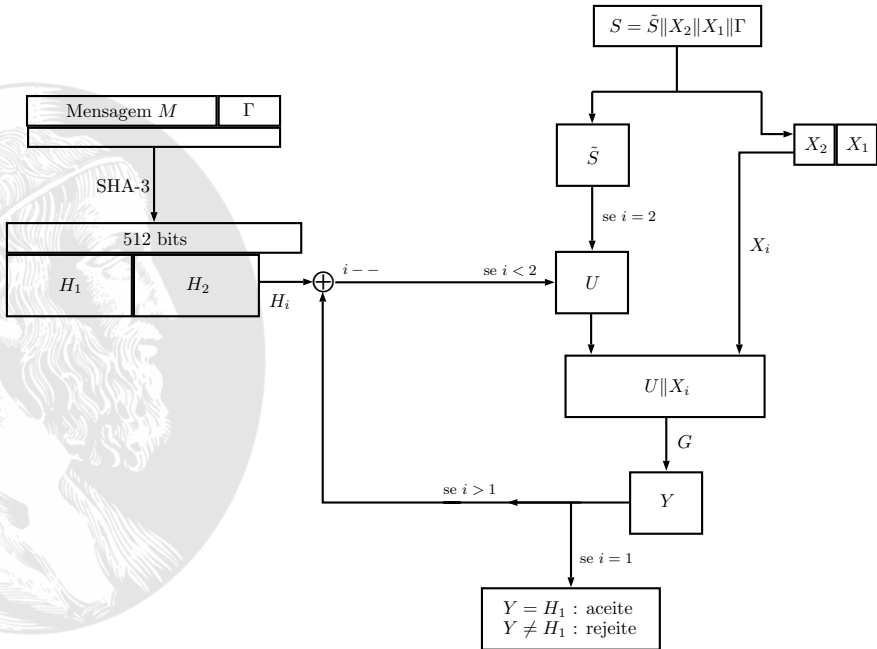
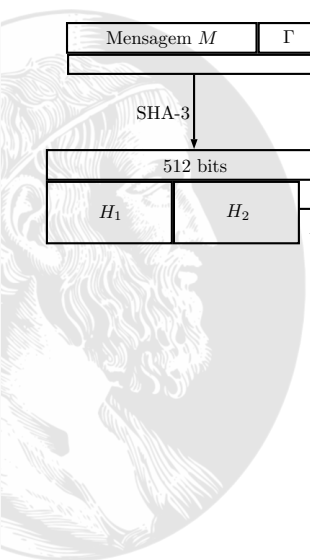
$$Y = G(U \| X_i).$$

- Defina um novo valor para a cadeia de 224 bits U como sendo:

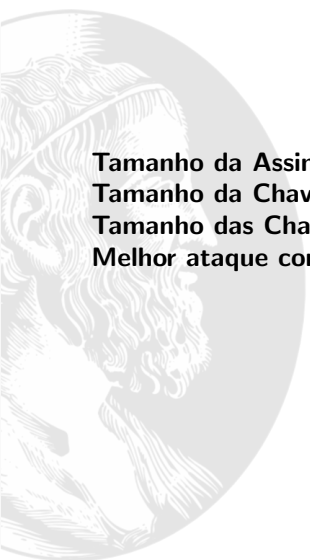
$$U = Y \oplus H_i.$$

- Se U é igual a cadeia 00...0, aceite a assinatura. Caso contrário, rejeite-a.





Quartz Aprimorado - Principais Características



Tamanho da Assinatura:	334 bits
Tamanho da Chave Pública:	739 Kbytes
Tamanho das Chaves Privadas:	8 Kbytes
Melhor ataque conhecido [JM03]:	2^{112} computações com 2^{112} chamadas ao oráculo aleatório

Quartz Aprimorado x Outros Protocolos

Criptosistema		q	d	m	n	Tamanho da Assinatura (em bits)	Ref.
Pós-Quântico	CyclicUOV	256	256	77	77	624	[PBB10a]
	Rainbow	16	30	58	58	352	[PBB10b]
	NC-Rainbow	256	17	26	26	672	[YST12]
	CyclicRainbow	256	17	26	26	344	[PBB10a]
	Quartz Aprimorada	2	129	224	231	334	Nosso
Quântico	ECDSA					400	[NIS09]
	RSA					2.048	[BR11]

Tabela: Tamanho das assinaturas de alguns criptosistemas.

Sumário

- 
- 1 Introdução
 - Motivação
 - Objetivos
 - Contribuições
 - 2 Criptosistemas de Chave Pública Multivariada
 - Problema MQ
 - Problema do Isomorfismo de Polinômios
 - Principais MQ -Trapdoors
 - Modificadores Genéricos
 - Hidden Field Equations - HFE
 - 3 Quartz Original e Quartz Aprimorado
 - Quartz Original
 - SHA-1
 - Quartz Aprimorado
 - Quartz Aprimorado x Outros Protocolos
 - 4 Testes Realizados
 - Tempos Obtidos
 - 5 Considerações Finais

Computadores Utilizados

Para esta simulação, utilizamos dois computadores distintos.
Sendo eles:

Brucutu: processador Intel Xeon E5645 de 2,4 GHz \times 24, com 128 GB de memória RAM, utilizando o Sistema Operacional Linux Debian 7.0 (wheezy), OpenJDK 1.6.0_27 IcedTea e Python 2.7.3;

Ewerton-PC: processador Intel Core i7-2670QM de 2,2 GHz, com 8 GB de memória RAM, utilizando o Sistema Operacional Linux Ubuntu 12.10 (quantal), Java 1.7.0_25 da Oracle e Python 2.7.3.

Tempos obtidos no Brucutu

			Quartz Original	Quartz Aprimorado
Inicialização dos Vetores	SHA-1	Média (ms)	158	-
		Intervalo (ms)	121 - 236	-
	SHA-3	Média (ms)	-	40
		Intervalo (ms)	-	34 - 57
Geração de Chaves	Média (s)		16,9	75,1
	Intervalo (s)		16,5 - 17,7	74,2 - 77,8
Assinatura	Média (s)		5,2	19,1
	Intervalo (s)		4,4 - 27,2	18,9 - 20,0
Verificação de Assinatura	Média (ms)		3.814	18
	Intervalo (ms)		4 - 3.927	17 - 40
Verificação de Assinatura Falsa	Média (ms)		60.074	180
	Intervalo (ms)		52.067 - 62.258	159 - 194


Tabela: Tempos obtidos durante a realização dos testes no Brucutu.

Tempos obtidos no Ewerton-PC

			Quartz Original	Quartz Aprimorado
Inicialização dos Vetores	SHA-1	Média (ms)	62	-
		Intervalo (ms)	47 - 130	-
	SHA-3	Média (ms)	-	15
		Intervalo (ms)	-	12 - 44
Geração de Chaves	Média (s)		18,5	87,0
	Intervalo (s)		15,6 - 26,8	72,2 - 108,3
Assinatura	Média (s)		5,4	16,6
	Intervalo (s)		4,3 - 169,2	16,5 - 25,6
Verificação de Assinatura	Média (ms)		164	35
	Intervalo (ms)		136 - 2.447	33 - 53
Verificação de Assinatura Falsa	Média (ms)		43.248	99
	Intervalo (ms)		36.197 - 54.591	96 - 145

Tabela: Tempos obtidos durante a realização dos testes no Ewerton-PC.

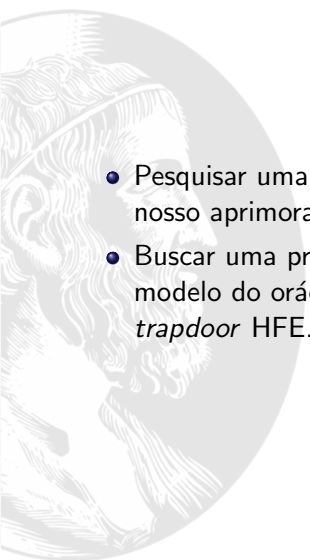
Sumário

- 
- 1 Introdução
 - Motivação
 - Objetivos
 - Contribuições
 - 2 Criptosistemas de Chave Pública Multivariada
 - Problema MQ
 - Problema do Isomorfismo de Polinômios
 - Principais MQ -Trapdoors
 - Modificadores Genéricos
 - Hidden Field Equations - HFE
 - 3 Quartz Original e Quartz Aprimorado
 - Quartz Original
 - SHA-1
 - Quartz Aprimorado
 - Quartz Aprimorado x Outros Protocolos
 - 4 Testes Realizados
 - Tempos Obtidos
 - 5 Considerações Finais

Considerações Finais

- Neste trabalho nós apresentamos um novo protocolo de assinatura digital, baseado no Quartz de Patarin, Courtois e Goubin [CGP01, PCG01], utilizando uma construção que **umenta o nível de segurança** para 2^{112} , contra os 2^{50} do protocolo original.
- Mostramos que devido aos parâmetros escolhidos nossa proposta **testará até 4.096 vezes menos** hipóteses de utilização da chave pública, durante a resolução da função G ;
- Constatamos que a substituição do SHA-1 pelo SHA-3 proporciona um **ganho de eficiência** de aproximadamente 75 % na inicialização dos vetores que serão utilizados pelos algoritmos de assinatura e verificação;
- Implementamos o Quartz (tanto em seu modelo original quanto aprimorado). Buscando comprovar sua **viabilidade em cenários “reais”** e contribuindo com as pesquisas realizadas na área de criptografia pós-quântica.

Trabalhos Futuros

- 
- Pesquisar uma maneira de reduzir o tamanho das chaves de nosso aprimoramento;
 - Buscar uma prova de segurança mais eficiente (*tight*) no modelo do oráculo aleatório para protocolos baseados na *trapdoor* HFE.



Obrigado!

Referências I

- [BBD09] Daniel J. Bernstein, Johannes Buchmann e Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer, 2009.
- [BERW08] Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp e Christopher Wolf. Time-area Optimized Public-key Engines: *MQ*-Cryptosystems as Replacement for Elliptic Curves? Em Elisabeth Oswald e Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, páginas 45–61. Springer Berlin Heidelberg, 2008.
- [BR11] Elaine Barker e Allen Roginsky. NIST Special Publication 800-131a - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. Relatório técnico, National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Washington DC. <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>, 2011. Último acesso em 09/07/2013.
- [CCC⁺09] AnnaInn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, EricLi-Hsiang Kuo, FrostYu-Shuang Lee e Bo-Yin Yang. SSE Implementation of Multivariate PKCs on Modern x86 CPUs. Em Christophe Clavier e Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, páginas 33–48. Springer Berlin Heidelberg, 2009.
- [CGP01] Nicolas T. Courtois, Louis Goubin e Jacques Patarin. Quartz, an asymmetric signature scheme for short signatures on PC. Primitive specification and supporting documentation (second revised version). 2001.
- [Cou04] Nicolas T. Courtois. Short signatures, provable security, generic attacks and computational security of multivariate polynomial schemes such as HFE, QUARTZ and SFLASH. Cryptology ePrint Archive, Report 2004/143. <http://eprint.iacr.org/2004/143>, 2004. Versão estendida e revista do artigo *Generic Attacks and the Security of Quartz* publicado no PKC 2003. Último acesso em 12/06/2013.

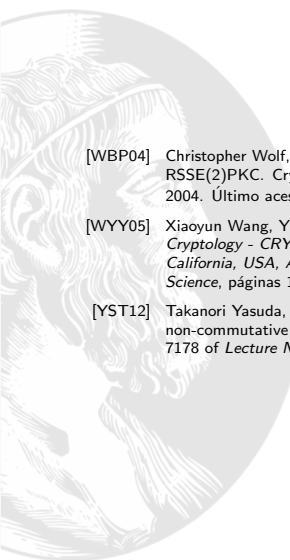
Referências II

- [Dan12] Quynh Dang. NIST Special Publication 800-107: Recommendation for Applications Using Approved Hash Algorithms. Relatório técnico, National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Washington DC.
<http://csrc.nist.gov/publications/nistpubs/800-107-rev1/sp800-107-rev1.pdf>, 2012.
Último acesso em 09/07/2013.
- [Deu85] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Ser. A*, A400:97–117, 1985.
- [DGS06] Jintai Ding, Jason E. Gower e Dieter Schmidt. *Multivariate public key cryptosystems*, volume 25 of *Advances in information security*. Springer, 2006.
- [DH76] Whitfield Diffie e Martin E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.
- [DWY07] Jintai Ding, Christopher Wolf e Bo-Yin Yang. ℓ -invertible cycles for Multivariate Quadratic (MQ) public key cryptography. Em Tatsuaki Okamoto e Xiaoyun Wang, editors, *Public Key Cryptography - PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, páginas 266–281. Springer Berlin Heidelberg, 2007.
- [Hei09] Raymond A. Heindl. *New Directions in Multivariate Public Key Cryptography*. Tese de Doutorado, Graduate School of Clemson University - Clemson, SC, 2009.
- [JM03] Antoine Joux e Gwenaëlle Martinet. Some weaknesses in Quartz Signature Scheme. NES/DOC/ENS/WP5/026/1. Relatório técnico, Janeiro 01 2003. Último acesso em 12/06/2013.
- [Jou04] Antoine Joux. Multicollisions in iterated hash functions. application to cascaded constructions. Em Matt Franklin, editor, *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, páginas 306–316. Springer Berlin Heidelberg, 2004.
- [KPG99] Aviad Kipnis, Jacques Patarin e Louis Goubin. Unbalanced Oil and Vinegar signature schemes. Em Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT 99*, volume 1592 of *Lecture Notes in Computer Science*, páginas 206–222. Springer Berlin Heidelberg, 1999.

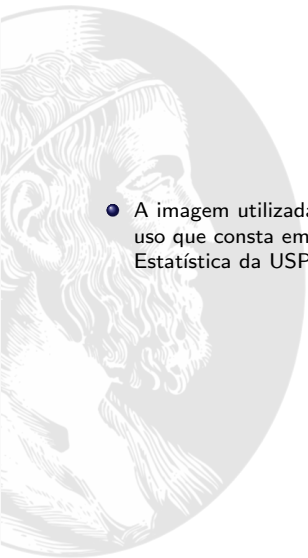
Referências III

- [MI88] Tsutomu Matsumoto e Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. Em *Lecture Notes in Computer Science on Advances in Cryptology - EUROCRYPT 88*, páginas 419–453, New York, NY, USA, 1988. Springer-Verlag New York, Inc.
- [NIS09] NIST. FIPS 186-3: Digital Signature Standard (DSS). Relatório técnico, National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Washington DC. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf, 2009. Último acesso em 16/07/2013.
- [Pat96] Jacques Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms. Em Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT 96*, volume 1070 of *Lecture Notes in Computer Science*, páginas 33–48. Springer-Verlag, 12–16 Maio 1996.
- [PBB10a] Albrecht Petzoldt, Stanislav Bulygin e Johannes Buchmann. CyclicRainbow – A Multivariate Signature Scheme with a Partially Cyclic Public Key. Em Guang Gong e KishanChand Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010*, volume 6498 of *Lecture Notes in Computer Science*, páginas 33–48. Springer Berlin Heidelberg, 2010.
- [PBB10b] Albrecht Petzoldt, Stanislav Bulygin e Johannes Buchmann. Selecting parameters for the Rainbow Signature Scheme. Em Nicolas Sendrier, editor, *Post-Quantum Cryptography*, volume 6061 of *Lecture Notes in Computer Science*, páginas 218–240. Springer Berlin Heidelberg, 2010.
- [PCG01] Jacques Patarin, Nicolas T. Courtois e Louis Goubin. QUARTZ, 128-bit Long Digital Signatures. Em David Naccache, editor, *Topics in Cryptology - CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, páginas 282–297. Springer Berlin Heidelberg, 2001.
- [PG97] Jacques Patarin e Louis Goubin. Trapdoor one-way permutations and Multivariate Polynomials - Extended Version. Em *Proc. of ICICS 97, LNCS 1334*, páginas 356–368. Springer, 1997.
- [Sho97] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

Referências IV

- 
- [WBP04] Christopher Wolf, An Braeken e Bart Preneel. Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC. Cryptology ePrint Archive, Report 2004/237. <http://eprint.iacr.org/2004/237>, 2004. Último acesso em 02/07/2013.
- [WYY05] Xiaoyun Wang, Yiqun Lisa Yin e Hongbo Yu. Finding collisions in the full SHA-1. Em *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, páginas 17–36. Springer, 2005.
- [YST12] Takanori Yasuda, Kouichi Sakurai e Tsuyoshi Takagi. Reducing the Key Size of Rainbow using non-commutative rings. Em Orr Dunkelman, editor, *Topics in Cryptology – CT-RSA 2012*, volume 7178 of *Lecture Notes in Computer Science*, páginas 68–83. Springer Berlin Heidelberg, 2012.

Créditos



- A imagem utilizada como plano de fundo em todos os slides segue a licença de uso que consta em <http://www.ime.usp.br> – © Instituto de Matemática e Estatística da USP.