

# Proposta de aprimoramento para o protocolo de assinatura digital Quartz

**Ewerton R. Andrade**

ewe@ime.usp.br

**Orientador: Routo Terada**

rt@ime.usp.br

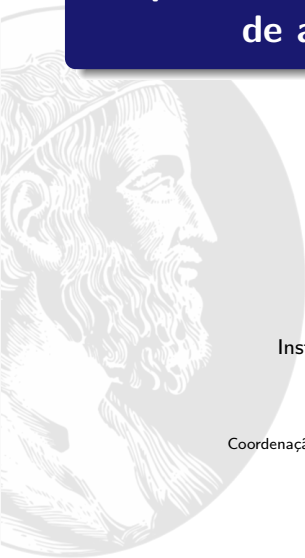
Instituto de Matemática e Estatística - IME  
Universidade de São Paulo - USP

*Agência de fomento:*

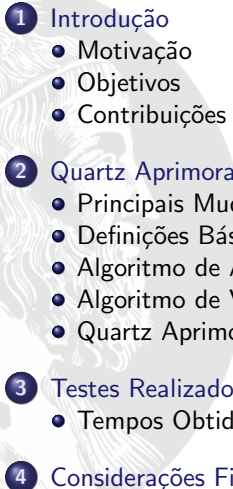
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES

Concurso de Teses e Dissertações

03 de novembro de 2014



# Agenda

- 
- 1 Introdução
    - Motivação
    - Objetivos
    - Contribuições
  - 2 Quartz Aprimorado
    - Principais Mudanças
    - Definições Básicas
    - Algoritmo de Assinatura
    - Algoritmo de Verificação
    - Quartz Aprimorado x Outros Protocolos
  - 3 Testes Realizados
    - Tempos Obtidos
  - 4 Considerações Finais

# Agenda

- 
- 1 Introdução
    - Motivação
    - Objetivos
    - Contribuições
  - 2 Quartz Aprimorado
    - Principais Mudanças
    - Definições Básicas
    - Algoritmo de Assinatura
    - Algoritmo de Verificação
    - Quartz Aprimorado x Outros Protocolos
  - 3 Testes Realizados
    - Tempos Obtidos
  - 4 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

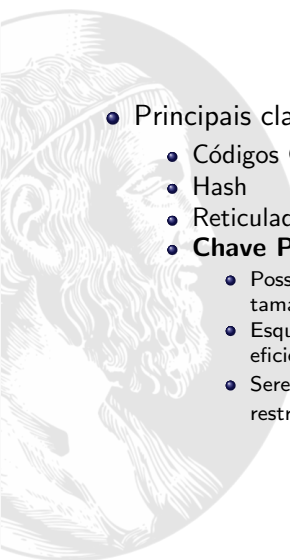
## Criptossistemas Clássicos (*Quânticos*)

- 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)

- 
- 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 [CCC<sup>+</sup>09];
      - Serem indicados como uma opção para sistemas embarcados com restrição de processamento [BBD09, 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 MQ** e IP (Isomorfismo de Polinômios);
- O problema MQ é **NP-completo** [PG97].



# Objetivos

Os objetivos principais deste trabalho são:

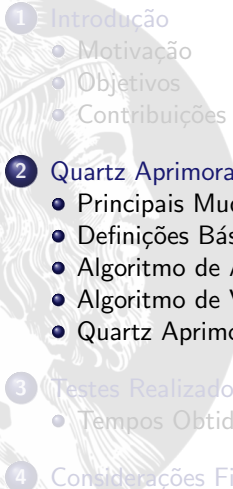
- **análise** do esquema de assinatura digital **Quartz**, proposto por Patarin, Courtois e Goubin, idealizado para gerar assinaturas extremamente curtas;
- a apresentação de um novo protocolo de assinatura digital **Quartz Aprimorado**, com foco no aumento da segurança;
- o desenvolvimento de uma **implementação 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.

# Agenda

- 
- 1 Introdução
    - Motivação
    - Objetivos
    - Contribuições
  - 2 Quartz Aprimorado
    - Principais Mudanças
    - Definições Básicas
    - Algoritmo de Assinatura
    - Algoritmo de Verificação
    - Quartz Aprimorado x Outros Protocolos
  - 3 Testes Realizados
    - Tempos Obtidos
  - 4 Considerações Finais

# Principais Mudanças

- Utilização de somente **uma transformação afim** no processo de assinatura das mensagens. Ou seja,  $\mathcal{P} = S \circ F$ ;
- **Substituição** do SHA-1 pelo SHA-3;
- **Concatenação** de um *salt*  $\Gamma$  à mensagem  $M$  antes de ser empregada a função de hash nesta mensagem.

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

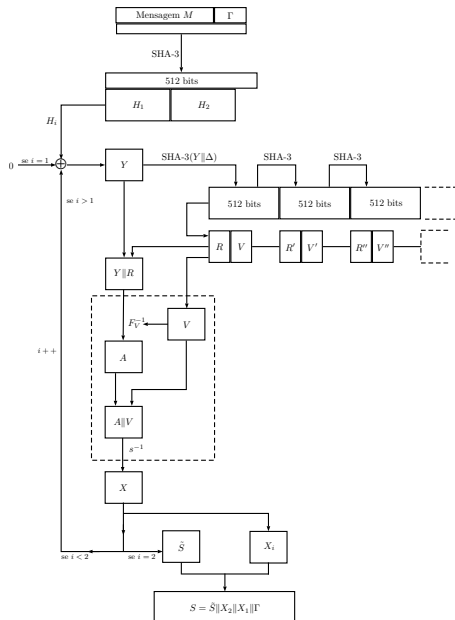
$$M_0 = \text{SHA-3}(M \parallel \Gamma).$$

- 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:

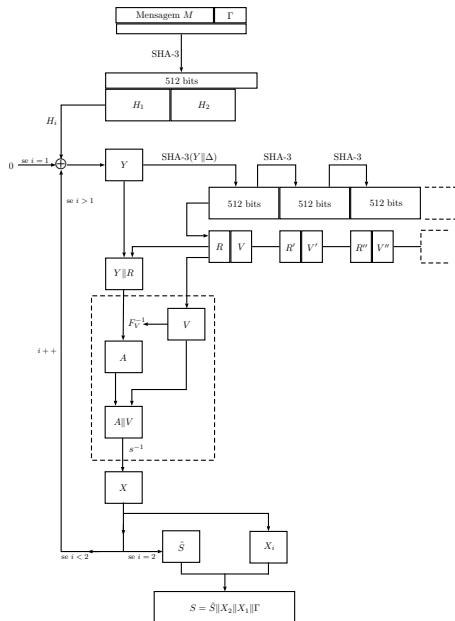
$$W = \text{SHA-3}(Y \parallel \Delta).$$

- 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:

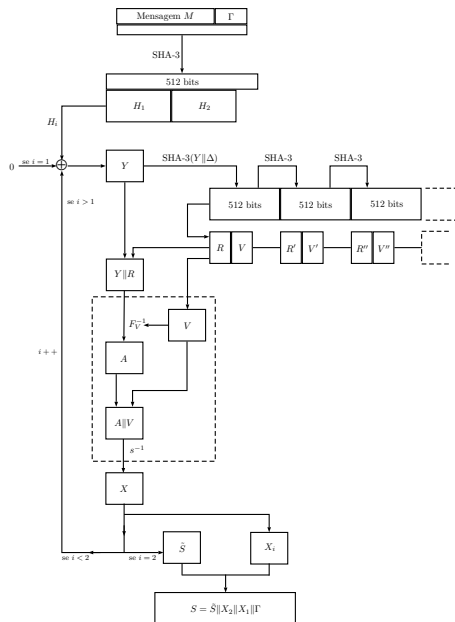
$$\tilde{S} = [X]_{0 \rightarrow 223}.$$

- 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:

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

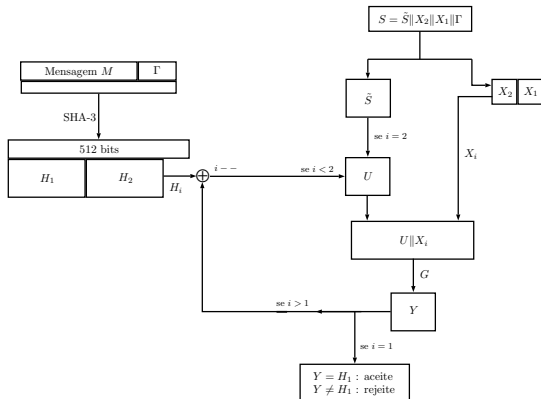
- Sejam  $X_2$  e  $X_1$  duas cadeias de 7 bits definidas por:

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

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

- Seja  $\Gamma$  uma cadeia de 96 bits definida por:

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



- Seja  $M_0$  uma cadeia de 512 bits definida por:

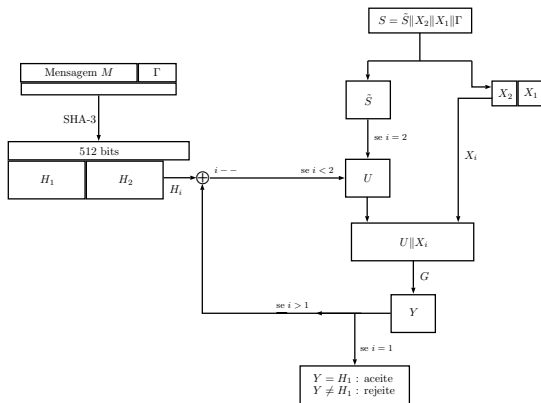
$$M_0 = \text{SHA-3}(M \parallel \Gamma).$$

- 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  $\tilde{S}$ .



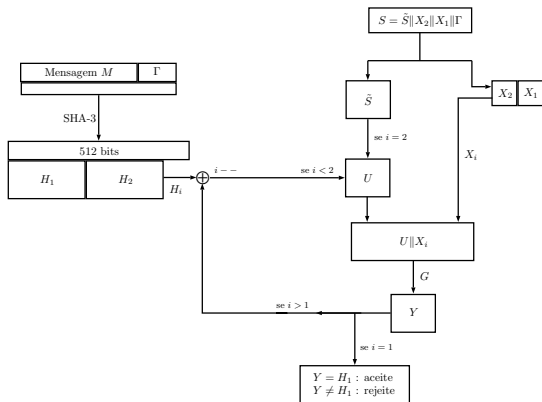
- Para  $i = 2$  até 1, faça:
  - Calcule a cadeia de 224 bits  $Y$  definida por:

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

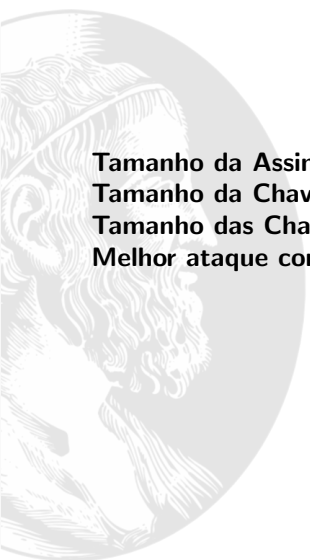
- Defina um novo valor para a cadeia de 224 bits  $U$  como sendo:

$$U = Y \oplus H_i.$$

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



# Quartz Aprimorado - Principais Características



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

# Quartz Aprimorado x Outros Protocolos

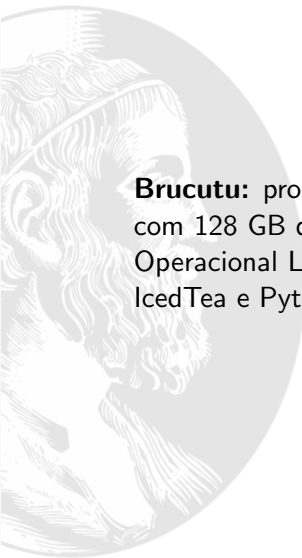
	<b>Criptossistema</b>	$q$	$d$	$m$	$n$	<b>Tamanho da Assinatura (em bits)</b>	<b>Ref.</b>
<i>Pós-Quântico</i>	CyclicUOV	256	256	77	77	624	[PBB10a]
	Rainbow	16	30	58	58	352	[PBB10b]
	NC-Rainbow	256	17	26	26	672	[YST12]
	CyclicRainbow	256	17	26	26	344	[PBB10a]
	Quartz Aprimorada	2	129	224	231	334	Nosso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

**Tabela :** Tamanho das assinaturas de alguns criptossistemas.

# Agenda

- 
- 1 Introdução
    - Motivação
    - Objetivos
    - Contribuições
  - 2 Quartz Aprimorado
    - Principais Mudanças
    - Definições Básicas
    - Algoritmo de Assinatura
    - Algoritmo de Verificação
    - Quartz Aprimorado x Outros Protocolos
  - 3 Testes Realizados
    - Tempos Obtidos
  - 4 Considerações Finais

# Computador Utilizado



**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.

# 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.



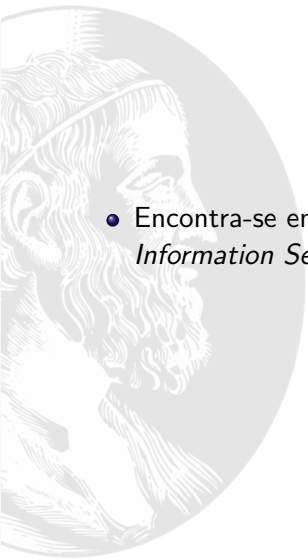
# Agenda

- 
- 1 Introdução
    - Motivação
    - Objetivos
    - Contribuições
  - 2 Quartz Aprimorado
    - Principais Mudanças
    - Definições Básicas
    - Algoritmo de Assinatura
    - Algoritmo de Verificação
    - Quartz Aprimorado x Outros Protocolos
  - 3 Testes Realizados
    - Tempos Obtidos
  - 4 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.

# Publicação



- Encontra-se em processo de **revisão** no *Brazilian Journal of Information Security and Cryptography* – ENIGMA.

# Trabalhos Futuros

Pensados durante a dissertação:

- 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.

# Trabalhos Futuros

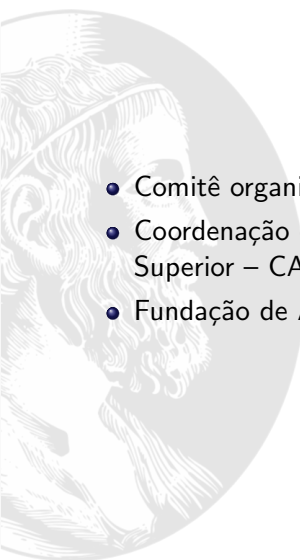
Pensados durante a dissertação:

- 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.

Idealizados mais recentemente:

- Utilizar **outras funções esponja** no lugar do SHA-3 (Keccak);
- Portar o código implementado para uma linguagem que permita uma melhor utilização dos conjuntos de **instruções avançadas** para tratamento de vetores (SIMD), nativas de processadores modernos.

# Agradecimentos

- 
- Comitê organizador do CTDSeg/SBSeg;
  - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES;
  - Fundação de Apoio à Universidade de São Paulo – FUSP.



Obrigado!

# Referências I

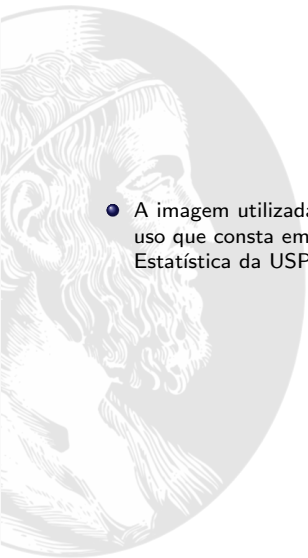
- [BBD09] Daniel J. Bernstein, Johannes Buchmann e Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer, 2009.
- [BR11] Elaine Barker e Allen Roginsky. NIST Special Publication 800-131a - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. Relatório 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<sup>+</sup>09] Annalnn-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 extendida e revista do artigo *Generic Attacks and the Security of Quartz* publicado no PKC 2003. Último acesso em 12/06/2013.
- [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.
- [DH76] Whitfield Diffie e Martin E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.
- [Hei09] Raymond A. Heindl. *New Directions in Multivariate Public Key Cryptography*. Tese de Doutorado, Graduate School of Clemson University - Clemson, SC, 2009.



# Referências II

- [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.
- [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](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.
- [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.