Implementação de protocolos de acordo de chave sem certificados digitais em dispositivos de poder computacional restrito

Rafael Will Macedo de Araujo
(rwill@ime.usp.br)

DCC – IME – USP

Março de 2013

CNPq no. 151134/2010-3

Objetivos

- Comparar protocolos de acordo de chave nos modelos baseado em identidade e sem certificado.
- Apresentar os resultados obtidos.

Roteiro

Curvas Elípticas sobre Corpos Finitos

- Seja $\mathbb{F}_q$ um corpo finito de ordem q, onde $q > 3$ é um número primo.
  - Como q é primo, então $\mathbb{F}_q$ coincide com $\mathbb{Z}_q$.
- Uma curva elíptica E sobre um corpo $\mathbb{F}_q$, representada por $E(\mathbb{F}_q)$ ou $E/\mathbb{F}_q$, é o conjunto dos pares $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ que satisfazem a equação:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

onde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$, com $\Delta \neq 0$.

Curvas Elípticas sobre Corpos Finitos

- Δ é o discriminante de $E(\mathbb{F}_q)$, e é definido como:

$$\begin{cases} \Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \\ d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1 a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \end{cases}$$

- O discriminante $\Delta \neq 0$ garante que não existirão duas ou mais retas tangentes distintas para um ponto na curva.
- Existe um ponto $\mathcal{O}$, dito ponto no infinito.

Operação sobre pontos em Curvas Elípticas

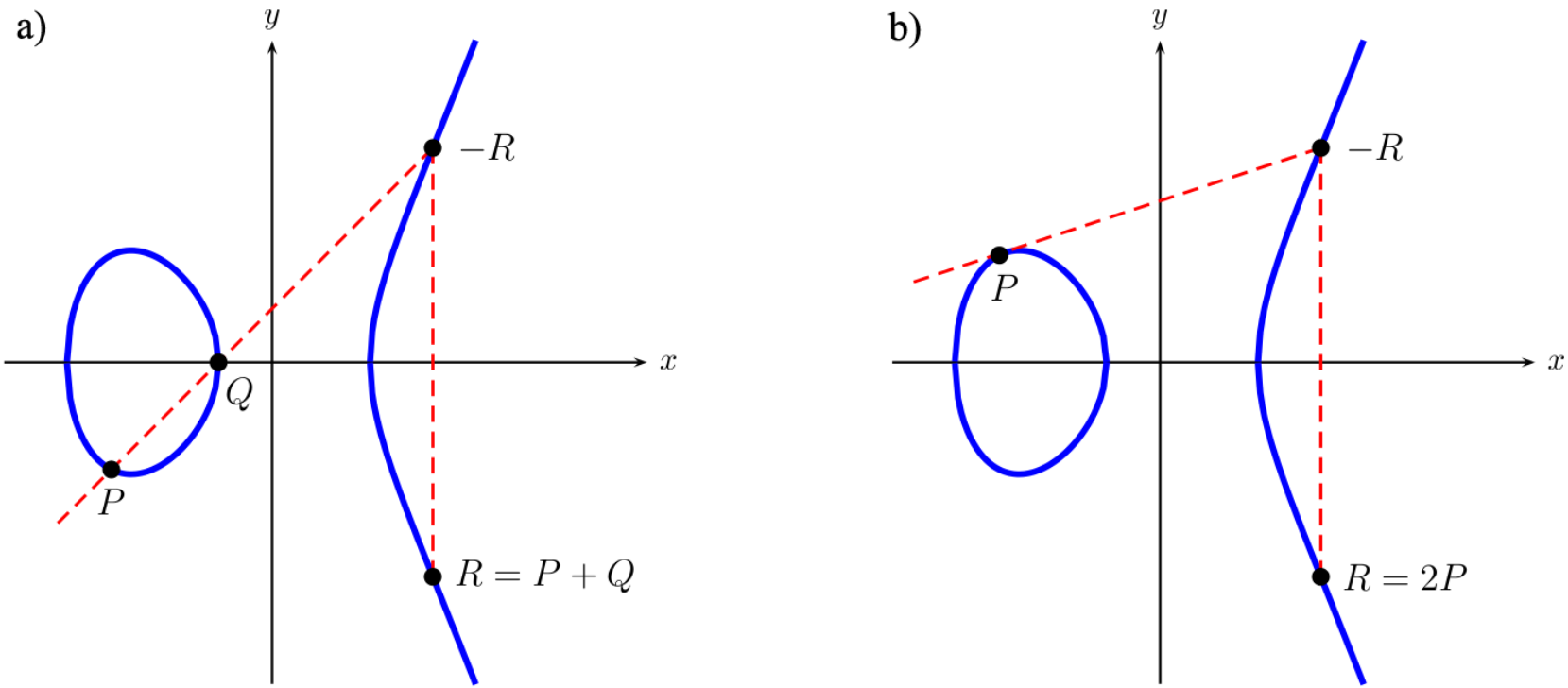


Figura: **a)** soma de dois pontos P e Q e **b)** dobramento de um ponto P em $E(\mathbb{F}_q)$

Emparelhamento Bilinear

Definição

- Mapeamento: $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Propriedades

- **Bilinear**: Para quaisquer $P, Q, R \in \mathbb{G}_1$ ou $\mathbb{G}_2$, e $a, b \in \mathbb{Z}_q$ tem-se:
  - $e(P + Q, R) = e(P, R).e(Q, R)$.
  - $e(P, Q + R) = e(P, Q).e(P, R)$.
  - $e(aQ, bQ) = e(Q, Q)^{ab} = e(abQ, Q) = e(Q, abQ)$.
- **Não-degenerado**: não mapeia todos os pares $\mathbb{G}_1 \times \mathbb{G}_2$ para o elemento identidade de $\mathbb{G}_T$.
- **Ser computável**: $\forall(P, Q), \exists R \rightarrow R \equiv e(P, Q)$.
  - Isto é, existe algoritmo **eficiente** (i.e., de tempo polinomial) para calcular $e(P, Q)$.

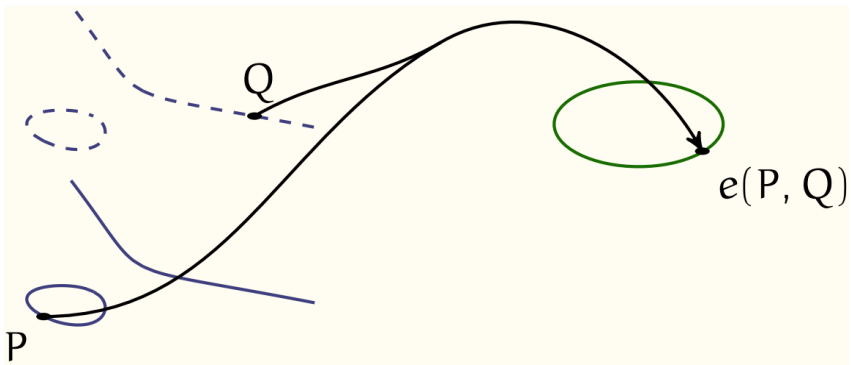


Figura: Emparelhamento bilinear [Cesena, 2010]

Emparelhamento Bilinear

Definição

- Mapeamento: $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Propriedades

- **Bilinear**: Para quaisquer $P, Q, R \in \mathbb{G}_1$ ou $\mathbb{G}_2$, e $a, b \in \mathbb{Z}_q$ tem-se:
  - $e(P + Q, R) = e(P, R).e(Q, R)$.
  - $e(P, Q + R) = e(P, Q).e(P, R)$.
  - $e(aQ, bQ) = e(Q, Q)^{ab} = e(abQ, Q) = e(Q, abQ)$.
- **Não-degenerado**: não mapeia todos os pares $\mathbb{G}_1 \times \mathbb{G}_2$ para o elemento identidade de $\mathbb{G}_T$.
- **Ser computável**: $\forall(P, Q), \exists R \rightarrow R \equiv e(P, Q)$.
  - Isto é, existe algoritmo **eficiente** (i.e., de tempo polinomial) para calcular $e(P, Q)$.

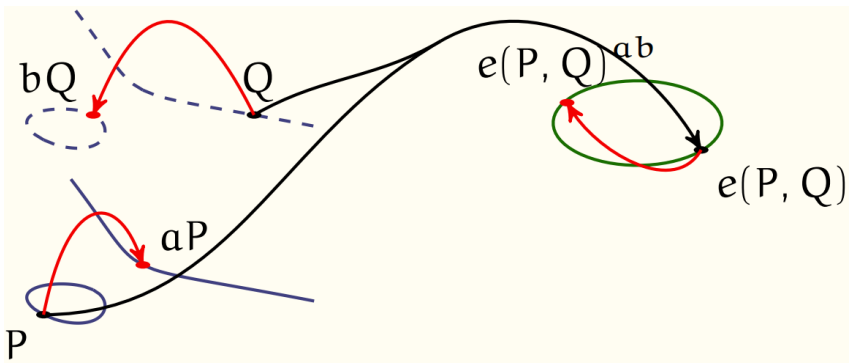


Figura: Emparelhamento bilinear [Cesena, 2010]

Tipos de Emparelhamentos Bilineares

- No trabalho de [Galbraith *et al*, 2006], são apresentados três tipos de emparelhamentos:
  - **Tipo 1**: $\mathbb{G}_1 = \mathbb{G}_2$, (emparelhamento simétrico).
  - **Tipo 2**: $\mathbb{G}_1 \neq \mathbb{G}_2$, e existe um isomorfismo eficientemente computável: $\phi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$.
  - **Tipo 3**: $\mathbb{G}_1 \neq \mathbb{G}_2$, contudo não existe isomorfismo que seja eficientemente computável entre $\mathbb{G}_1$ e $\mathbb{G}_2$.

Tipos de Emparelhamentos Bilineares

- No trabalho de [Galbraith *et al*, 2006], são apresentados três tipos de emparelhamentos:
  - **Tipo 1**: $\mathbb{G}_1 = \mathbb{G}_2$, (emparelhamento simétrico).
    - Existe algoritmo de *hash* eficiente que mapeia cadeias de *bits* aleatórias em $\mathbb{G}_1$.
  - **Tipo 2**: $\mathbb{G}_1 \neq \mathbb{G}_2$, e existe um isomorfismo eficientemente computável: $\phi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$.
    - Não existe algoritmo de *hash* eficiente que mapeia cadeias de *bits* aleatórias em $\mathbb{G}_2$.
  - **Tipo 3**: $\mathbb{G}_1 \neq \mathbb{G}_2$, contudo não existe isomorfismo que seja eficientemente computável entre $\mathbb{G}_1$ e $\mathbb{G}_2$.
    - Existe algoritmo de *hash* "eficiente" que mapeia cadeias de *bits* aleatórias em $\mathbb{G}_2$.

Problemas Computacionais de Interesse

Problema do logaritmo discreto

Dados P e $R \in E(\mathbb{F}_q)$, P gerador de $E(\mathbb{F}_q)$, encontrar $s \in \mathbb{Z}_q$ tal que:

$$R = sP$$

OBS: Note que $sP = \underbrace{P + P + \cdots + P}_{s \text{ vezes}}$.

Problemas *Diffie-Hellman* (DHP)

Considere $P \in \mathbb{G}$ (aditivo) e $a, b, c \in \mathbb{Z}_q$:

- **DDHP** (*Decision*-DHP): dados: $P, aP, bP, cP \in \mathbb{G}$; decidir: $abP = cP$.
- **CDHP** (*Computacional*-DHP): dados: $P, aP, bP \in \mathbb{G}$; encontrar: abP.
- **GDHP** (*Gap*-DHP): dados: $P, aP, bP \in \mathbb{G}$; encontrar: abP, com ajuda de um oráculo de decisão (que dados $aP, bP, cP \in \mathbb{G}$, decide se $abP = cP$).
- **BDHP** (*Bilinear*-DHP): dados: $P, aP, bP, cP \in \mathbb{G}$; encontrar: $e(P, P)^{abc}$.

Comprimento Mínimo das Chaves

Segurança (bits)	Algoritmo simétrico	RSA	ECC	Razão de crescimento
80	Skipjack	1024	160	$\approx 1 : 6$
112	3DES	2048	224	$\approx 1 : 9$
128	AES-128	3072	256	$1 : 12$
192	AES-192	7680	384	$1 : 20$
256	AES-256	15360	512	$1 : 30$

Roteiro

Modelo Baseado em Identidade (*ID-Based*)

- Modelo proposto em 1984 por A. Shamir.
  - Somente em 2001 foram publicados esquemas de criptografia (*encryption*) no modelo baseado em identidades [Boneh & Franklin, 2001] e [Cocks, 2001].
- A chave pública deixa de ser um valor gerado aleatoriamente, e passa ser a própria **identidade do usuário**.
- Pressupõe a existência de um **Gerador de Chaves Privadas** (PKG - *Private Key Generator*). Trata-se de uma **Autoridade de Confiança**, responsável por:
  - Gerar e guardar a chave-mestra secreta do sistema.
  - Calcular as chaves secretas de todos os usuários.
  - Entregar as chaves secretas dos usuários de forma segura (com sigilo e autenticidade).

Modelo Baseado em Identidade (*ID-Based*)

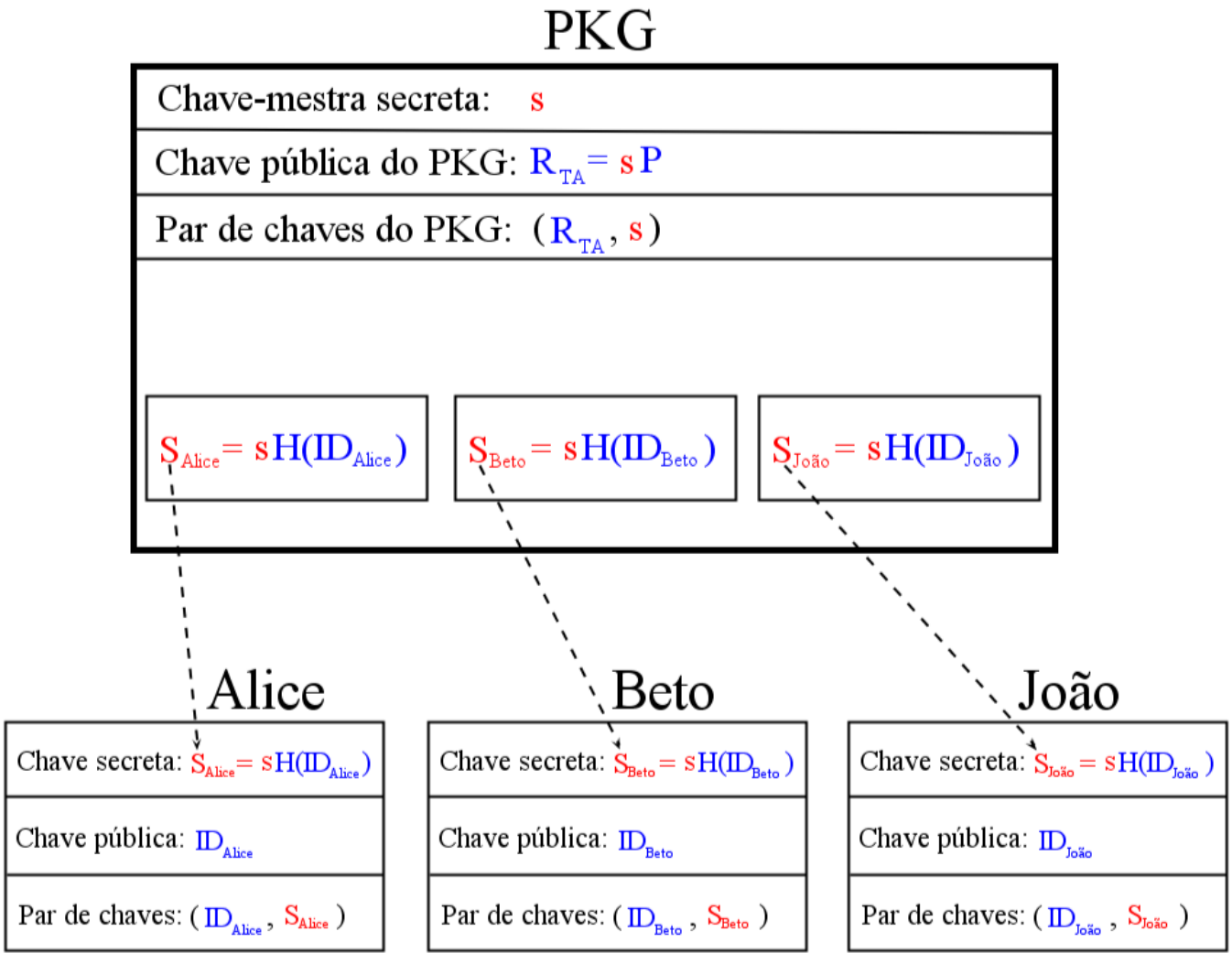


Figura: Diagrama do modelo baseado em identidade

Modelo Baseado em Identidade (*ID-Based*)

Algumas vantagens

- Chave pública de fácil memorização.
- Certificação implícita.
- Infraestrutura simples.

Algumas desvantagens

- Alta criticidade da chave-mestra secreta.
- Custódia de chaves.
- Não há irretratabilidade (o PKG pode personificar qualquer usuário).

Modelo sem Certificado (*Certificateless*)

- Modelo proposto em 2003 por S. Al-Riyami e K. Paterson.
  - Modelo intermediário entre o baseado em identidade e a ICP.
- Elimina a propriedade de custódia de chaves, inerente ao modelo baseado em identidade.
- Pressupõe a existência de um **Centro Gerador de Chaves** (KGC - *Key Generator Center*), responsável por:
  - Gerar e guardar a chave-mestra secreta do sistema.
  - Calcular as chaves secretas *parciais* de todos os usuários.
  - Entregar as chaves secretas parciais dos usuários de forma segura (com sigilo e autenticidade).

Modelo sem Certificado (*Certificateless*)

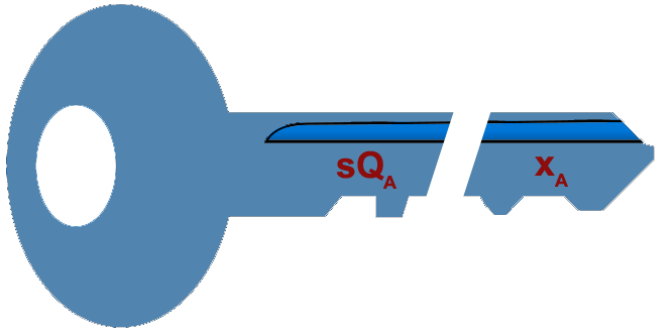


Figura: Chaves secretas parciais

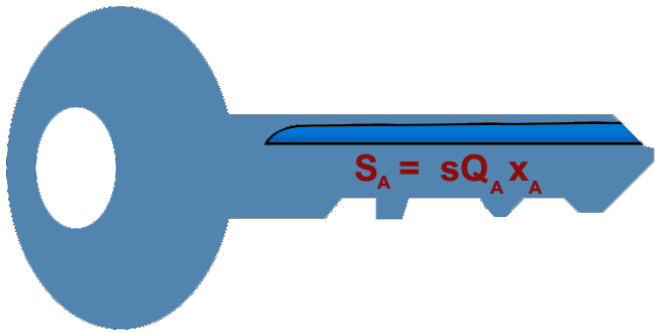


Figura: Chave secreta completa

Modelo sem Certificado (*Certificateless*)

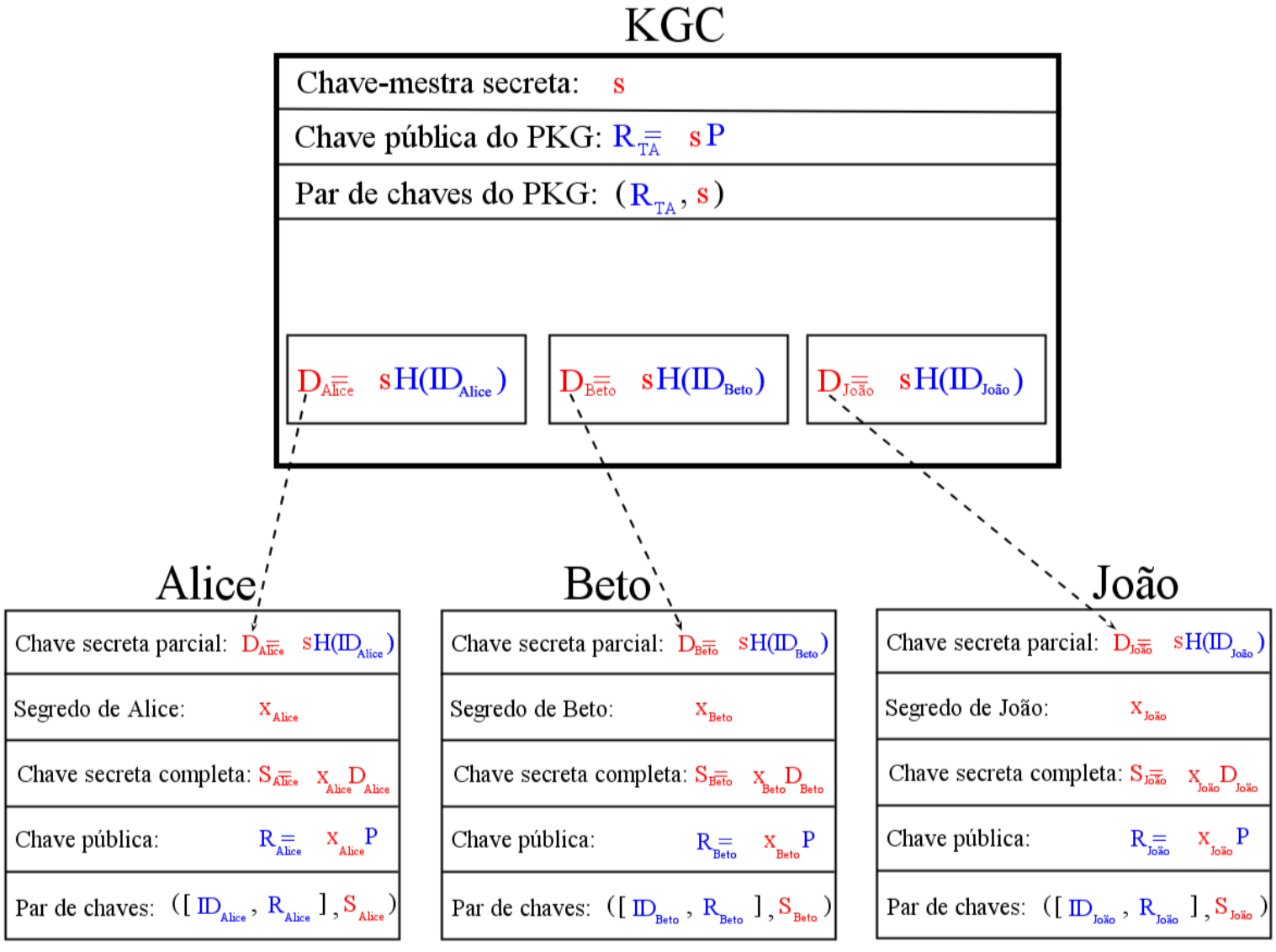


Figura: Diagrama do modelo sem certificado

Modelo sem Certificado (*Certificateless*)

Algumas vantagens

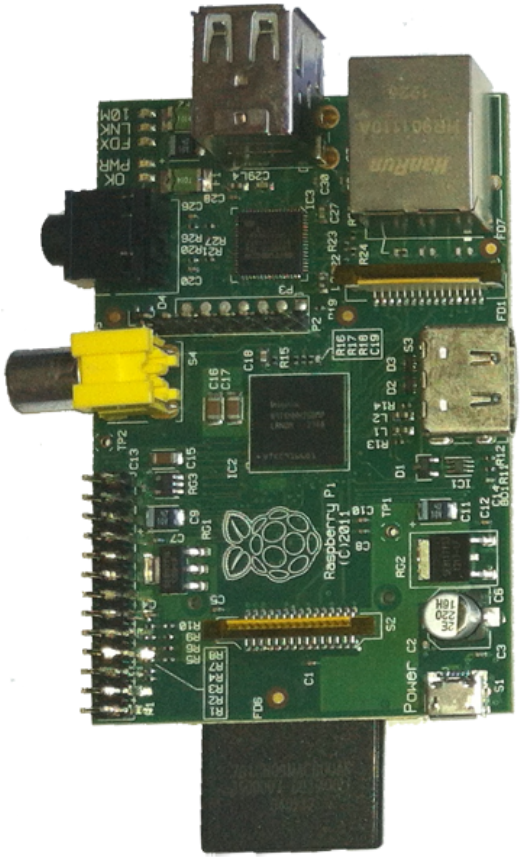
- Elimina a custódia de chaves.
- Menor criticidade da chave mestra.
- Controle do usuário sobre a renovação de chaves.
- Certificação implícita.

Algumas desvantagens

- Requer um repositório ou alguma outra forma de distribuição de chaves públicas.
- Possibilidade de substituição da chave pública por algum mal intencionado (dificuldade em verificar a legitimidade da chave pública).
- Vulnerabilidade ao ataque DoD (*Denial of Decryption*). A substituição de uma chave pública impede que a mensagem seja decifrada.

Roteiro

Hardware utilizado



Raspberry Pi

Motorola Milestone

Hardware utilizado

- **Servidor (KGC)**:
  - Processador: Intel Core 2 Duo T5800, 2.0 GHz
  - Memória RAM: 3 GB, DDR2, 800 MHz
  - Conexão de rede: 100 Mbps, por cabo
  - Sistema operacional: Ubuntu 12.04 LTS, 32 bits
- **Raspberry Pi**:
  - Processador: Broadcom BCM2835 (intruções ARMv6, *single core*), 700 MHz
  - Memória RAM: 256 MB, LPDDR2
  - Conexão de rede: 100 Mbps, por cabo
  - Sistema operacional: Debian "Wheezy" (armhf)
- **Smartphone**:
  - Modelo: Motorola Milestone
  - Processador: Cortex-A8 (intruções ARMv7, *single core*), 600 MHz
  - Memória RAM: 256 MB, LPDDR
  - Conexão de rede: 54 Mbps, *Wi-Fi* (IEEE 802.11g)
  - Sistema operacional: Android 2.2
- **Roteador Wi-Fi**:
  - Modelo: D-Link DIR-300
  - Conexão de rede: 4x 100 Mbps (LAN), 54 Mbps (WLAN)

Comunicação

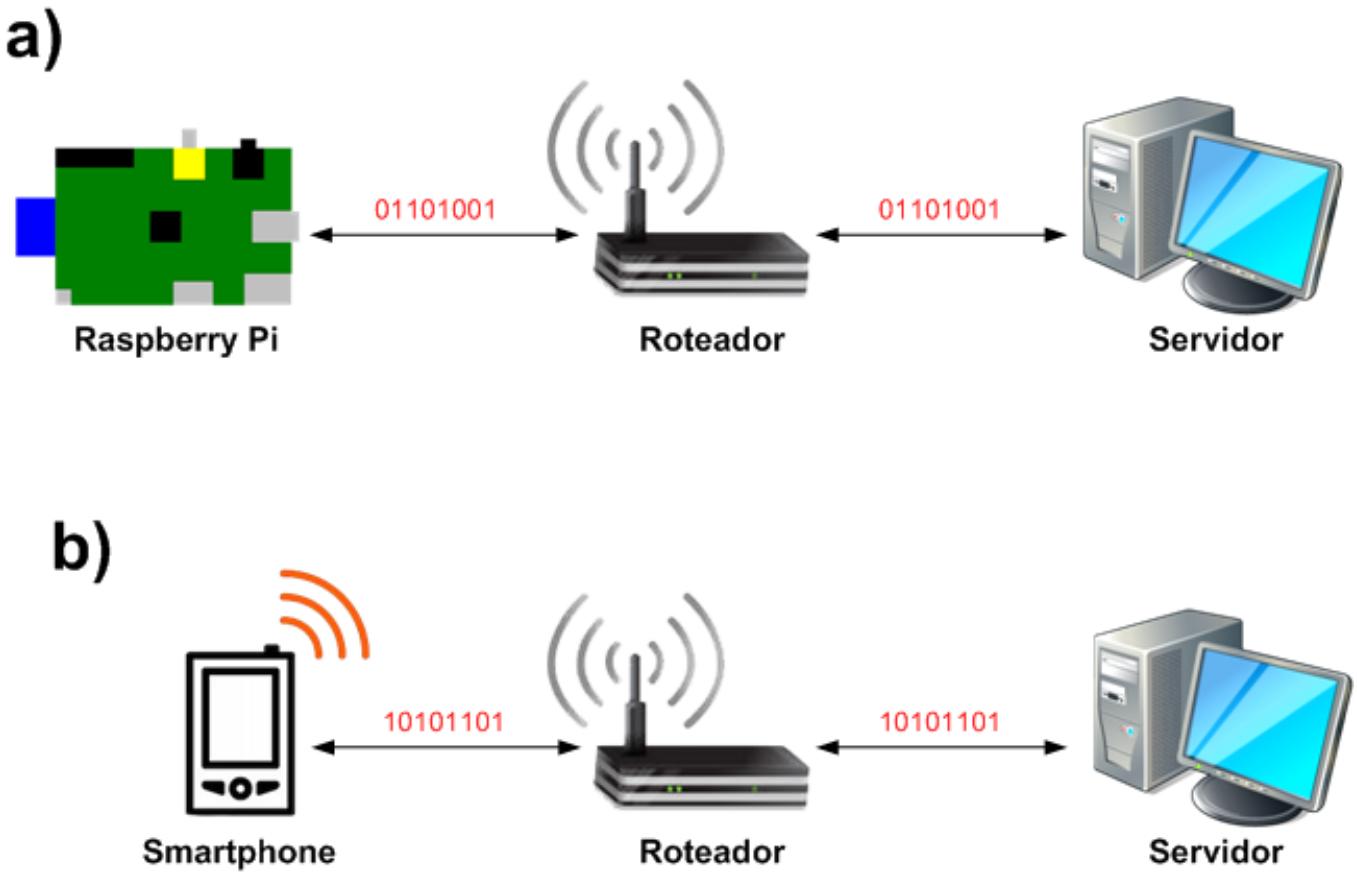


Figura: Comunicação entre o servidor e os dispositivos: **a)** Raspberry Pi (ARMv6) e **b)** Motorola Milestone (ARMv7)

Biblioteca criptográfica *Relic-toolkit*

- Escrita principalmente em linguagem de programação C.
- Suporte para várias arquiteturas de processadores: x86, x86-64, ARM, AVR, MSP.
- Operações sobre números inteiros de precisão arbitrária, corpos finitos, curvas elípticas, emparelhamentos bilineares.
- Outras opções: processamento paralelo (ambientes *multi-core*), diferentes geradores de números pseudoaleatórios, diferentes *timers* (CYCLE, ANSI/POSIX *compatible*, *per-thread*, *per-process*, *realtime*), possibilidade de uso da biblioteca GMP como backend aritmético, diferentes sistemas operacionais, etc.

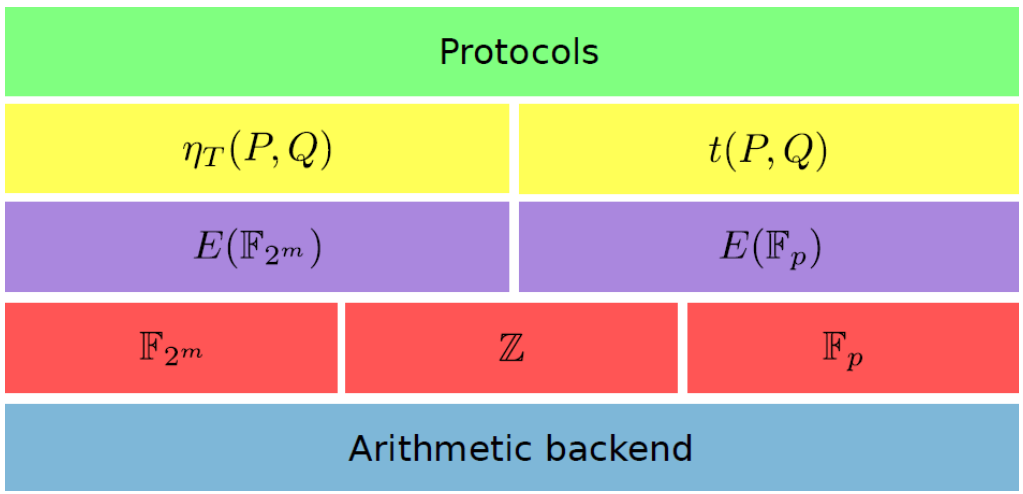


Figura: Esrutura da *Relic-toolkit* [Aranha, 2012]

Curvas Elípticas e Emparelhamentos na *Relic-toolkit*

- **Curvas binárias**
  - ETAT_T271: 70 bits
  - ETAT_S353: 80 bits
  - ETAT_S1223: 128 bits
  - Emparelhamento: ηT

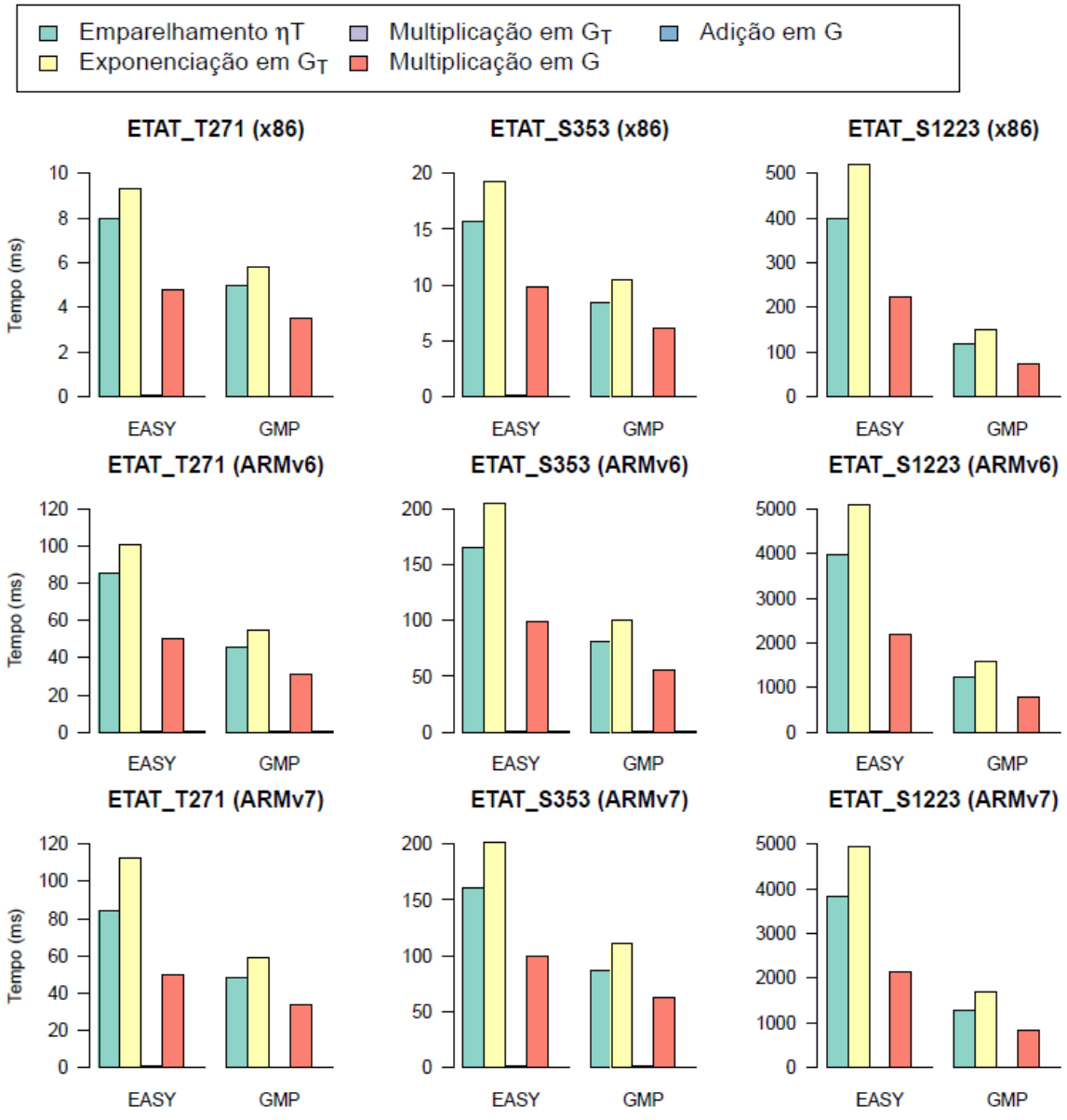
- **Curvas primas**
  - BN_P158: 80 bits
  - BN_P254: 126 bits
  - BN_P256: 128 bits
  - BN_P638: 192 bits
  - Emparelhamento: O-Ate

Operações em Curvas Binárias

	ETAT_T271			ETAT_S353			ETAT_S1223		
Backend EASY	**x86**	**ARMv6**	**ARMv7**	**x86**	**ARMv6**	**ARMv7**	**x86**	**ARMv6**	**ARMv7**
Emparelhamento	8.0	85.4	84.4	15.7	165.7	160.3	398.9	3972.0	3839.0
Exponenciação em $\mathbb{G}_T$	9.3	100.6	112.6	19.3	205.2	200.9	518.2	5099.9	4948.5
Multiplicação em $\mathbb{G}_T$	0.07	0.7	0.6	0.1	1.1	1.0	0.8	8.1	7.8
Multiplicação em $\mathbb{G}$	4.8	50.1	49.6	9.9	99.2	99.3	222.3	2198.1	2124.8
Adição em $\mathbb{G}$	0.04	0.4	0.4	0.06	0.7	0.6	0.5	4.6	3.9
Backend GMP									
Emparelhamento	5.0	46.0	48.6	8.4	80.7	86.3	117.7	1228.5	1289.4
Exponenciação em $\mathbb{G}_T$	5.8	54.6	58.7	10.5	100.0	111.4	150.4	1590.3	1679.9
Multiplicação em $\mathbb{G}_T$	0.04	0.4	0.4	0.06	0.5	1.3	0.2	2.4	2.3
Multiplicação em $\mathbb{G}$	3.5	31.4	33.8	6.1	56.2	62.4	75.4	785.3	821.5
Adição em $\mathbb{G}$	0.03	0.2	0.2	0.03	0.3	0.3	0.1	1.4	2.2

- Média de 20 rodadas.

Operações em Curvas Binárias

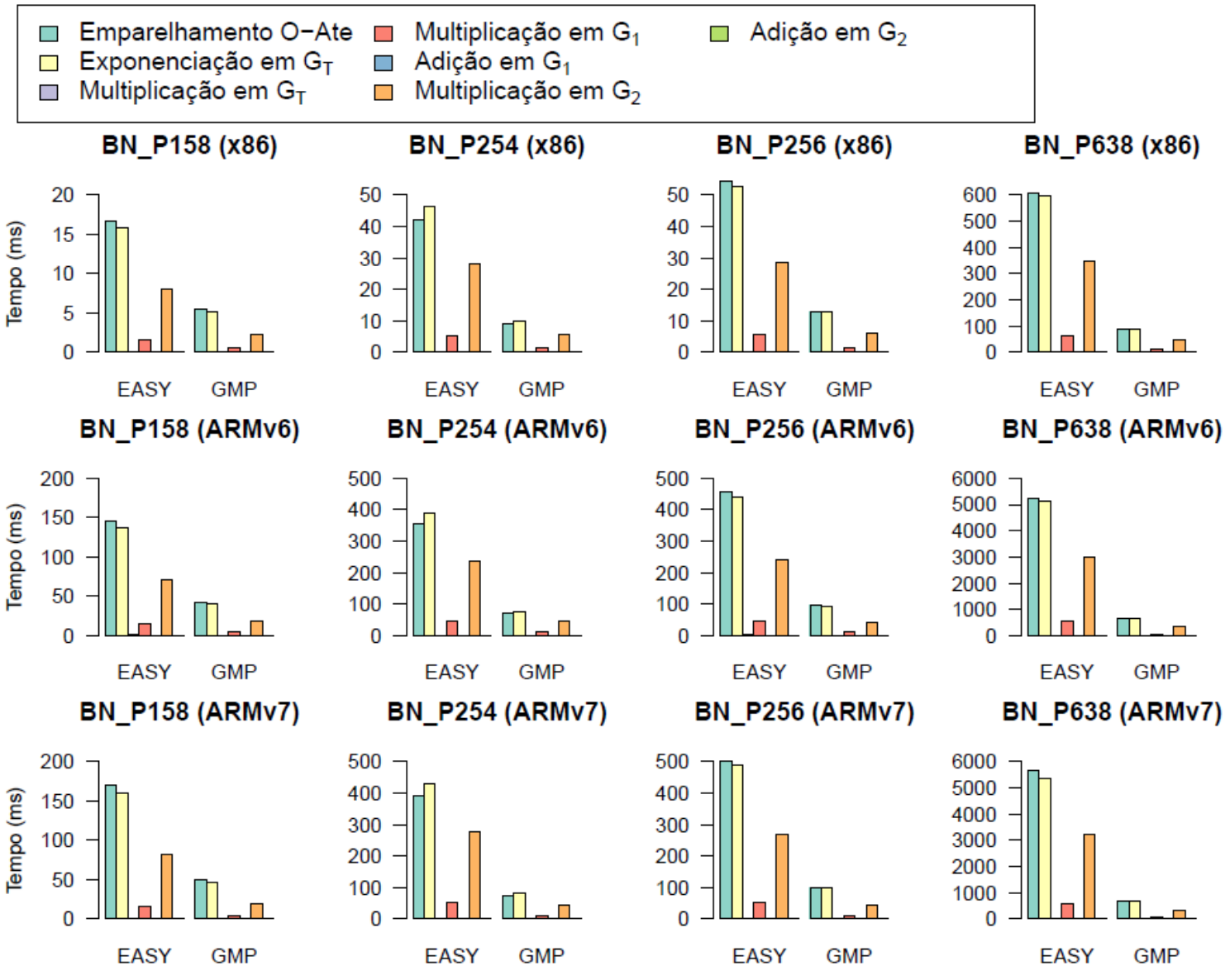


Operações em Curvas Primas

	BN_P158			BN_P254			BN_P256			BN_P638		
EASY	**x86**	**ARMv6**	**ARMv7**	**x86**	**ARMv6**	**ARMv7**	**x86**	**ARMv6**	**ARMv7**	**x86**	**ARMv6**	**ARMv7**
Emp.	16.7	145.9	169.7	42.1	353.8	389.3	54.3	457.5	501.7	605.1	5221.3	5674.6
Exp. $\mathbb{G}_T$	15.8	137.3	160.7	46.4	387.7	429.4	52.7	441.1	487.2	595.1	5118.8	5364.1
Mul. $\mathbb{G}_T$	0.1	1.0	1.0	0.2	1.7	1.6	0.2	1.9	3.0	1.0	8.7	9.5
Mul. $\mathbb{G}_1$	1.6	14.7	15.9	5.4	46.2	53.0	5.5	46.4	51.8	65.0	548.1	602.3
Ad. $\mathbb{G}_1$	0.01	0.1	0.1	0.02	0.2	0.2	0.02	0.2	0.2	0.1	0.9	0.9
Mul. $\mathbb{G}_2$	8.1	70.8	82.6	28.2	238.9	278.5	28.5	241.0	267.7	345.7	3008.9	3208.2
Ad. $\mathbb{G}_2$	0.03	0.3	0.2	0.1	0.5	0.5	0.1	0.5	0.5	0.3	2.3	2.3
GMP												
Emp.	5.5	42.5	50.1	9.0	71.3	74.7	13.1	96.0	100.3	89.1	637.5	685.5
Exp. $\mathbb{G}_T$	5.2	40.0	46.7	9.9	77.8	80.9	12.8	94.1	98.7	88.2	634.2	671.6
Mul. $\mathbb{G}_T$	0.04	0.3	0.3	0.04	0.31	0.3	0.1	0.4	0.4	0.1	1.0	1.0
Mul. $\mathbb{G}_1$	0.6	4.6	4.7	1.3	11.5	10.9	1.4	10.5	10.3	9.9	71.9	80.9
Ad. $\mathbb{G}_1$	0.005	0.03	0.03	0.01	0.05	0.05	0.01	0.05	0.06	0.02	0.13	0.12
Mul. $\mathbb{G}_2$	2.3	17.8	19.6	5.7	45.5	45.4	6.2	42.8	46.1	47.7	332.5	352.4
Ad. $\mathbb{G}_2$	0.01	0.1	0.1	0.01	0.11	0.1	0.01	0.11	0.1	0.04	0.28	0.28

- Média de 20 rodadas.

Operações em Curvas Primas



Roteiro

Protocolos Estudados

- **ID-Based**:
  - HC: Huang, Cao. 2009
  - LCNH: Li, Chen, Ni, Hao. 2011

- **Certificateless**:
  - LBG: Lippold, Boyd, Gonzalez Nieto. 2009
  - GOT: Goya, Okida, Terada. 2010
  - GNT: Goya, Nakamura, Terada. 2011

Operações (sem pré-computação)

	Quantidade de Operações				
Protocolo	**Emparelhamento**	**Exponenciação $\mathbb{G}_T$**	**Multiplicação em $\mathbb{G}_T$**	**Multiplicação em $\mathbb{G}$**	**Adição em $\mathbb{G}$**
HC	2	0	0	2	4
LCNH	6	2	2	1	0
LCNH-Gap	3	1	1	1	0
LBG	10	4	4	4	0
LBG-Gap	5	2	2	4	0
GOT	8	2	2	5	4
GOT-Gap	4	1	1	5	2
GNT	4	0	1	6	4

Operações (com pré-computação)

	Quantidade de Operações				
Protocolo	**Emparelhamento**	**Exponenciação $\mathbb{G}_T$**	**Multiplicação em $\mathbb{G}_T$**	**Multiplicação em $\mathbb{G}$**	**Adição em $\mathbb{G}$**
HC	2	0	0	2	4
LCNH	2	2	2	1	0
LCNH-Gap	1	1	1	1	0
LBG	4	2	2	3	0
LBG-Gap	2	1	1	3	0
GOT	2	0	0	4	4
GOT-Gap	1	0	0	4	2
GNT	2	0	0	4	4

Tempos sem pré-computação (*ID-Based*)

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
HC	184	328	116	185	239
LCNH	442	793	385	680	828
LCNH-Gap	252	452	197	329	432

Tabela: Tempos (em milisegundos) de execução no *Raspberry Pi*

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
HC	206	360	115	180	270
LCNH	470	862	435	555	929
LCNH-Gap	249	486	226	326	473

Tabela: Tempos (em milisegundos) de execução no *Smartphone*

Tempos com pré-computação (*ID-Based*)

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
HC*	184	328	116	185	239
LCNH	260	478	198	360	424
LCNH-Gap	161	293	104	179	227

Tabela: Tempos (em milisegundos) de execução no *Raspberry Pi*

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
HC*	206	360	115	180	270
LCNH	288	474	221	299	478
LCNH-Gap	178	318	122	186	243

Tabela: Tempos (em milisegundos) de execução no *Smartphone*

* O protocolo HC não possui valores que possam ser pré-computados.

Tempos sem pré-computação (*Certificateless*)

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
LBG	841	1497	691	1090	1443
LBG-Gap	495	890	339	549	746
GOT	662	1182	490	760	1032
GOT-Gap	426	760	285	403	587
GNT	409	720	224	346	472

Tabela: Tempos (em milisegundos) de execução no *Raspberry Pi*

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
LBG	872	1574	765	1163	1630
LBG-Gap	508	964	417	610	857
GOT	698	1241	557	850	1201
GOT-Gap	478	799	306	437	592
GNT	445	791	229	400	517

Tabela: Tempos (em milisegundos) de execução no *Smartphone*

Tempos com pré-computação (*Certificateless*)

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
LBG	418	744	307	489	636
LBG-Gap	270	483	155	255	339
GOT	248	440	118	191	251
GOT-Gap	203	359	77	120	161
GNT	252	444	120	190	252

Tabela: Tempos (em milisegundos) de execução no *Raspberry Pi*

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
LBG	449	812	343	493	730
LBG-Gap	296	541	202	291	361
GOT	268	494	149	222	305
GOT-Gap	229	406	94	149	166
GNT	279	488	148	226	297

Tabela: Tempos (em milisegundos) de execução no *Smartphone*

Gráfico (tempos com pré-computação)

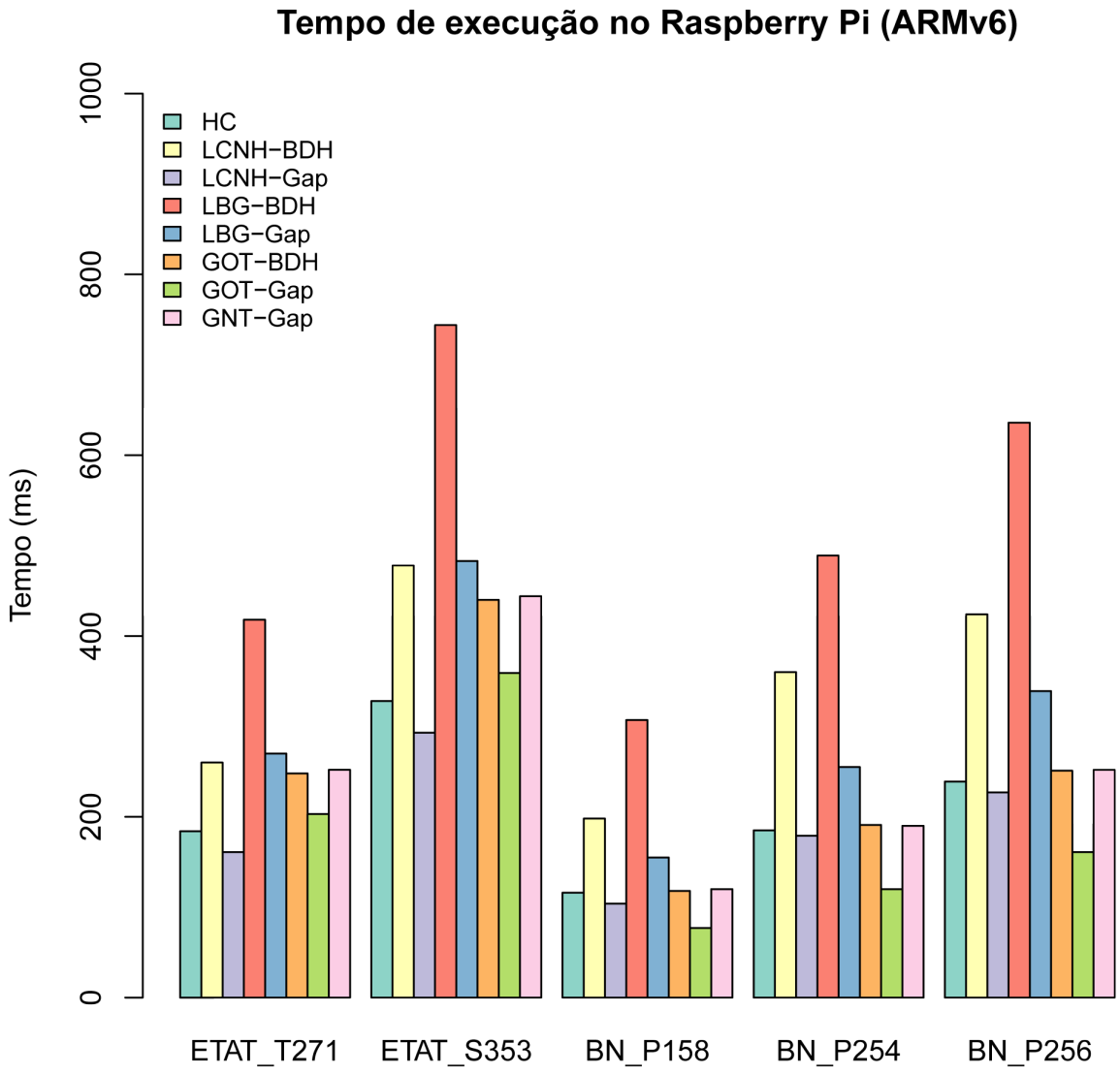
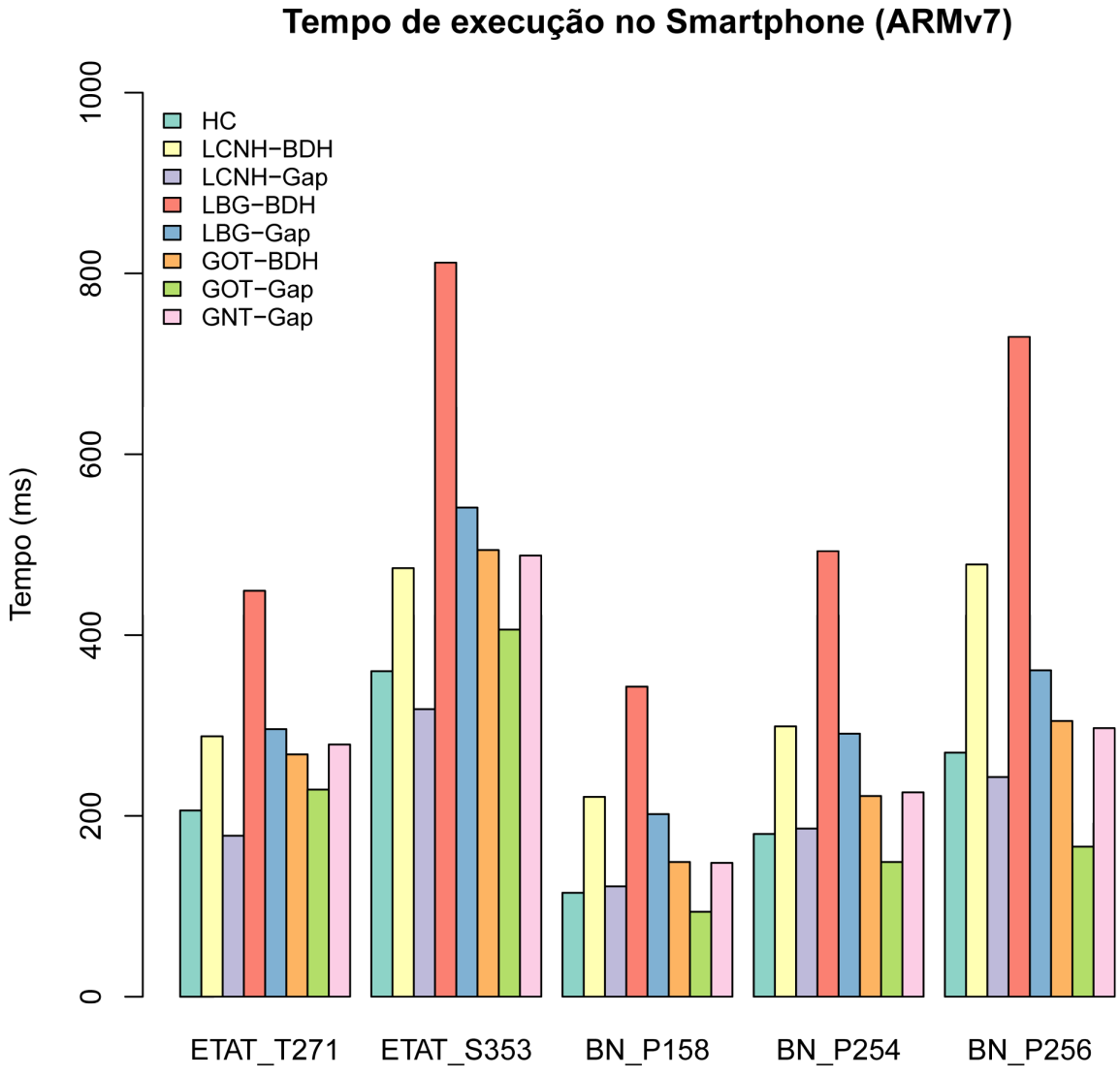


Gráfico (tempos com pré-computação)

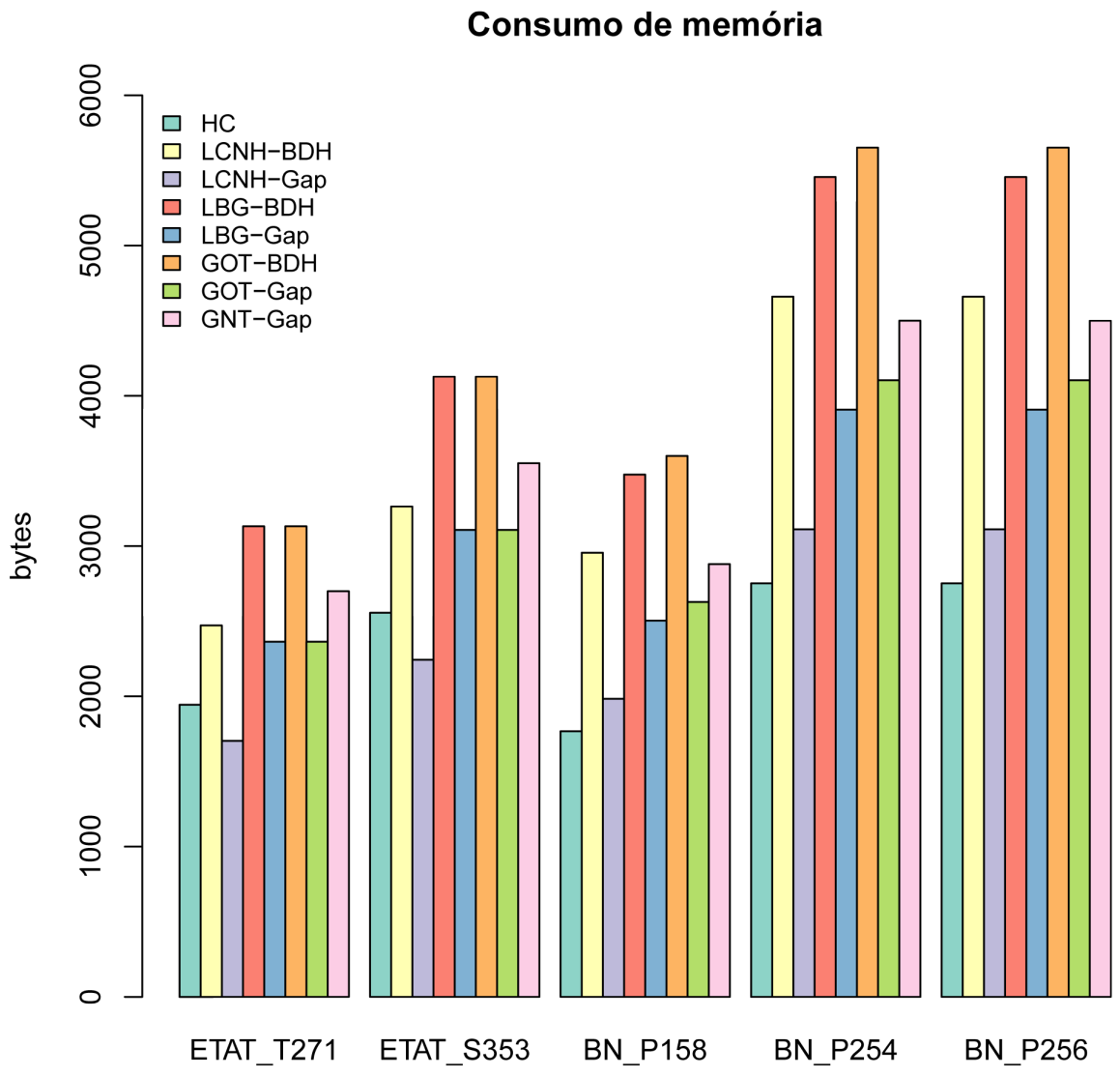


Uso de Memória

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
HC	1944	2556	1768	2752	2752
LCNH	2472	3264	2956	4660	4660
LCNH-Gap	1704	2244	1984	3112	3112
LBG	3132	4128	3476	5456	5456
LBG-Gap	2364	3108	2504	3908	3908
GOT	3132	4128	3600	5652	5652
GOT-Gap	2364	3108	2628	4104	4104
GNT	2700	3552	2880	4500	4500

Tabela: Memória utilizada por cada protocolo (*bytes*)

Gráfico (uso de memória)



Comprimento das Mensagens Trocadas

	Curva elíptica				
Protocolo	**ETAT_T271**	**ETAT_S353**	**BN_P158**	**BN_P254**	**BN_P256**
HC	224	296	252	396	396
LCNH	224	296	252	396	396
LCNH-Gap	224	296	252	396	396
LBG	448	592	504	792	792
LBG-Gap	448	592	504	792	792
GOT	448	592	504	792	792
GOT-Gap	448	592	504	792	792
GNT	448	592	504	792	792

Tabela: Comprimento das mensagens trocadas (*bytes*)

Referências Bibliográficas

- AL-RIYAMI. S, PATERSON. K. **Certificateless Public Key Cryptography**. ASIACRYPT 2003.
- ARANHA, D. **Efficient Binary Field Arithmetic and Applications to Curve-based Cryptography**. Tutorial. CHES 2012.
- BONEH. D, FRANKLIN. M. **Identity based encryption from the Weil pairing**. Proceedings of CRYPTO 2001.
- CESENA, E.**Trace Zero Varieties in Pairing-based Cryptography**. Tese de doutorado. Università degli studi Roma Tre. 2010.

Referências Bibliográficas

- GOYA, D. NAKAMURA, D. TERADA, R. **Acordo de chave seguro contra autoridade mal intencionada**. SBSeg 2011.
- GOYA, D. OKIDA, C. TERADA, R. **Acordo de chave com autenticação sem certificado digital**. I2TS, 2010.
- HUANG, H. CAO, Z. **An ID-based Authenticated Key Exchange Protocol Based on Bilinear Diffie-Hellman Problem**. ASIACCS 2009.
- LIPPOLD, G. BOYD, C. GONZALEZ NIETO, J. **Strongly secure certificateless key agreement**. Pairing 2009.
- NI, L. CHEN, G. LI, J. HAO, Y. **Strongly secure identity-based authenticated key agreement protocols**. Computers & Electrical Engineering. 2011.

Perguntas?

Obrigado!

http://www.ime.usp.br/~rwill