Reconciliação de chaves através de um canal público usando acelerômetros

Universidade Federal de Ouro Preto
ICEB – Instituto de Ciências Exatas e Biológicas
DECOM - Departamento de Computação
Orientador: Ricardo Augusto Rabelo Oliveira

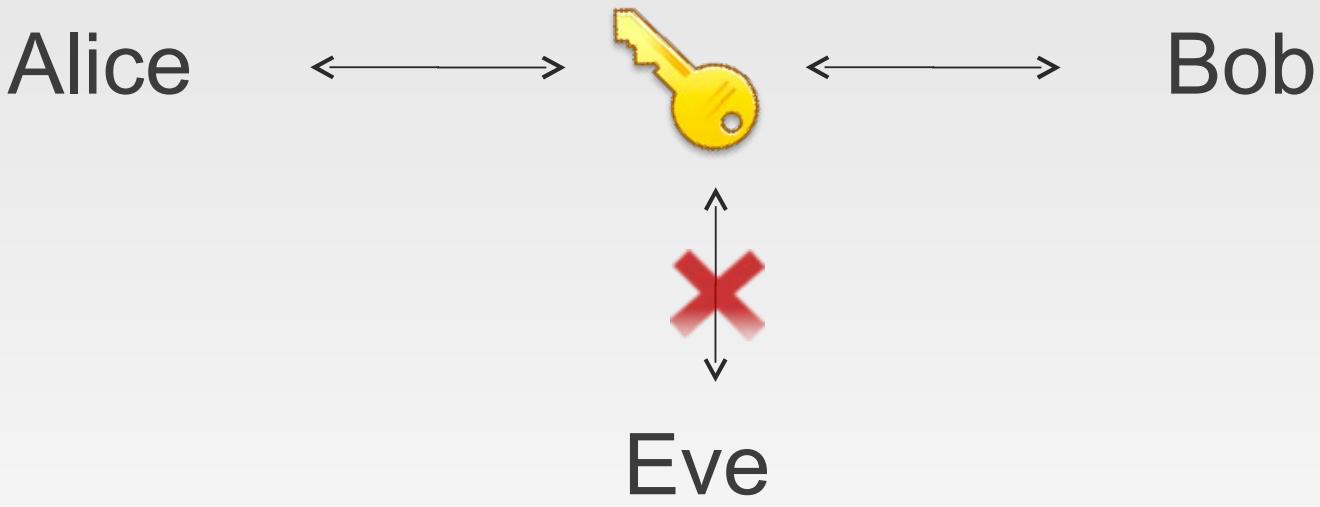
Aluno: Pedro Henrique N. Castro

Sumário

- Introdução
- Motivação
- Trabalhos relacionados
- Metodologia
- Experimentos e análise de resultados
- Conclusão

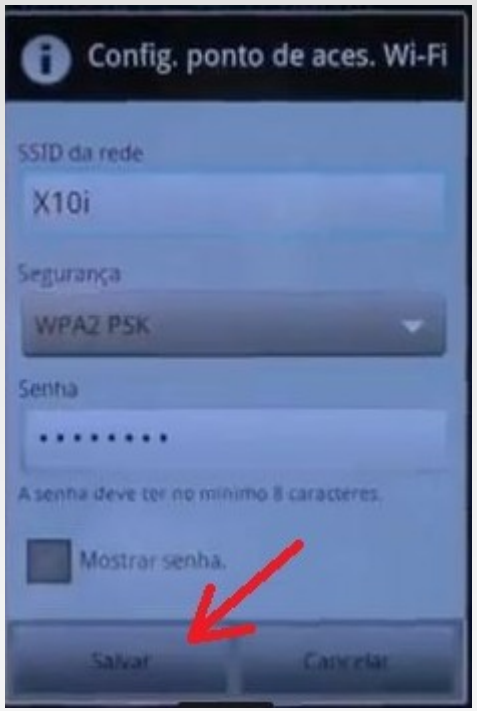
Introdução

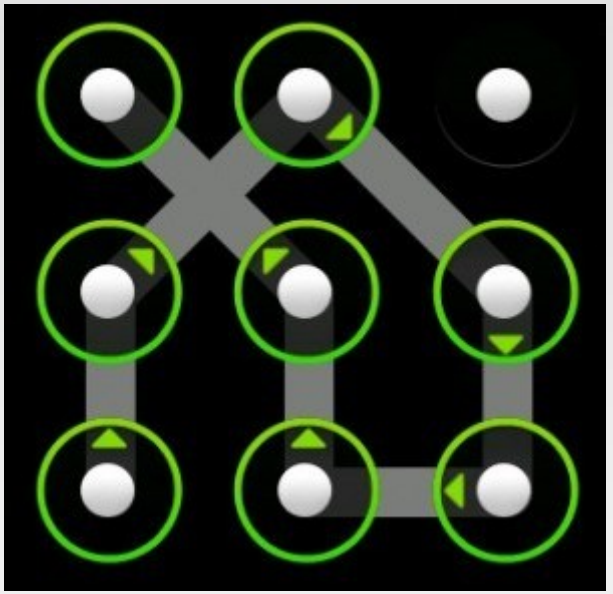
- Chaves são responsáveis por manter o segredo em um sistema criptográfico



Introdução

- Senhas





Introdução

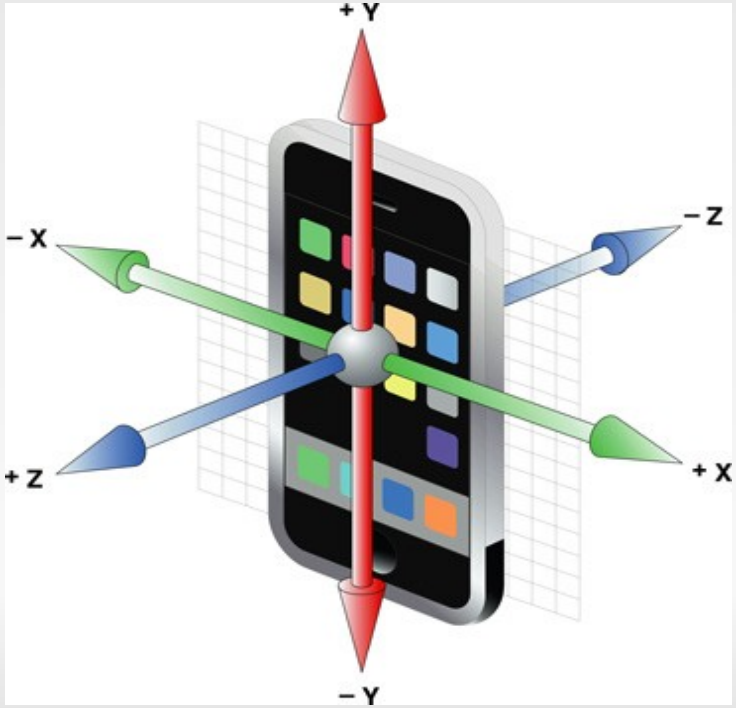
- Foto

Introdução

- A segurança de um sistema criptográfico deve-se basear na força da chave
- Chaves consideradas seguras possuem um mínimo de cerca de 128 bits
- Outras formas de se obter chaves: vídeo, som, movimento, etc

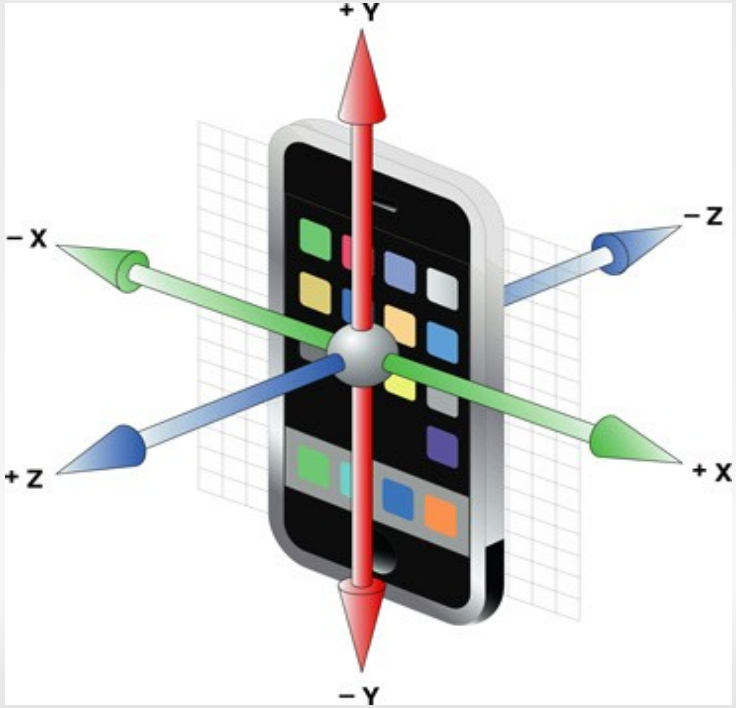
Introdução - Acelerômetro

- Acelerômetros medem a força aplicada no dispositivo nas 3 dimensões (X, Y, Z)
- Um dispositivo posicionado deitado sobre uma mesa mede (0, 0, 9,81), pois G ≈ 9,81 m/s²



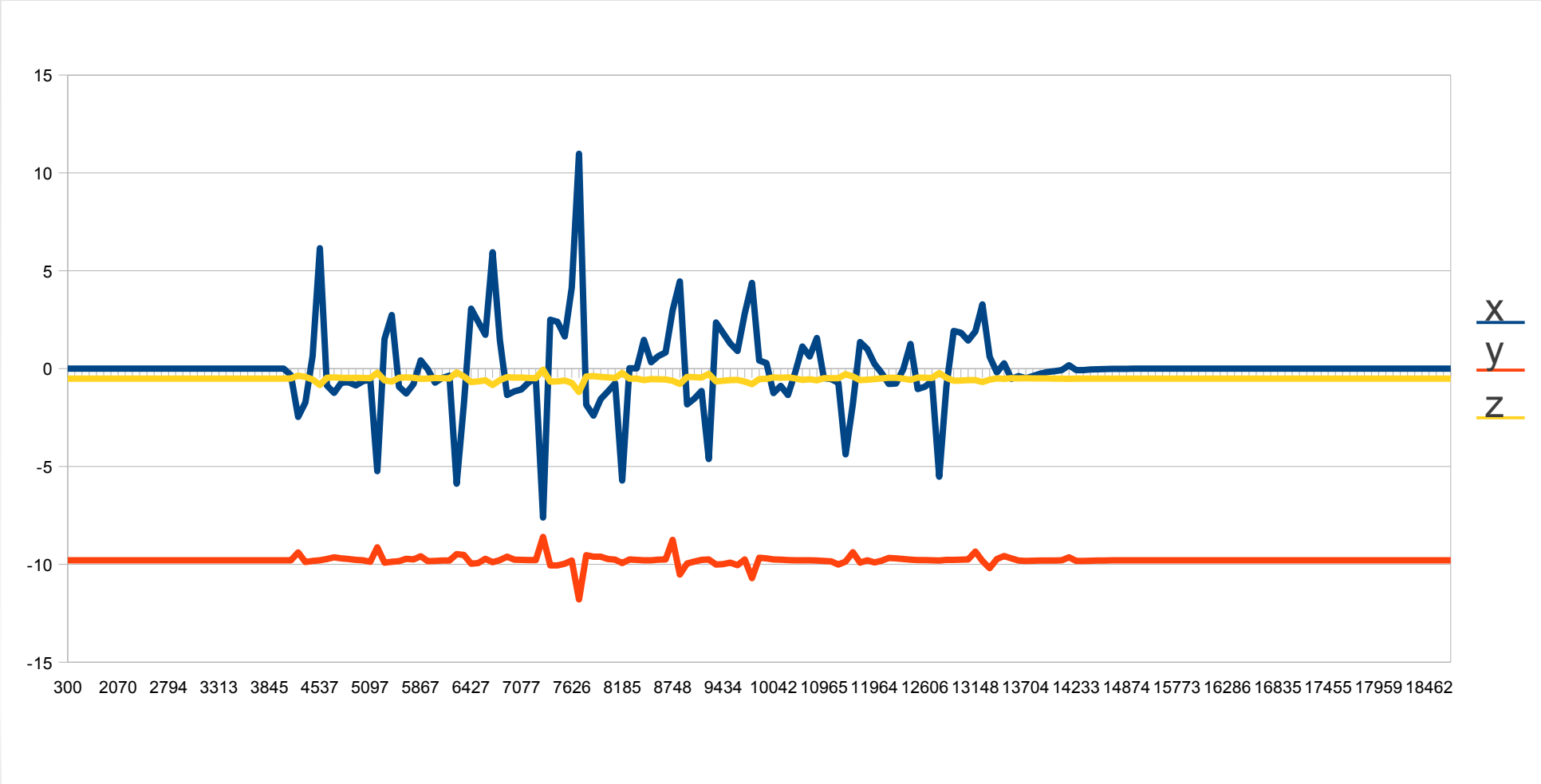
Introdução - Acelerômetro

- Um dispositivo em queda livre mede (0, 0, 0)



Introdução - Acelerômetro

- Exemplo de variação no eixo X



Introdução - Acelerômetro

Motorola Xoom

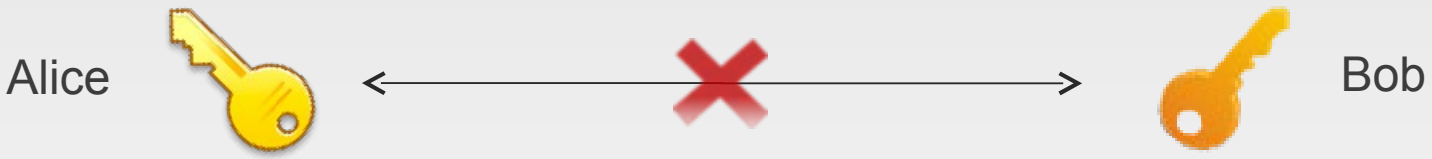
Samsung Galaxy

Introdução – Reconciliação de chaves

- Em sistemas simétricos, Alice e Bob devem possuir a mesma chave

Introdução – Reconciliação de chaves

- Existem casos onde as chaves diferem em pequenas quantidades, devido a ruídos na obtenção das mesmas

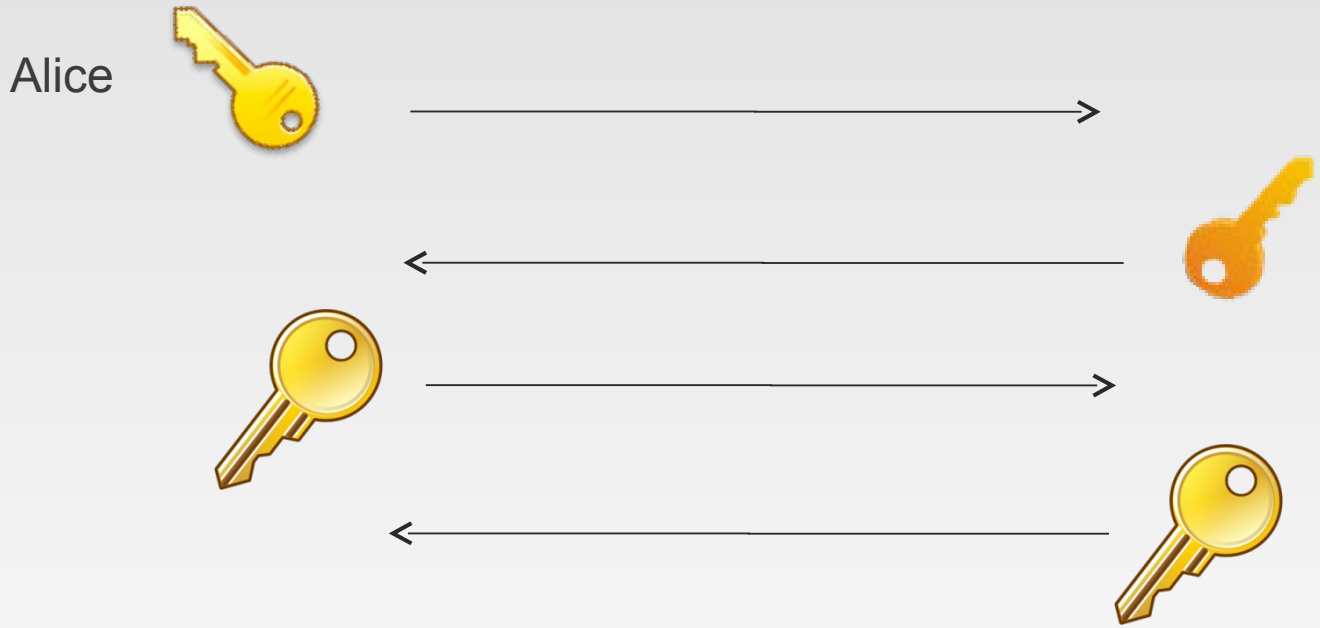


Introdução – Reconciliação de chaves

- A reconciliação consiste em transformar duas chaves criptográficas diferentes KA e KB em uma única chave comum KC

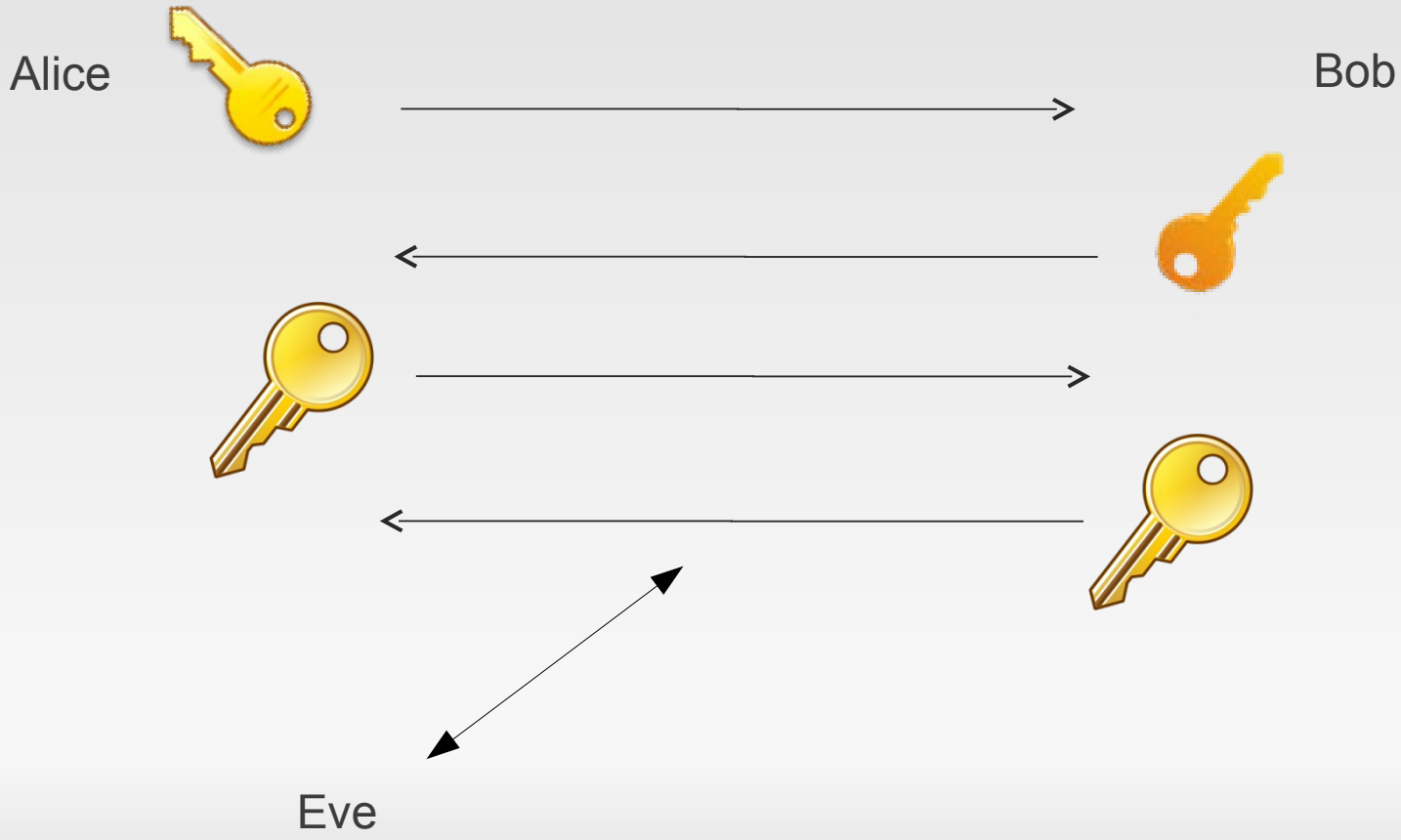
Introdução – Reconciliação de chaves

- Essa reconciliação é realizado através de trocas de informações por um canal público



Introdução – Reconciliação de chaves

- A chave deve continuar secreta, mesmo que haja um 3º elemento com total acesso ao canal



Introdução – Reconciliação de chaves

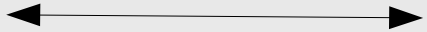
- Os protocolos de reconciliação não enviam as chaves pelo canal público, mas os bits de paridade da mesma
- É necessário que ambas as chaves KA e KB, possuem uma diferença consideravelmente pequena
- Protocolos mais comuns: BBBSS e Cascade

Introdução – Primitiva CONFIRM

1 erro:

K_A = 1101 0100

paridade = 0



K_B = 1101 0000

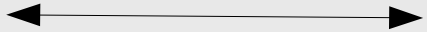
paridade = 1

Introdução – Primitiva CONFIRM

3 erros:

K_A = 1101 0100

paridade = 0



K_B = 1101 1010

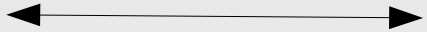
paridade = 1

Introdução – Primitiva CONFIRM

2 erros:

K_A = 1101 0100

paridade = 0



K_B = 1101 1000

paridade = 0

Introdução – Primitiva CONFIRM

- Probabilidade de acerto = 1 as paridades são diferentes
- Probabilidade de acerto = 0,5 as paridades são iguais
- Alice e Bob escolhem um subconjunto e repetem o procedimento *k* vezes para probabilidade de acerto de $1-2^{-k}$

Introdução – Primitiva BINARY

- Chave de 16 bits:
  - K_A: 1101 0100 1010 0110
  - K_B: 1101 0000 1010 0110

Introdução – Primitiva BINARY

- Chave de 16 bits:
  - K_A: 1101 0100 1010 0110
  - K_B: 1101 0000 1010 0110

Introdução – Primitiva BINARY

- Chave de 16 bits:
  - K_A: 1101 0100 1010 0110
  - K_B: 1101 0000 1010 0110

Introdução – Primitiva BINARY

- Chave de 16 bits:
  - K_A: 1101 0100 1010 0110
  - K_B: 1101 0000 1010 0110

Introdução – Primitiva BINARY

- Chave de 16 bits:
  - K_A: 1101 0100 1010 0110
  - K_B: 1101 0000 1010 0110

Introdução – Primitiva BICONF

- BICONF = CONFIRM + BINARY

Introdução – Permutação

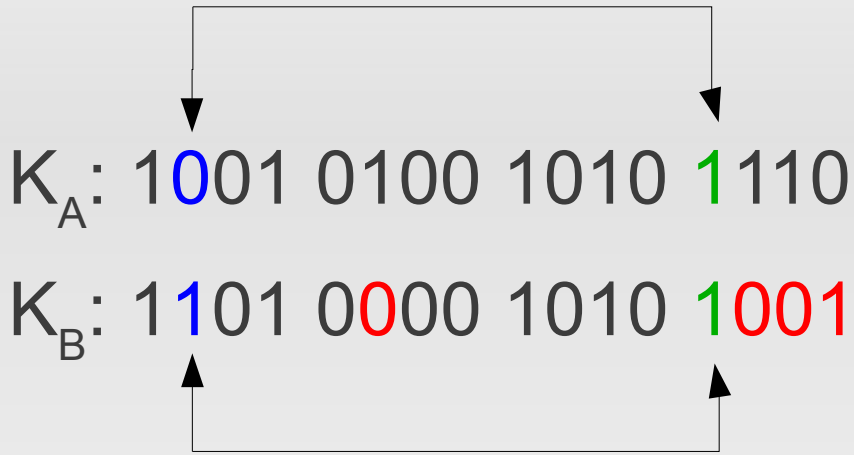
K_A: 1101 0100 1010 0110

K_B: 1101 0000 1010 1001

Introdução – Permutação

Troca 2º bit com o 13º

Introdução – Permutação



Troca 2º bit com o 13º

Introdução – Permutação

K_A: 1001 0100 1010 1110

K_B: 1101 0000 1010 1001

Troca 2º bit com o 13º

Introdução – Permutação

- Alice escolhe uma função de permutação p: $\{0,1\}^N \rightarrow \{0,1\}^N$ e envia a descrição a Bob
- As permutações permitem distribuir melhor os erros ("espalhar")
- O número de erros (bits diferentes) continuam o mesmo

Introdução – BBBSS

- Algoritmo:
  - Aplica-se a permutação
  - Divide-se K_A e K_B em blocos de tamanho *w*
    - K_A: 1101 | 0100 | 1010 | 0110
    - K_B: 1101 | 0000 | 1010 | 0110
  - Para cada bloco, aplica-se BICONF
- O procedimento é repetido *k* vezes para alcançar a probabilidade 2^{-k} de falha

Introdução – Cascade

- Algoritmo: para cada passo i=[1..p]:
  - Aplica-se a permutação
  - Divide-se K_A e K_B em blocos de tamanho *w*
    - K_A: 1101 | 0100 | 1010 | 0110
    - K_B: 1101 | 0000 | 1010 | 0110
  - Para cada bloco, aplica-se BICONF
  - Executa Cascade para cada passo anterior a i

Introdução – Cascade

- Passo 1 (ímpar)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0011 | 1010 | 0110

Introdução – Cascade

- Passo 1 (ímpar)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0011 | 1010 | 0110
- Corrigido (par)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0111 | 1010 | 0110

Introdução – Cascade

- Passo 1 (par)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0111 | 1010 | 0110

Introdução – Cascade

- Passo 1 (par)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0111 | 1010 | 0110
- Corrigido pelo passo 2 (ímpar)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0101 | 1010 | 0110

Introdução – Cascade

- Passo 1 (par)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0111 | 1010 | 0110
- Corrigido pelo passo 2 (ímpar)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0101 | 1010 | 0110
- Corrigido pelo passo 1 (par)
  - K_A: 1101 | 0100 | 1010 | 0110
  - K_B: 1101 | 0100 | 1010 | 0110

Sumário

- Introdução
- Motivação
- Trabalhos relacionados
- Metodologia
- Experimentos e análise de resultados
- Conclusão

Motivação

- Problema:
  - Como extrair chaves idênticas a partir de informações similares, trocando informações por um canal público sem comprometer a segurança?
  - Como fazê-lo utilizando menos recursos possível e com conforto?

Motivação

- Objetivos:
  - Gerar chaves confiáveis a partir de dados dos acelerômetros
  - Utilizar protocolos seguros com provas formais para reconciliar as chaves com baixo consumo de recursos
  - Prover uma base de dados de acelerômetros para estudos

Sumário

- Introdução
- Motivação
- Trabalhos relacionados
- Metodologia
- Experimentos e análise de resultados
- Conclusão

Trabalhos relacionados

- Are you with me? - Using accelerometers to determine if two devices are carried by the same person [Lester et al, 2004]
  - Determinar se 2 dispositivos são carregados pela mesma pessoa
  - Acelerômetros: ADXL202E, LIS3L02 e CXL02LF3
  - Magnitude do vetor resultante
  - Aplica FFT
  - Correlação Linear

Trabalhos relacionados

- Shake well before use: authentication based on accelerometer data [Mayrhofer, R. and Gellersen, H., 2007]
- Shake well before use: two implementations for implicit context authentication [Mayrhofer, R. and Gellersen, H., 2007]
- Shake well before use: Intuitive and secure pairing of mobile devices [Mayrhofer, R. and Gellersen, H., 2009]
  - Acelerômetros: ADXL202JE e Nokia 5500
  - Magnitude e FFT
  - Diffie-Hellman e Magnitude Squared Coherence
  - Candidate Key Protocol

Trabalhos relacionados

- The martini synch [Kirovski, D., Sinclair, M., and Wilson, D., 2007]
  - Variação da amplitude
  - BCH codes para detectar e corrigir erros

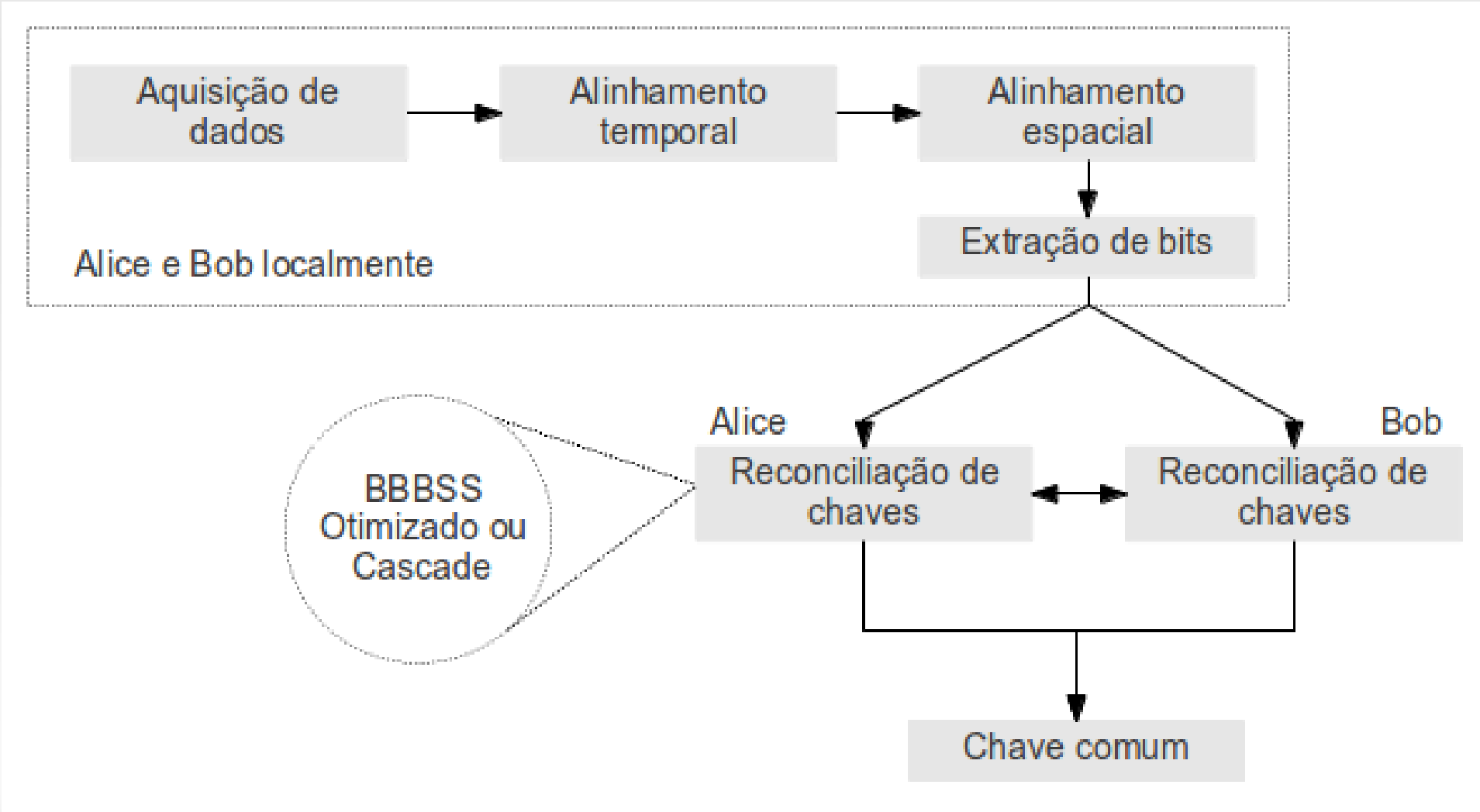
Trabalhos relacionados

- Experimental quantum cryptography [Bennett et al., 1992]
  - BBBSS
- On reconciliation of discrepant sequences shared through quantum mechanical channels [Yamazaki et al., 1997]
  - BBBSS Otimizado
- Secret-key reconciliation by public discussion [Brassard and Salvail, 1994]
  - Shell e Cascade

Sumário

- Introdução
- Motivação
- Trabalhos relacionados
- Metodologia
- Experimentos e análise de resultados
- Conclusão

Metodologia

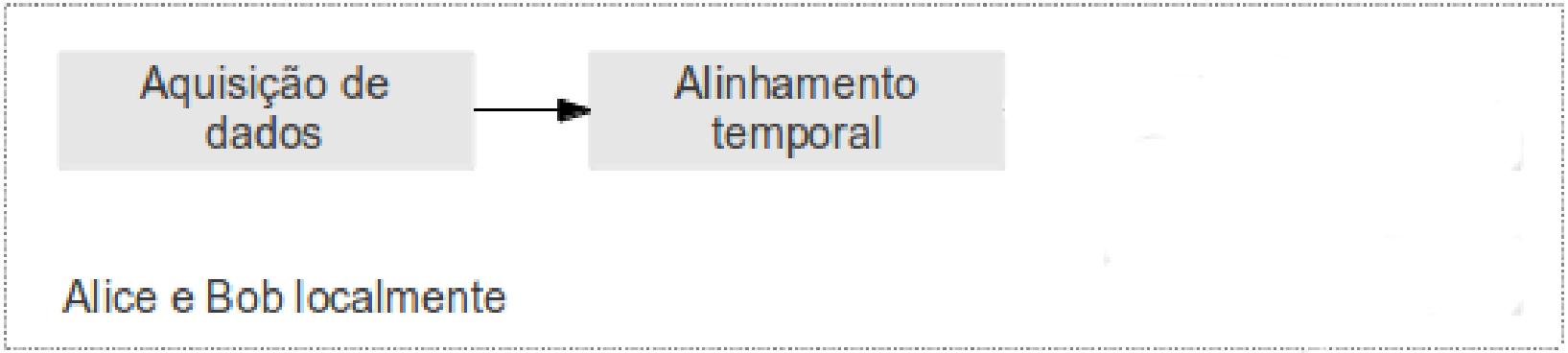


Metodologia

Metodologia – Aquisição de dados

- Taxa de amostragem: 50 Hz
  - ShakeWell – 100 a 600 Hz
  - MartiniSynch – 220 Hz
- API Java SensorManager
  - *TYPE_ACCELEROMETER*
  - *SENSOR_DELAY_FASTEST*

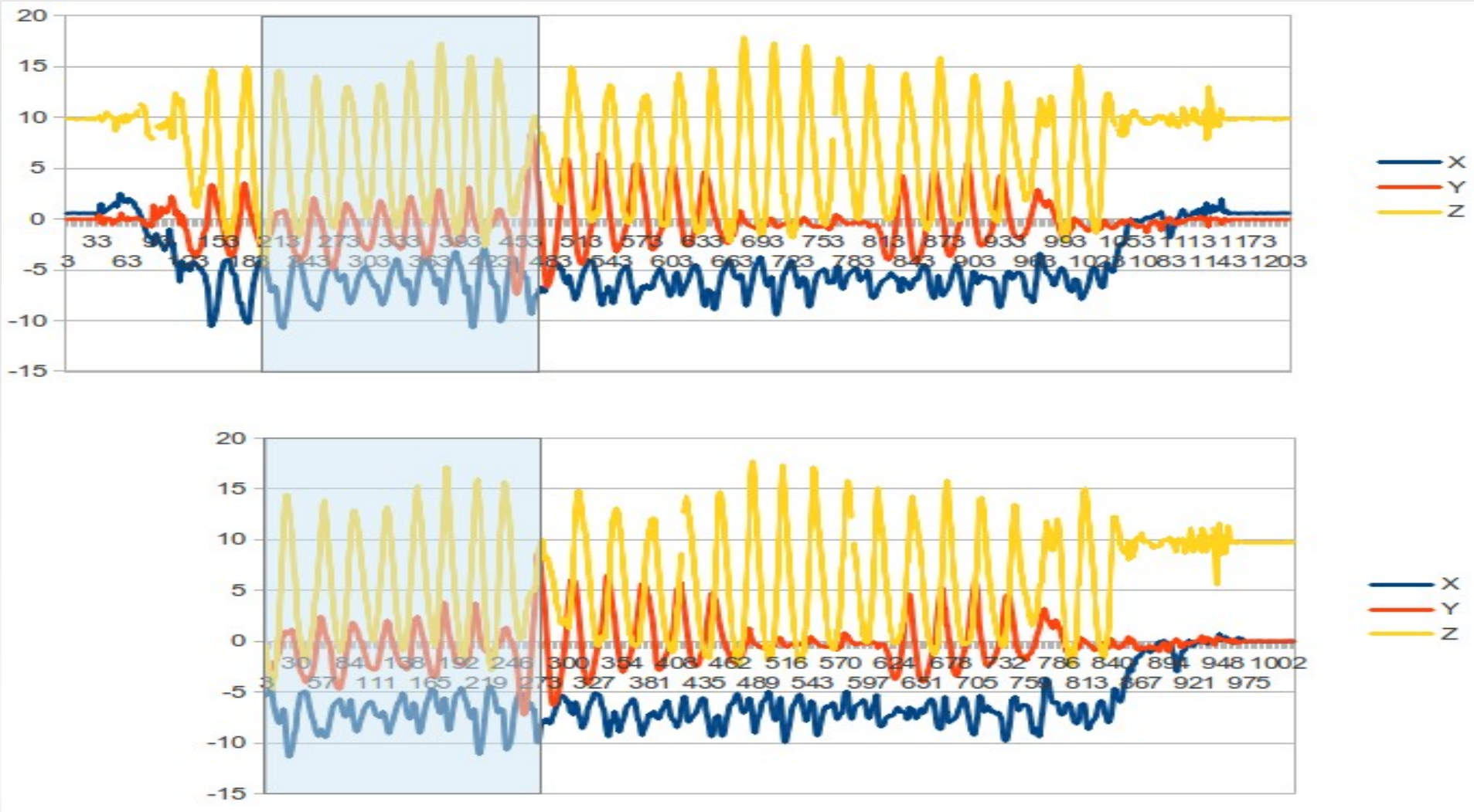
Metodologia



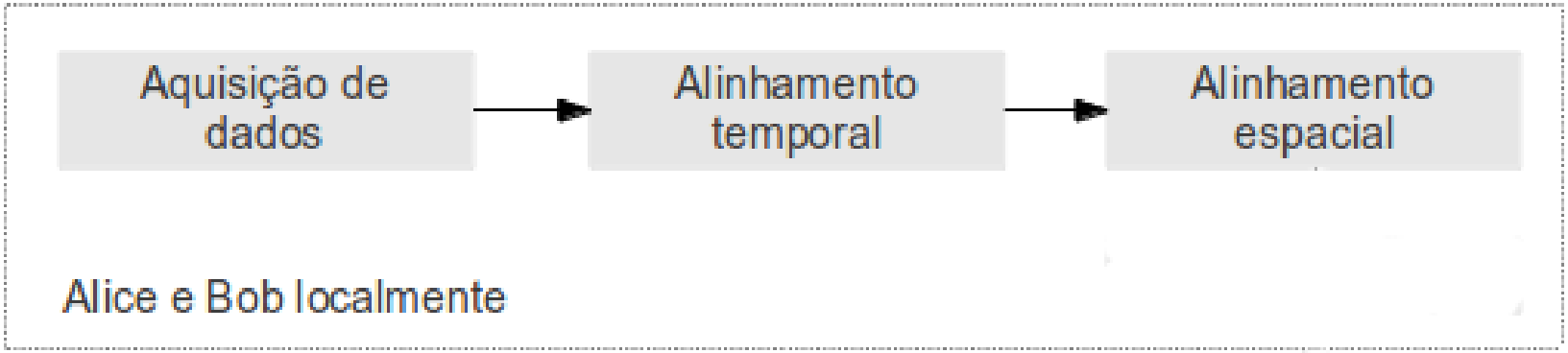
Metodologia – Alinhamento temporal

- Gatilho manual
  - ShakeWell – gatilho manual e detecção de movimento brusco
  - MartiniSynch – gatilho manual e detecção de movimento brusco e teste de proximidade
- Média dos valores em intervalos de 100 ms

Metodologia – Alinhamento temporal



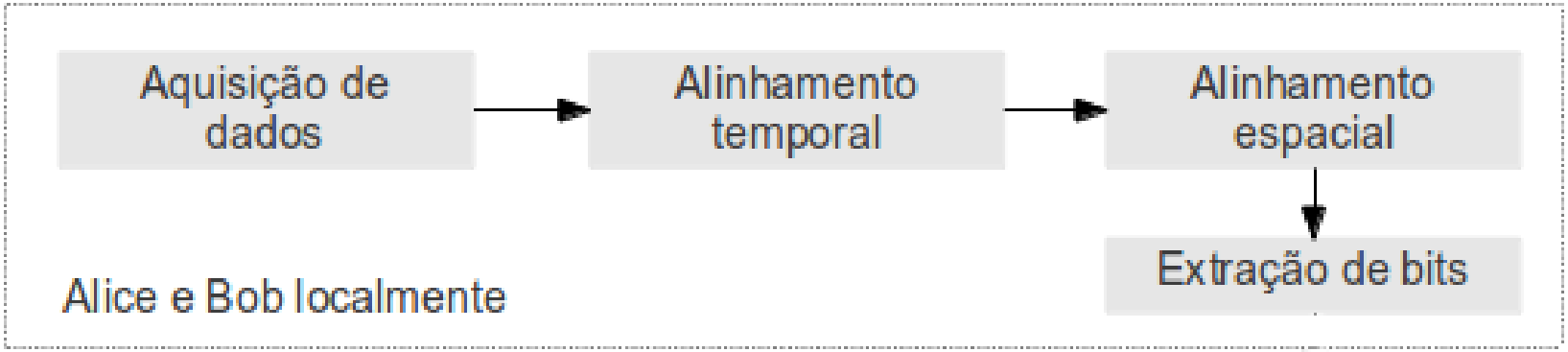
Metodologia



Metodologia – Alinhamento espacial

- Eixos independentes concatenados
  - ShakeWell – magnitude do vetor resultante
  - MartiniSynch – eixos independentes concatenados
- Transformada Wavelets
  - ShakeWell – FFT
  - MartiniSynch – Quantização

Metodologia



Metodologia – Extração de bits

- Tabela de transformação para binário – 3 bits

Intervalo	Binário
≤ -2.5	000
> -2.5 e ≤ -1.5	001
> -1.5 e ≤ -0.5	011
> -0.5 e ≤ 0.5	010
> 0.5 e ≤ 1.5	110
> 1.5 e ≤ 2.5	111
> 2.5 e ≤ 3.5	101
> 3.5	100

Metodologia – Extração de bits

- Tabela de transformação para binário – 4 bits

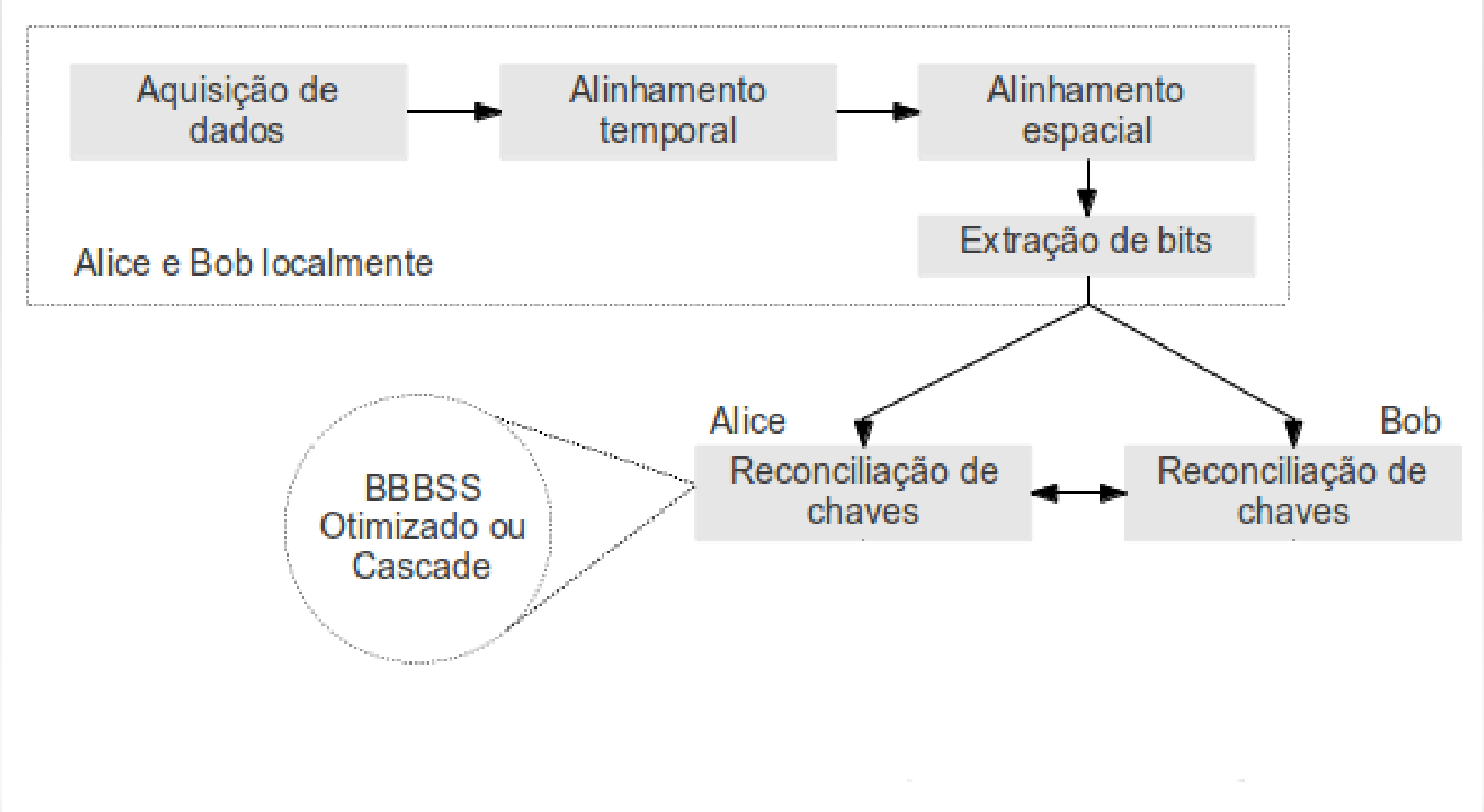
Intervalo	Binário
≤ -3.5	1000
> -3.5 e ≤ -2.5	1001
> -2.5 e ≤ -1.5	1011
> -1.5 e ≤ -0.5	1010
> -0.5 e ≤ 0.5	0010
> 0.5 e ≤ 1.5	0011
> 1.5 e ≤ 2.5	0001
> 2.5 e ≤ 3.5	0000
> 3.5	0100

Metodologia – Extração de bits

- Tabela de transformação para binário – 5 bits

Intervalo	Binário
≤ -15.5	11110
> -15.5 e ≤ -14.5	11111
> -14.5 e ≤ -13.5	11101
> -13.5 e ≤ -12.5	11100
> -12.5 e ≤ -11.5	10100
> -11.5 e ≤ -10.5	10101
> -10.5 e ≤ -9.5	10111
> -9.5 e ≤ -8.5	10110
> -8.5 e ≤ -7.5	10010
> -7.5 e ≤ -6.5	10011
> -6.5 e ≤ -5.5	10001
> -5.5 e ≤ -4.5	10000
> -4.5 e ≤ -3.5	11000
> -3.5 e ≤ -2.5	11001
> -2.5 e ≤ -1.5	11011
> -1.5 e ≤ -0.5	11010
> -0.5 e ≤ 0.5	01010
> 0.5 e ≤ 1.5	01011
> 1.5 e ≤ 2.5	01001
> 2.5 e ≤ 3.5	01000
> 3.5 e ≤ 4.5	00000
> 4.5 e ≤ 5.5	00001
> 5.5 e ≤ 6.5	00011
> 6.5 e ≤ 7.5	00010
> 7.5 e ≤ 8.5	00110
> 8.5 e ≤ 9.5	00111
> 9.5 e ≤ 10.5	00101
> 10.5 e ≤ 11.5	00100
> 11.5 e ≤ 12.5	01100
> 12.5 e ≤ 13.5	01101
> 13.5 e ≤ 14.5	01111
> 14.5	01110

Metodologia



Metodologia – BBBSS

- Parâmetros
  - Tamanho inicial do bloco (7 – 20 bits):

$$w_0 = \lceil 1/e_0 \rceil$$

  - A cada iteração *i* a taxa de erros e_i e o tamanho do bloco w_i são recalculados
  - Taxa de erro: 5 – 16%
  - K: 10

Metodologia - BBBSS

- Provendo segurança:
  - Remoção do último bit do bloco cuja paridade foi revelada

Metodologia – Cascade

- Parâmetros
  - Tamanho inicial do bloco (7 – 20 bits):

$$w_0 = \lceil 1/e_0 \rceil$$

  - Tamanho do bloco é dobrado a cada passo:

$$w_i = 2 * w_{i-1}$$

  - Taxa de erro: 5 – 16%
  - Número de passos: 4

Metodologia – Cascade

- Privacy Amplification
  - N = M – R
  - M: tamanho original da chave
  - R: número de bits revelados
  - N: tamanho da nova chave

$$F = \{0,1\}^M \rightarrow \{0,1\}^N$$

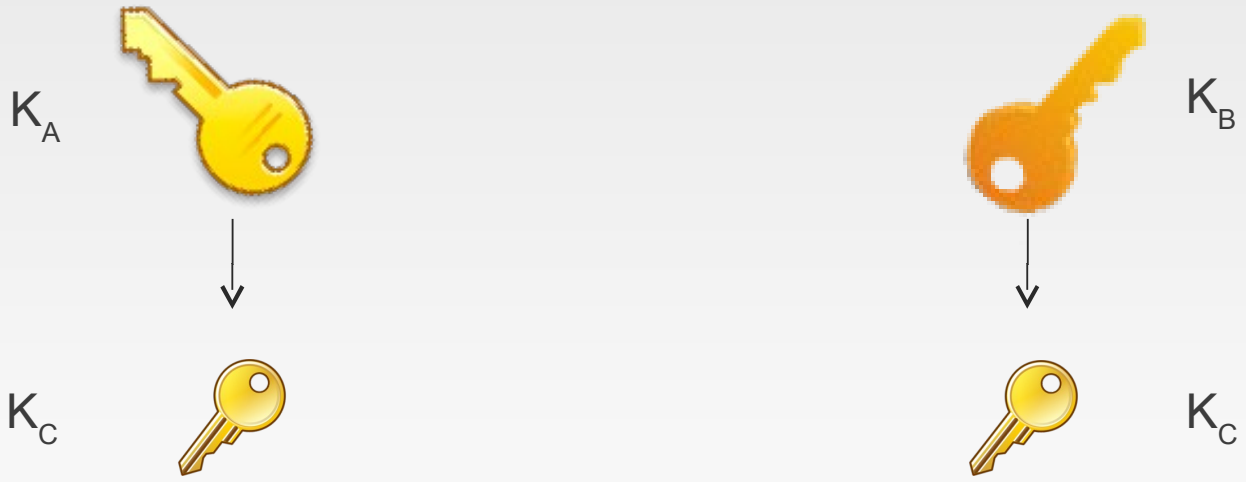
Metodologia – Cascade

- Privacy Amplification
  - Matriz N x M:

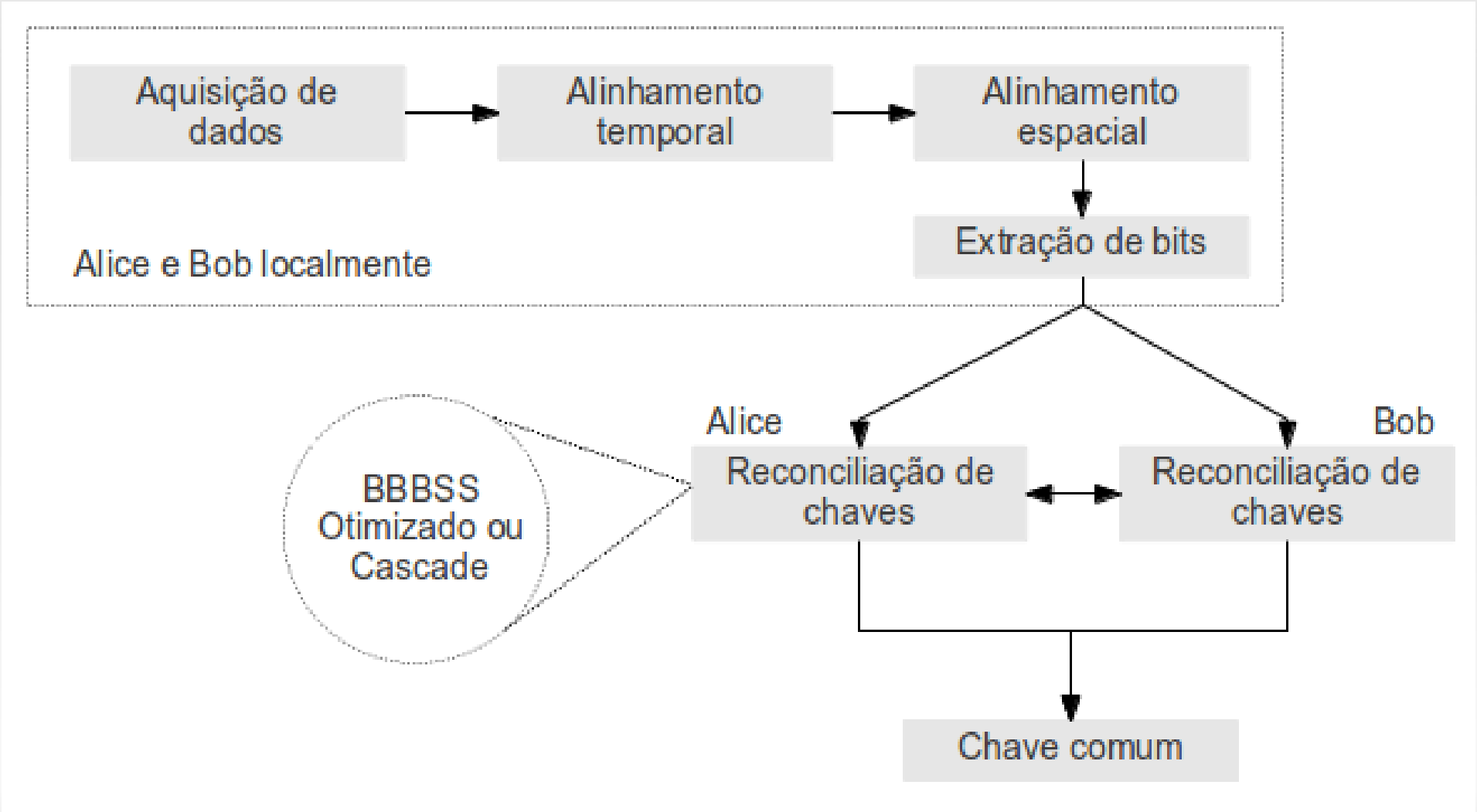
Matriz					K		K'
0	1	0	0		1		0
1	0	1	1	x	0	=	1
1	1	0	1		1		0
					1		

Metodologia - Reconciliação de chaves

- Ao final das reconciliações de todas as sub-chaves, elas se juntam para formar uma chave K_C comum a Alice e Bob, substituindo as chaves iniciais K_A e K_B.



Metodologia



Sumário

- Introdução
- Motivação
- Trabalhos relacionados
- Metodologia
- Experimentos e análise de resultados
- Conclusão

Experimentos e análise de resultados

- Tablets Motorola Xoom e Samsung Galaxy Tab emparelhados
- 25 testes de 5 segundos com o MX e 25 com o SG
- Experimentos agrupados em correlatos e não-correlatos

Experimentos e análise de resultados – Extração de bits

- Motorola

	Bits		Error rate	
	$\bar{x}$	σ	$\bar{x}$	σ
Related (3 bits)	441.000	0.000	0.106	0.032
Unrelated (3 bits)	-	-	0.329	0.048
Related (4 bits)	588.000	0.000	0.090	0.028
Unrelated (4 bits)	-	-	0.305	0.046
Related (5 bits)	735.000	0.000	0.126	0.036
Unrelated (5 bits)	-	-	0.308	0.038

Experimentos e análise de resultados – Extração de bits

- Samsung

	Bits		Error rate	
	$\bar{x}$	σ	$\bar{x}$	σ
Related (3 bits)	441.120	4.013	0.109	0.037
Unrelated (3 bits)	-	-	0.358	0.038
Related (4 bits)	588.960	3.322	0.090	0.030
Unrelated (4 bits)	-	-	0.329	0.036
Related (5 bits)	736.200	4.153	0.124	0.043
Unrelated (5 bits)	-	-	0.341	0.037

Experimentos e análise de resultados - Reconciliação BBBSS

- Motorola

e	$\bar{x}$	σ	False-negatives	False-positives
0.05	464.5	30.4	0.92	0.0
0.06	444.7	60.0	0.84	0.0
0.07	427.7	54.3	0.68	0.0
0.08	389.6	54.4	0.48	0.0
0.09	304.3	55.2	0.36	0.0
0.10	314.5	61.6	0.32	0.0
0.11	302.7	75.7	0.16	0.0
0.12	270.1	86.7	0.04	0.0
0.13	228.7	75.6	0.04	0.0
0.14	203.4	49.1	0.16	0.0
0.15	187.2	41.3	0.28	0.0
0.16	171.5	32.5	0.52	0.0

Experimentos e análise de resultados - Reconciliação BBBSS

- Samsung

e	$\bar{x}$	σ	False-negatives	False-positives
0.05	473.0	27.8	0.88	0.0
0.06	438.0	34.6	0.76	0.0
0.07	402.8	52.6	0.64	0.0
0.08	374.7	46.6	0.60	0.0
0.09	316.4	69.2	0.32	0.0
0.10	317.7	75.9	0.28	0.0
0.11	300.1	78.0	0.12	0.0
0.12	267.3	68.4	0.20	0.0
0.13	238.6	74.1	0.04	0.0
0.14	200.1	51.2	0.08	0.0
0.15	181.5	48.8	0.24	0.0
0.16	172.7	36.0	0.44	0.0

Experimentos e análise de resultados - Reconciliação Cascade

- Motorola

e	$\bar{x}$	σ	False-negatives	False-positives
0.05	336.1	38.3	0.76	0.0
0.06	345.1	46.2	0.68	0.0
0.07	326.7	46.8	0.48	0.0
0.08	328.8	44.7	0.56	0.0
0.09	302.5	58.6	0.32	0.0
0.10	288.8	65.9	0.24	0.0
0.11	274.9	70.6	0.16	0.0
0.12	273.9	66.4	0.12	0.0
0.13	264.6	64.6	0.04	0.0
0.14	266.5	64.5	0.04	0.0
0.15	255.0	61.5	0.04	0.0
0.16	251.1	65.8	0.00	0.0

Experimentos e análise de resultados - Reconciliação Cascade

- Samsung

e	$\bar{x}$	σ	False-negatives	False-positives
0.05	363.6	43.9	0.76	0.0
0.06	332.4	65.8	0.72	0.0
0.07	345.2	52.1	0.60	0.0
0.08	308.7	73.2	0.40	0.0
0.09	296.8	69.5	0.28	0.0
0.10	285.7	65.3	0.20	0.0
0.11	283.2	73.3	0.20	0.0
0.12	277.2	66.9	0.12	0.0
0.13	276.4	62.0	0.12	0.0
0.14	281.6	58.3	0.20	0.0
0.15	255.6	65.8	0.04	0.0
0.16	264.5	58.0	0.08	0.0016

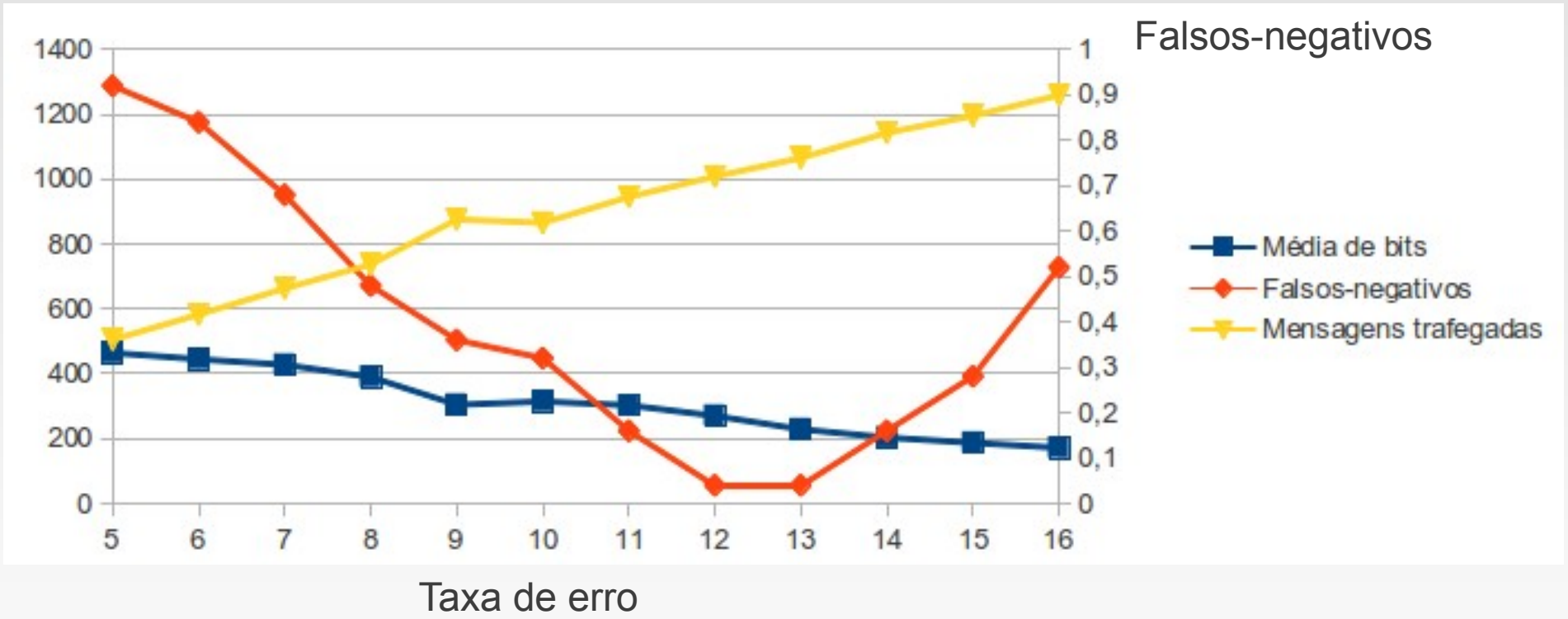
Experimentos e análise de resultados – Troca de mensagens

Table 9: Message exchange

	BBBSS			Cascade		
e	Related	Unrelated	Both	Related	Unrelated	Both
0.05	565.15	503.6	506.05	558.3	631.4	628.45
0.06	651.55	582	584.8	585.7	728.5	722.8
0.07	732.55	661.6	664.45	593.65	801.75	793.45
0.08	808.4	736.15	739	634.35	918.35	907.05
0.09	982.05	873.1	877.4	679.65	1048.25	1033.55
0.1	975.05	863.2	867.65	710.05	1134.25	1117.25
0.11	1039.35	943.05	946.9	728.6	1133.35	1117.15
0.12	1113.4	1004.8	1009.15	737.65	1239.6	1219.55
0.13	1181.1	1065.15	1069.75	750.7	1345.95	1322.2
0.14	1243.9	1140.6	1144.7	741.3	1344.25	1320.15
0.15	1292.25	1193.25	1197.25	783.15	1497.85	1469.3
0.16	1355.3	1256.85	1260.75	777.1	1496.6	1467.85

Experimentos e análise de resultados – Gráfico comparativo

- BBBSS (Motorola)

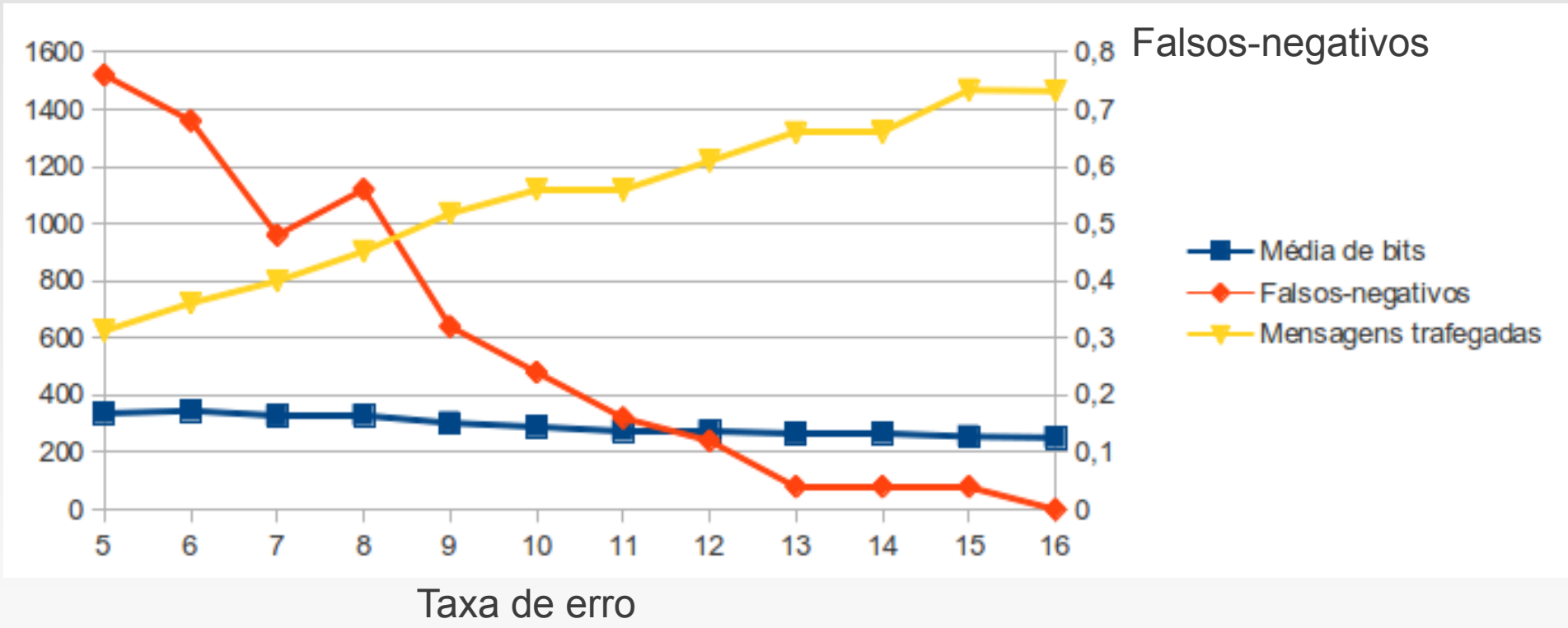


Experimentos e análise de resultados – Gráfico comparativo

- BBBSS (Samsung)

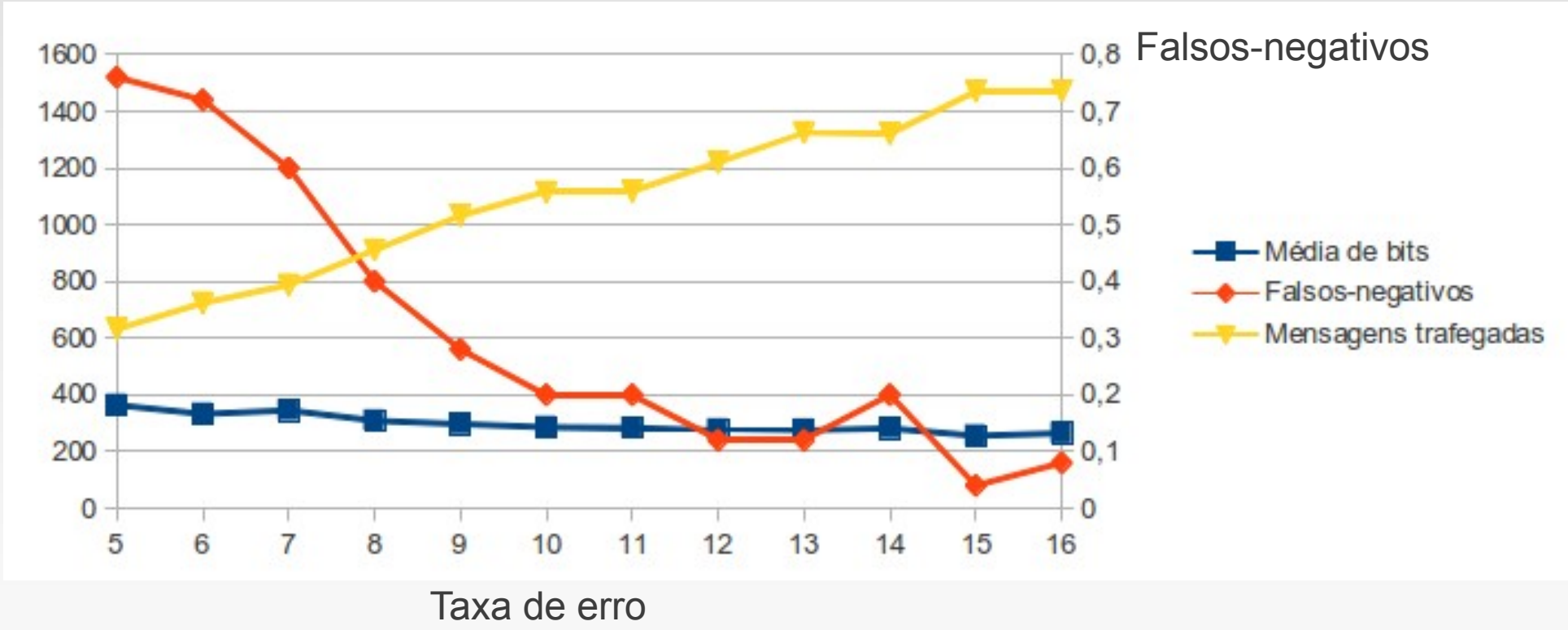
Experimentos e análise de resultados – Gráfico comparativo

- Cascade (Motorola)



Experimentos e análise de resultados – Gráfico comparativo

- Cascade (Samsung)



Experimentos e análise de resultados

- Desempenho

	ShakeWell (ShaVe)	ShakeWell (ShaCK)	MartiniSync	BBBSS (13%)	Cascade (15%)
False-positives	0.0	0.0	-	0.0	0.0
False-negatives	0.1024	0.12	0.02	0.04	0.04
Entropy (bits)/s	7 - 10	7 - 10	10 - 15	25.6 - 78	29.4 - 73.4
Minimum time for the 128 bits key	12 - 20 s	12 - 20 s	6 - 12 s	3 - 5 s	3 - 5 s

Sumário

- Introdução
- Motivação
- Trabalhos relacionados
- Metodologia
- Experimentos e análise de resultados
- Conclusão

Conclusão

- É possível aplicar os protocolos de Reconciliação de Chaves com precisão
- Pode-se gerar chaves de 128 bits em 5s contra os 6s e 12s exigidos nos trabalhos anteriores
- Flexibilidade

Conclusão

- Trabalhos futuros:
  - Novas métricas: processamento e a quantidade de memória envolvida
  - Testes com dispositivos diferentes
  - Implementar os protocolos do ShakeWell e MartiniSynch