Inatel
Instituto Nacional de Telecomunicações

Redes Neurais Artificiais Aplicadas à Geração de Chaves Criptográficas Binárias

Gustavo Pasqua de Oliveira Celani
Marcelo Vinícius Cysneiros Aragão

Santa Rita do Sapucaí, Novembro de 2018

Sumário

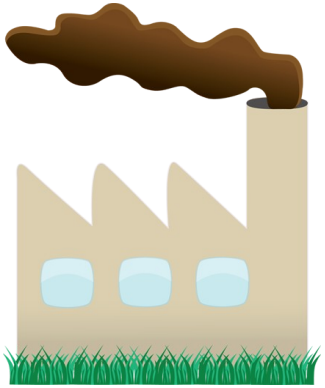
Inatel
Instituto Nacional de Telecomunicações

- → Introdução
- → Objetivos e contribuições do trabalho
- → Revisão da Teoria
- → Revisão da Bibliografia
- → Proposta
- → Experimentos
- → Resultados
- → Conclusão

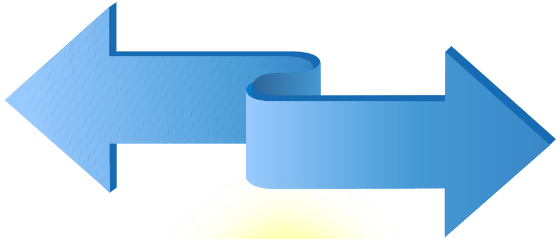
Introdução

Introdução

Inatel
Instituto Nacional de Telecomunicações



Era Industrial



Patrimônio Intelectual

Era da Informação (Era Digital)

Introdução

Inatel
Instituto Nacional de Telecomunicações

→ **Usuários** podem ser alvo de ataques tanto **diretamente** quanto **indiretamente**

→ Perda de dados se torna algo **catastrófico**

G1 ECONOMIA

TECNOLOGIA

Uber admite que omitiu ataque hacker que roubou dados de 57 milhões de usuários em 2016

Incidente atingiu informações tanto de motoristas quanto passageiros; informação foi revelada nesta terça-feira (21) pelo novo presidente da companhia.

Por G1

21/11/2017 20h52 · Atualizado há 11 meses

InfoMoney

POR RODRIGO TOLOTTI UMPIERES - EM MERCADOS / BITCOIN - 19 DEZ, 2017 19H28

Corretora de Bitcoin sul-coreana declara falência após ataque hacker

Este é o segundo ataque hacker em oito meses e, desta vez, a companhia perdeu 17% de suas reservas de ativos

Disponível em <https://bit.ly/2PWLRG4>. Acessado em nov 2018

Introdução

Inatel
Instituto Nacional de Telecomunicações

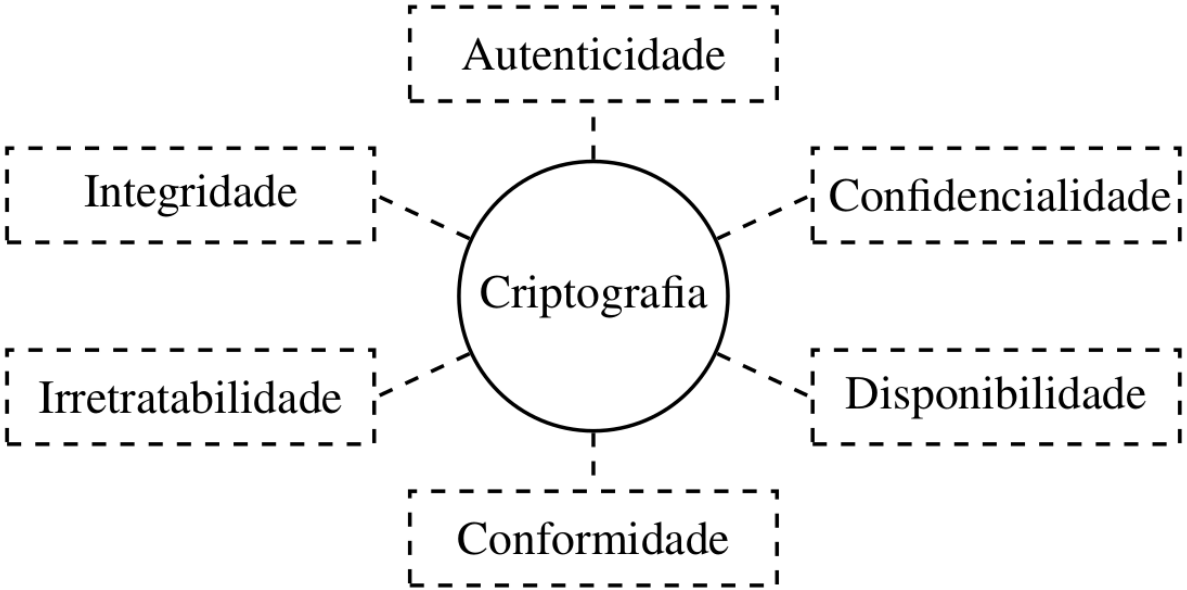
Dados

Segurança da Informação (SI)

Introdução

Inatel
Instituto Nacional de Telecomunicações

→ A **criptografia** é uma das principais ferramentas da Segurança da Informação



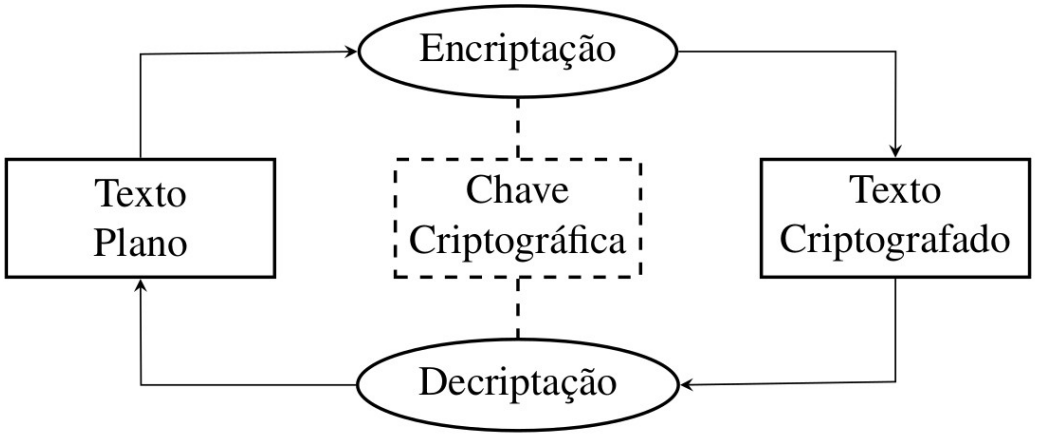
Introdução

Inatel
Instituto Nacional de Telecomunicações

→ Os algoritmos de criptografia necessitam de **uma ou mais chaves**
→ As chaves criptográficas têm a função de parametrizar as operação dos algoritmos
→ **Somente uma chave** (ou conjunto) é capaz de descriptografar uma mensagem

Exemplo:

→ Criptografia simétrica
→ Uma chave envolvida
→ Chave compartilhada



Introdução

Inatel
Instituto Nacional de Telecomunicações

→ A maneira mais comum de gerar chaves é utilizando valores **pseudoaleatórios**

→ Para garantir a pseudoaleatoriedade, é necessário colher **entropia** do sistema

```
gustavo@GustavoCelani-PC:~$ gpg --generate-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Gustavo
Email address: gustavo@mailserver.com
You selected this USER-ID:
    "Gustavo <gustavo@mailserver.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 1AF3B3A05D532FF1 marked as ultimately trusted
gpg: revocation certificate stored as '/home/gustavo/.gnupg/openpgp-revocs.d/A43
public and secret key created and signed.

pub   rsa3072 2018-11-11 [SC] [expires: 2020-11-10]
      A4328983DFB120AFB8267CF31AF3B3A05D532FF1
uid                      Gustavo <gustavo@mailserver.com>
sub   rsa3072 2018-11-11 [E] [expires: 2020-11-10]
```

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
```

Introdução

Inatel
Instituto Nacional de Telecomunicações

→ A quantidade de entropia é diretamente proporcional ao **tamanho da chave**

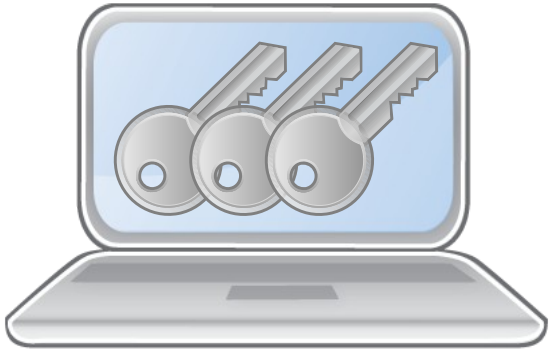
→ Sistemas com **fontes de entropia limitadas** se tornam ineficientes

Objetivos e Contribuições do Trabalho

Objetivos / Contribuições

Inatel
Instituto Nacional de Telecomunicações

- → **Gerar chaves** criptográficas binárias utilizando criptografia neural
- → Procedimento **metrificado** com base nos parâmetros necessários
- → Gerar chaves com **tamanho arbitrário** de forma otimizada
- → Apontar **potenciais melhorias** nos modelos atualmente propostos



Revisão da Teoria

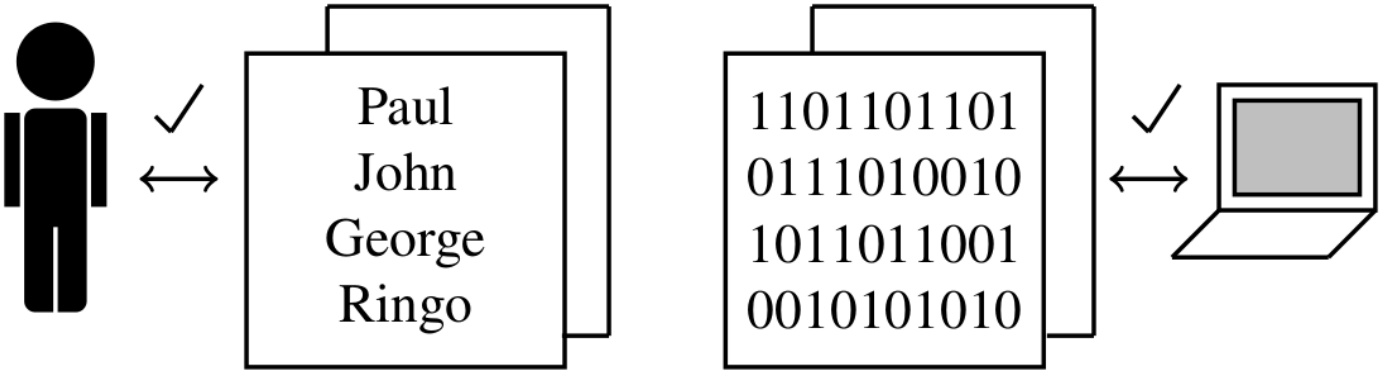
Revisão da Teoria

Inatel
Instituto Nacional de Telecomunicações

- → Segurança da Informação
- → Criptografia
- → Chaves Criptográficas
- → Criptografia Neural
- → Redes Neurais Artificiais

Segurança da Informação

→ **Informação** é tudo aquilo considero relevante o suficiente para ser **processado ou armazenado**, tanto por humanos, quanto por máquinas



→ Mecanismos de defesa **físicos**:

→ Infraestrutura
→ Blindagem
→ Restrição de acesso
→ Vigilantes

Mecanismos de defesa **lógicos**:

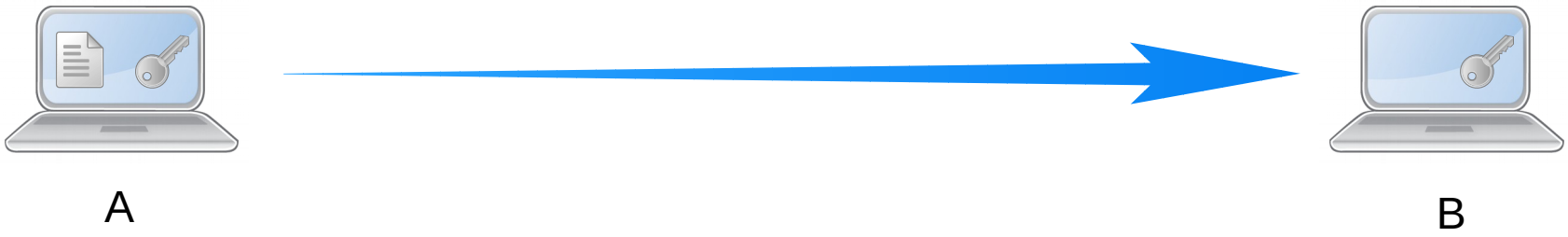
→ Protocolos de comunicação
→ Certificação digital
→ Garantia de integridade *(hashing)*
→ *Firewall* de rede
→ *Proxy* de rede
→ Anti-virus
→ **Criptografia**

Criptografia

→ Funcionamento

A

→ Funcionamento



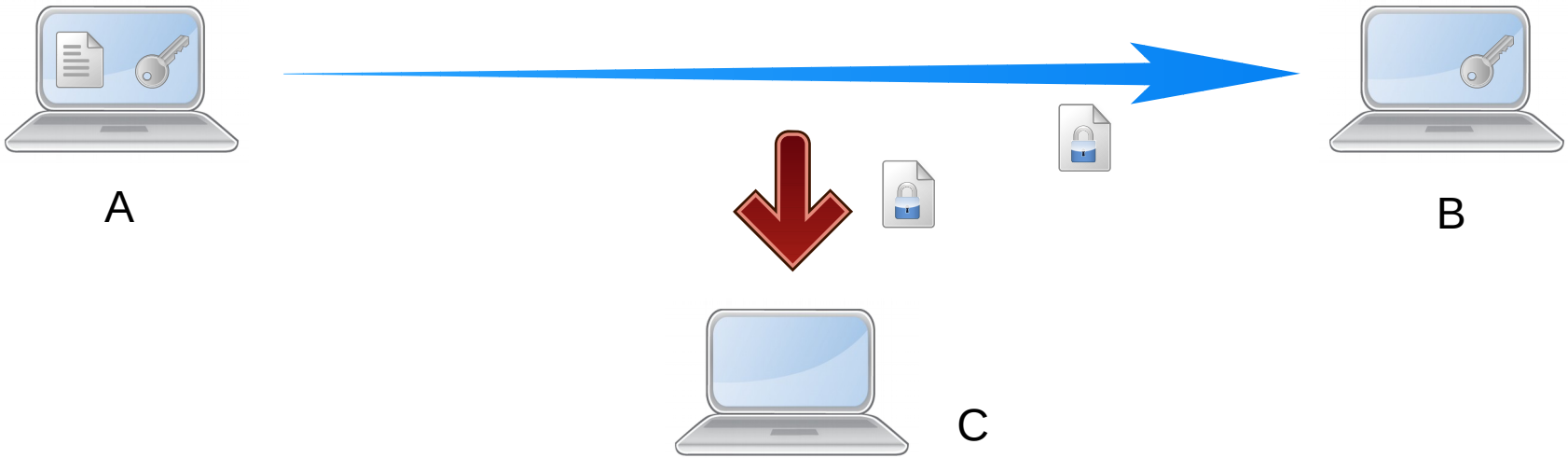
→ Funcionamento

→ Funcionamento

A

B

→ Funcionamento



→ Funcionamento

A

B

C

Algoritmos Criptográficos Relevantes

Criptografia

Inatel
Instituto Nacional de Telecomunicações

- → **Cifra de César –** Chave inteira
- → ***Data Encryption Standard* (DES) –** Chave de 64 bits
- → ***Blowfish* –** Chaves de até 448 bits
- → ***Twofish* –** Chave de 256 bits
- → ***Triple DES* (*3DES*) –** Chave de 64 bits
- → ***Cast-128 (Cast5)* –** Chave de até 128 bits
- → ***Cast-256 (Cast6)* –** Chave de até 256 bits
- → ***Advanced Encryption Standard* (AES) –** Chave de 256 bits

Chaves Criptográficas

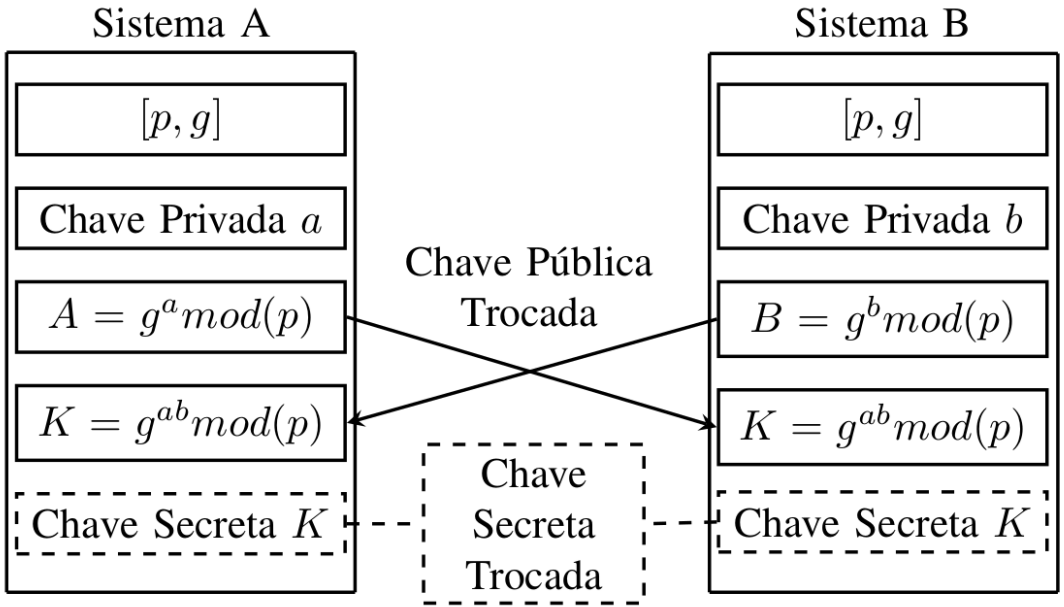
Chaves Criptográficas

Inatel
Instituto Nacional de Telecomunicações

→ **Chave pública**

→ **Chave privada**

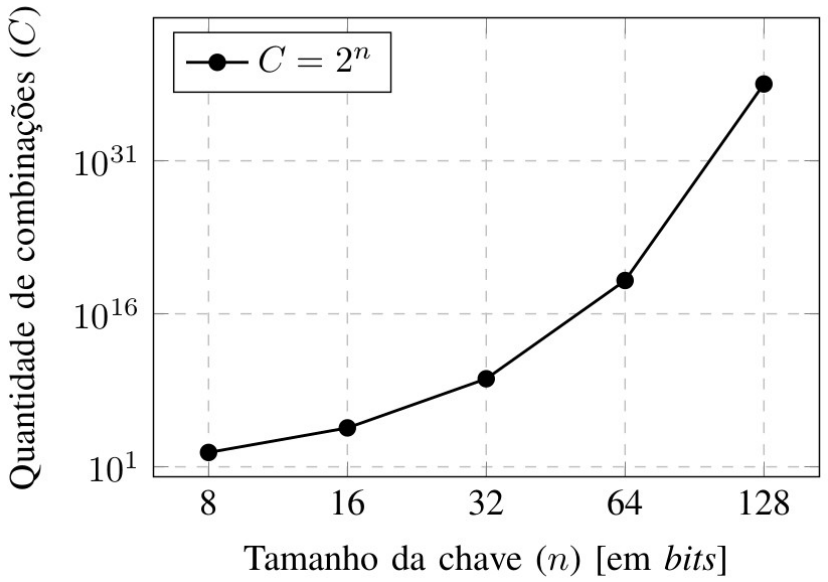
→ **Protocolo Diffie-Hellman**



Chaves Criptográficas

Inatel
Instituto Nacional de Telecomunicações

- → **Ataque de Força Bruta**
- → **Simples** e comum
- → Busca **exaustiva**
- → Testa todas as combinações possíveis
- → 100% eficaz
- → Computacionalmente **inviável** dependendo do comprimento da chave

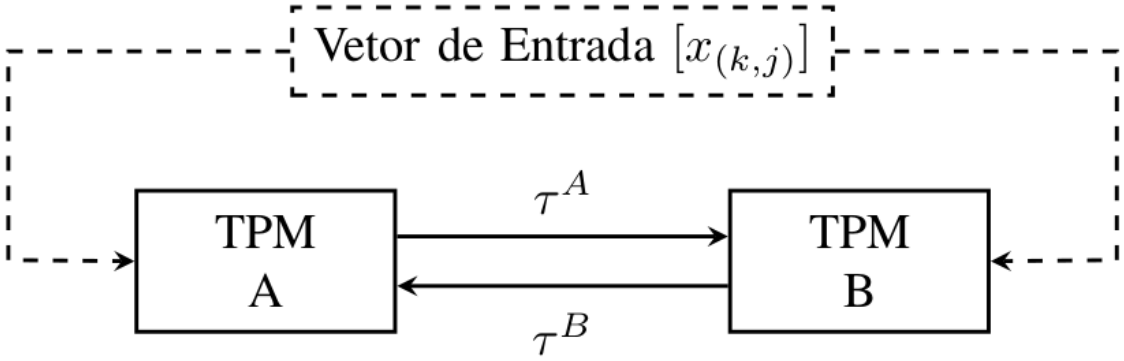


Criptografia Neural

Criptografia Neural

Inatel
Instituto Nacional de Telecomunicações

- → Utiliza redes neurais artificiais na **geração** e **troca** de chaves criptográficas
- → Utiliza uma configuração de rede neural artificial chamada ***Tree Parity Machine***
- → Explora a **sincronização mútua** entre duas *Tree Parity Machines*
- → **Vetores de entrada** compartilhados
- → **Vetor de pesos sinápticos** são as chaves resultantes ao final da sincronização



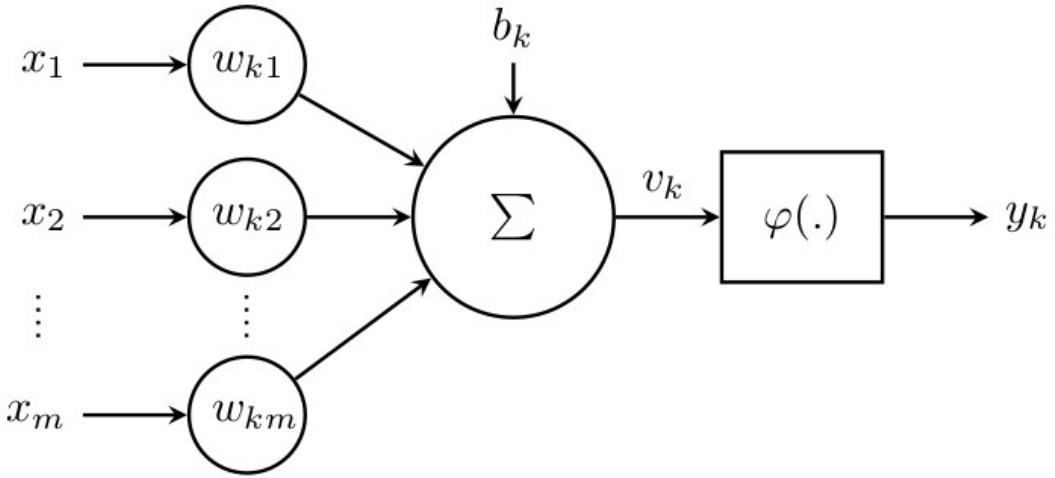
Redes Neurais Artificiais

Redes Neurais Artificiais

Inatel
Instituto Nacional de Telecomunicações

→ Reproduzir computacionalmente o processamento realizado pelo **cérebro** humano

→ Agregação de unidades discretas baseadas em **neurônios** biológicos

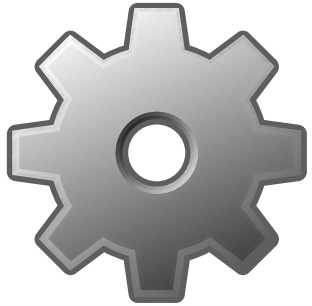


→ ***Tree Parity Machine***

→ ***Multilayer***: Possui múltiplas camadas
→ ***Feedforward***: Saídas não realimentam neurônios anteriores

→ Parâmetros necessários:

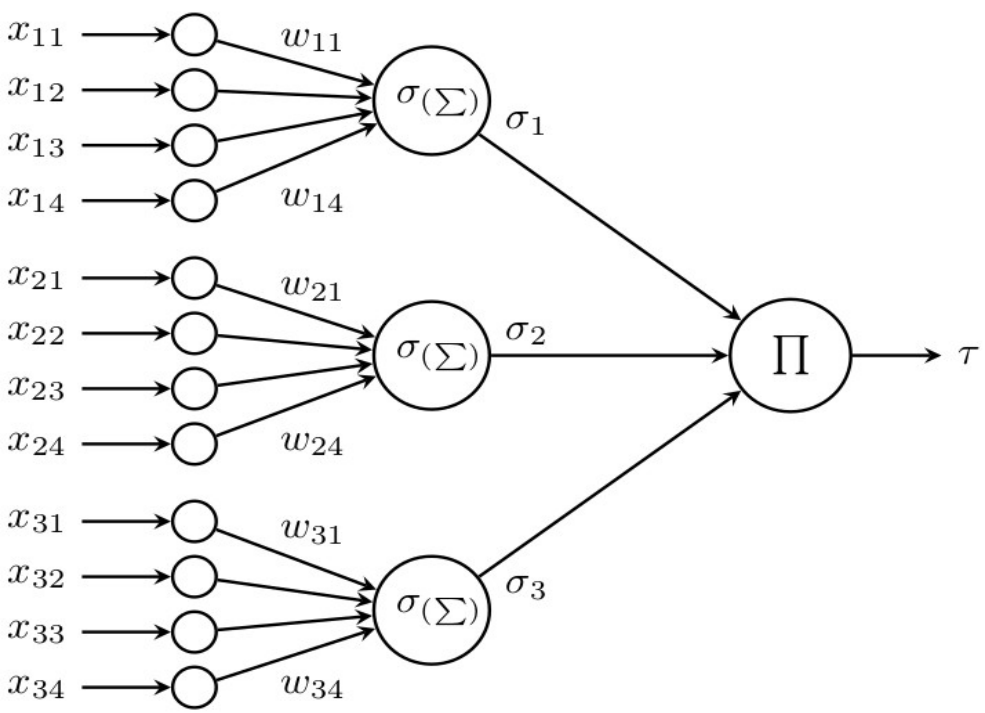
→ **K**: Número de neurônios na camada escondida
→ **N**: Número de entradas para cada neurônio
→ **L**: Faixa de valores possíveis para os pesos sinápticos



→ ***Tree Parity Machine***

→ Exemplo:

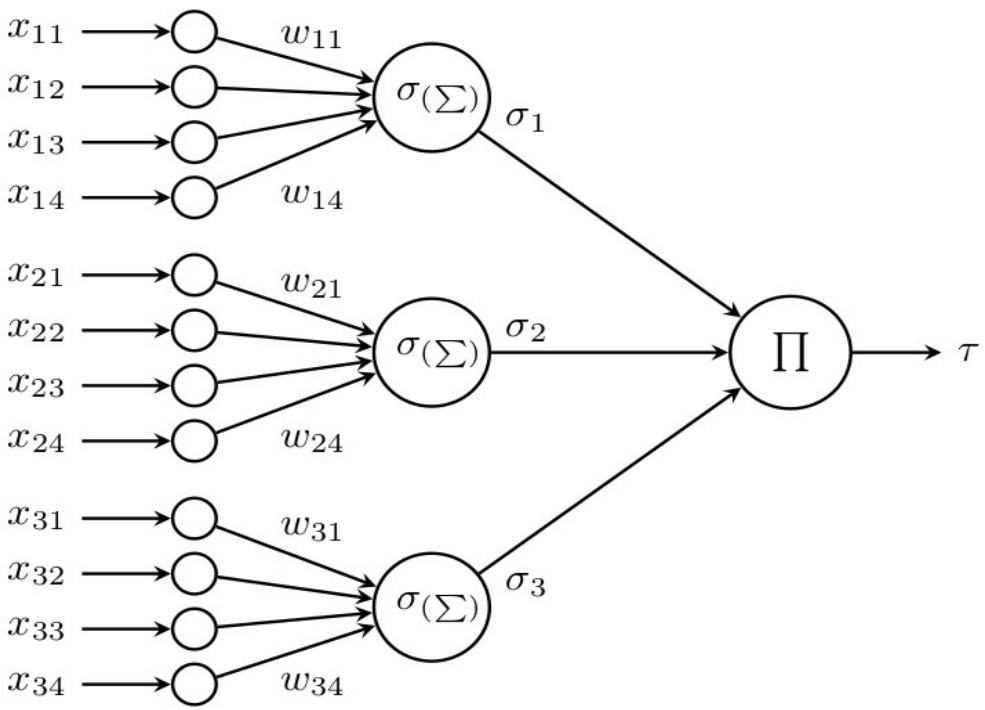
→ K = 3
→ N = 4



→ ***Tree Parity Machine***

→ Saída:

$$\tau^{A/B} = \prod_{k=1}^{K} \sigma_k^{A/B} = \prod_{k=1}^{K} \sigma \left(\sum_{n=1}^{N} w_{k,n}^{A/B} \times x_{k,n}^{A/B} \right)$$



Revisão Bibliográfica

Revisão Bibliográfica

Inatel
Instituto Nacional de Telecomunicações

→ Gerar chaves utilizando características **biométricas** como fonte de **entropia**

→ Características consideradas **únicas** obtidas em seres vivos
→ Tornam o procedimento **mais aleatório**
→ Estreitamente **dependente** de entradas externas

→ **Monrose et al. (2001)**

→ Captura de voz
→ Impressão digital

→ **Chang et al. (2004)**

→ Captura de imagens faciais
→ Identificação de iris

Revisão Bibliográfica

Inatel
Instituto Nacional de Telecomunicações

→ Em 2007, **Ruttor** propôs a técnica de sincronização entre *Tree Parity Machines* baseando-se em seus aprendizados mútuos

→ Os pesos sinápticos são **inicializados aleatoriamente**
→ Saídas eram compartilhadas
→ Caso as saídas coincidissem, a **regra de aprendizado** era aplicada
→ O **critério de parada** era a igualdade de ambos os vetores de pesos sinápticos

→ Estudo com relação aos principais ataques:

→ Ataque simples
→ Ataque de maioria
→ Ataque geométrico
→ Ataque genético

Revisão Bibliográfica

→ **Piazentin** realizou um estudo baseado em Ruttor no ano de 2011

→ Foram analisados os parâmetros em relação a segurança aos ataques:
→ **K**: Número de neurônios na camada escondida
→ **N**: Número de entradas para cada neurônio
→ **L**: Faixa de valores possíveis para os pesos sinápticos

→ O próprio autor afirma que o **desempenho não pôde ser aferido**
→ Utilização de linguagem de alto nível (**Python**)
→ Não foi possível definir uma **configuração ideal** para os parâmetros estudados

Revisão Bibliográfica

Inatel
Instituto Nacional de Telecomunicações

→ **Revankar et al.** propôs um mecanismo de **entrada dinâmica** em 2010

→ As entradas **dependem do estado atual** da *Tree Parity Machine*

$$h_k = \frac{1}{\sqrt{N}} \times \sum_{l=1}^{L} (c_{k,+l} - c_{k,-l})$$

→ A **sincronização** utilizando as consultas propostas ocorreu **mais rápida**

→ Quantidade de **informação trocada** entre as redes foi **maior**

→ T**empo total de geração da chave foi maior** do que quando utilizados vetores de entrada pseudoaleatórios

→ **Allam e Abbas** (2010)

→ Técnica de transmissão de **conteúdo falso** durante o processo de sincronização

→ Durante a sincronização, são enviadas mensagens errônias baseadas nas **distâncias estimadas** entre os pesos sinápticos das *Tree Parity Machines*

→ Evita vários tipos de ataques

$$\left| h_k^{A/B} \right| = \left| \sum_{n=1}^{N} (w_{k,n}^{A/B} \times x_{k,n}^{A/B}) \right|$$

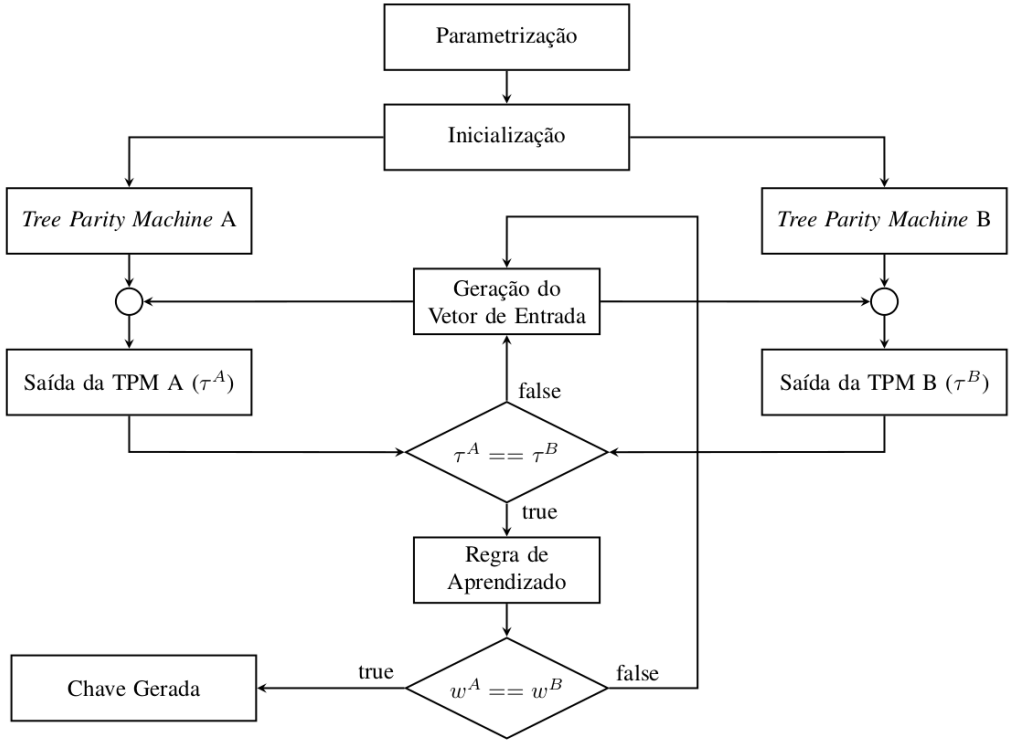
Proposta

Proposta

Inatel
Instituto Nacional de Telecomunicações

- → **Implementar** a rede neural artificial *Tree Parity Machine*
- → Utilizar linguagem de programação **C**
- → **Sincronizar** duas *Tree Parity Machines*
- → Gerar chaves criptográficas binárias como resultado do processo
- → Realizar **experimentos** com o objetivo de otimizar o processo

Proposta


Parametrização
Inicialização
Tree Parity Machine A
Tree Parity Machine B
Geração do Vetor de Entrada
Saída da TPM A (τ^A)
Saída da TPM B (τ^B)
false
$\tau^A == \tau^B$
true
Regra de Aprendizado
Chave Gerada
true
$w^A == w^B$
false

Metodologia

Metodologia

→ **Regras de Aprendizado**

→ *Hebbian*

$$W_{k,n}^{A/B} = w_{k,n}^{A/B} + x_{k,n}\tau^{A/B}\Theta(\tau^{A/B}\sigma_k^{A/B})\Theta(\tau^A\tau^B)$$

→ Anti-*Hebbian*

$$W_{k,n}^{A/B} = w_{k,n}^{A/B} - x_{k,n}\sigma_k^{A/B}\Theta(\tau^{A/B}\sigma_k^{A/B})\Theta(\tau^A\tau^B)$$

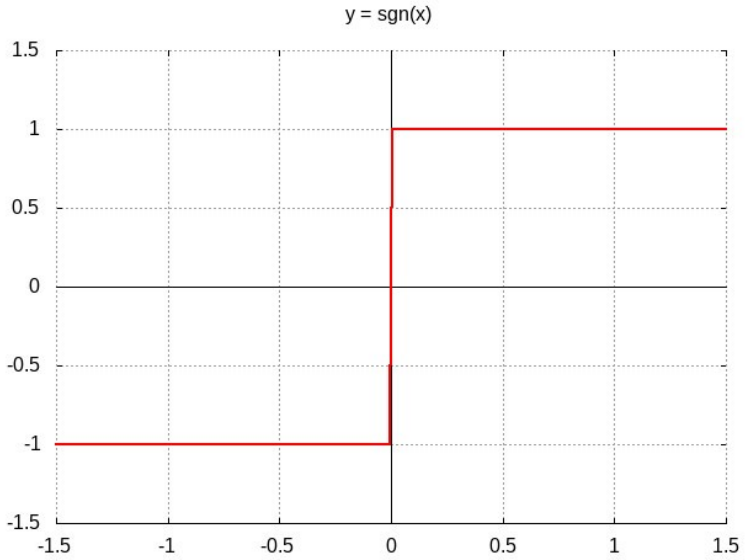
→ *Random Walk*

$$W_{k,n}^{A/B} = w_{k,n}^{A/B} + x_{k,n}\Theta(\tau^{A/B}\sigma_k^{A/B})\Theta(\tau^A\tau^B)$$

→ **Funções de Ativação**

→ Sinal

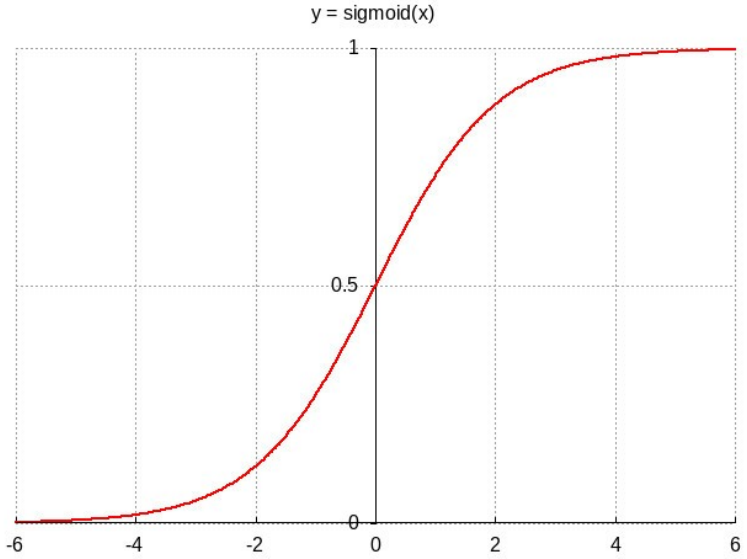
$$\varphi(x) := \begin{cases} -1 & \text{if } x \leq 0 \\ +1 & \text{if } x > 0 \end{cases}$$



→ **Funções de Ativação**

→ Sigmóide

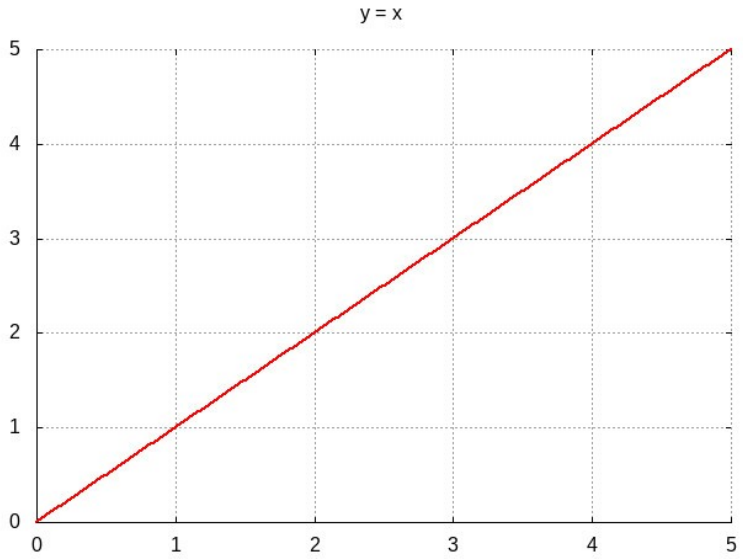
$$\varphi(x) = \frac{1}{1 + e^{-x}}$$



→ **Funções de Ativação**

→ Linear

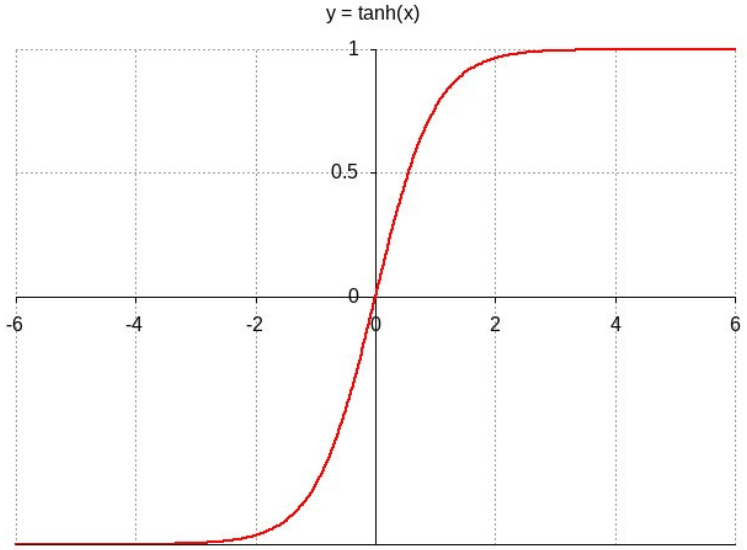
$$\varphi(x) = x$$



→ **Funções de Ativação**

→ Tangente Hiperbólica

$$\varphi(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}}$$



Metodologia

Inatel
Instituto Nacional de Telecomunicações

→ **Integridade dos Dados**

→ **Semente** de geração pseudo-aleatória fixada

→ Cada configuração de *Tree Parity Machine* gerou **100 chaves consecutivas**

→ Foram utilizadas chaves de **1Kib** (1024 bits)

→ As métricas fazem referência à média aritmética dos valores obtidos no processo de geração de cada uma das 100 chaves

Metodologia

Inatel
Instituto Nacional de Telecomunicações

→ **Métricas: Chaves repetidas**

→ Número de chaves repetidas em cada conjunto

→ Probabilidade de ocorrência de cada chave

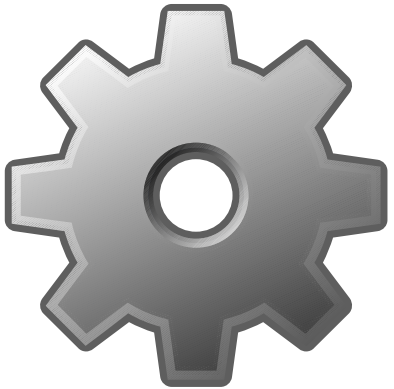
$$P_k[\%] = \frac{1}{2^{(K \times N)}} \times 100$$

Metodologia

Inatel
Instituto Nacional de Telecomunicações

→ **Métricas: Épocas de Treinamento**

→ Máximo
→ Mínimo
→ Média



→ **Métricas: Volume de dados**

→ Volume de dados trocados entre as duas *Tree Parity Machines* (em Bytes)

$$V[Bytes] = \frac{epochs\_avg \times [(K \times N) + K + 2]}{8}$$

Metodologia

→ **Métricas: Comprimento do vetor de entrada**

$$I_{[K,N]} = (K \times N) + K$$

Metodologia

→ **Métricas: Tempo de geração**

→ Máximo
→ Mínimo
→ Média

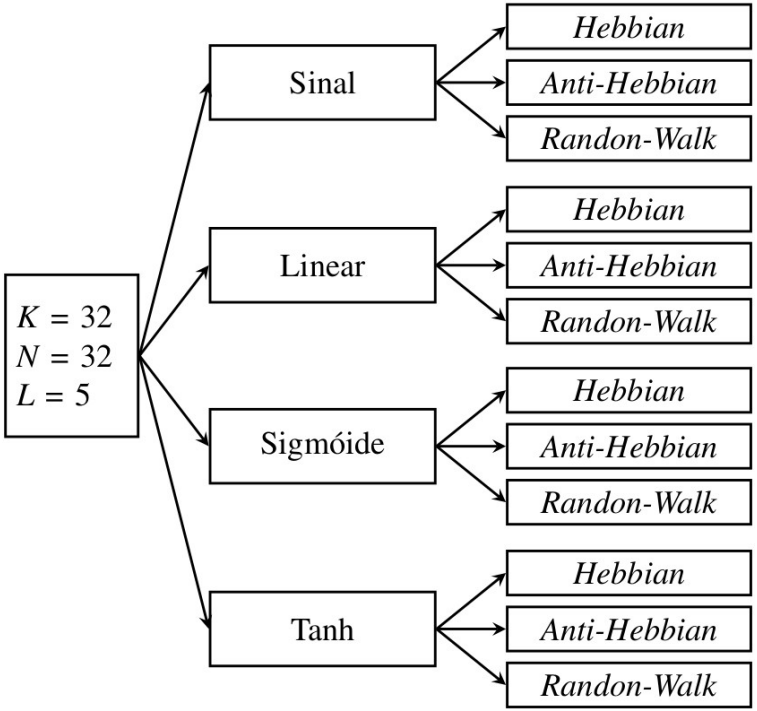
- Sistema Operacional: Xubuntu
- Processador: Intel(R) Core(TM) i7-5500U
- Clock Rate: 2.40 GHz
- Arquitetura: x86_64
- Núcleos: 4
- Memória RAM: 16 GB

Experimentos e Resultados

Experimento 1

Experimento 1

→ **Aferir influência das regras de aprendizado**

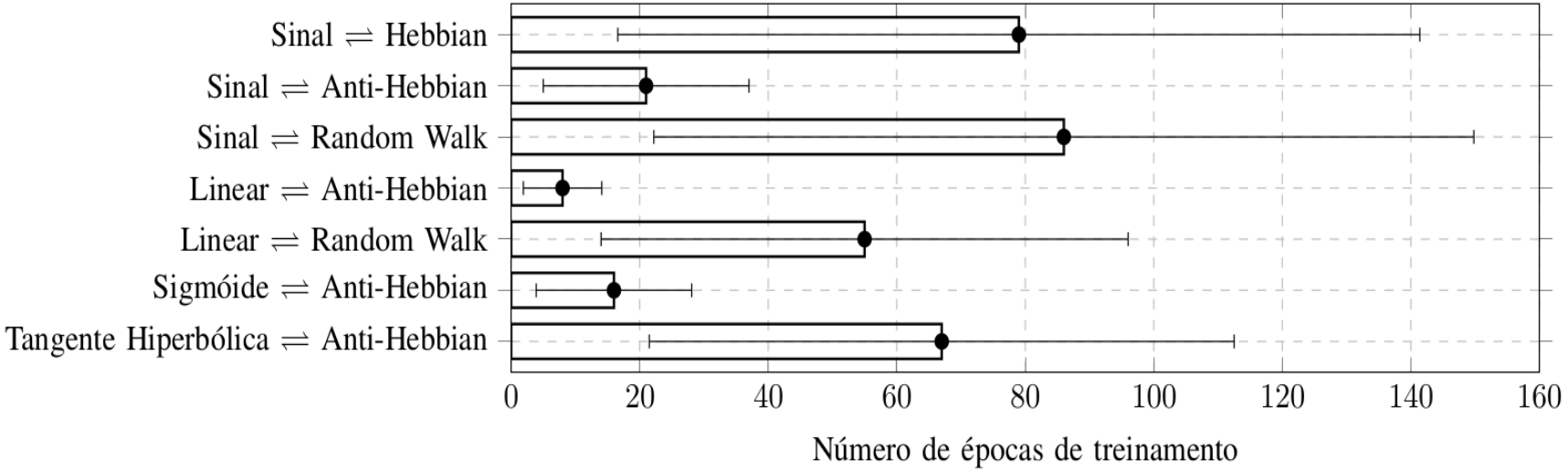


Experimento 1

Configurações descartadas nas análises		
Função de Ativação	Regra de Aprendizado	Motivo do Descarte
Sigmóide	*Random Walk*	Não convergiu
Tangente Hiperbólica	*Random Walk*	Não convergiu
Sigmóide	*Hebbian*	Chaves repetidas
Linear	*Hebbian*	Chaves repetidas
Tangente Hiperbólica	*Hebbian*	Chaves repetidas

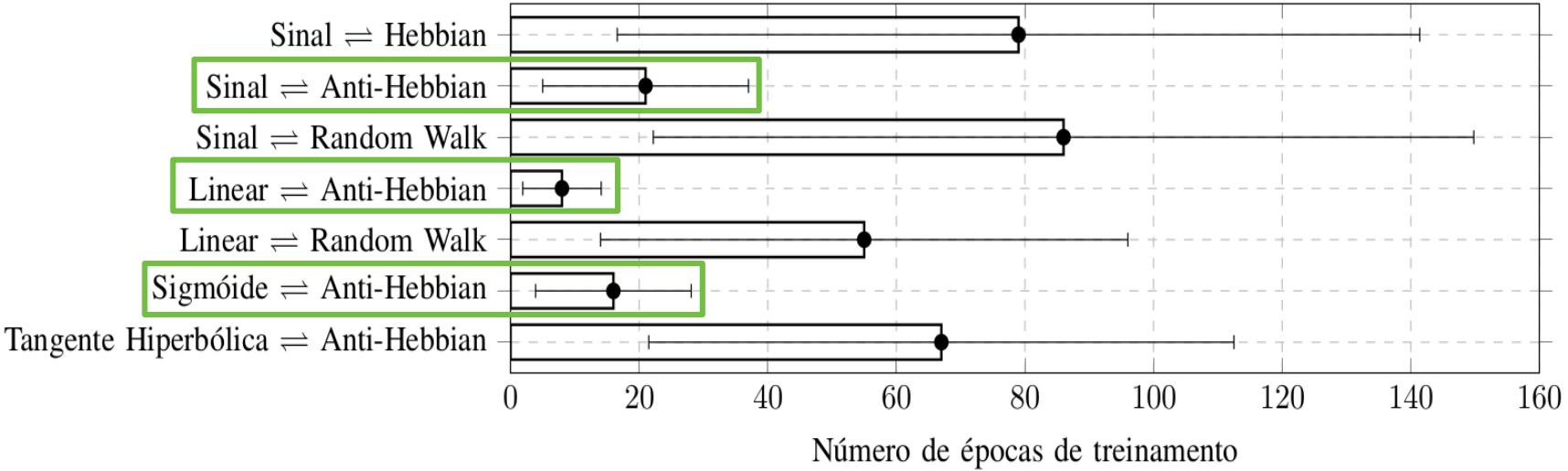
Experimento 1

Inatel
Instituto Nacional de Telecomunicações



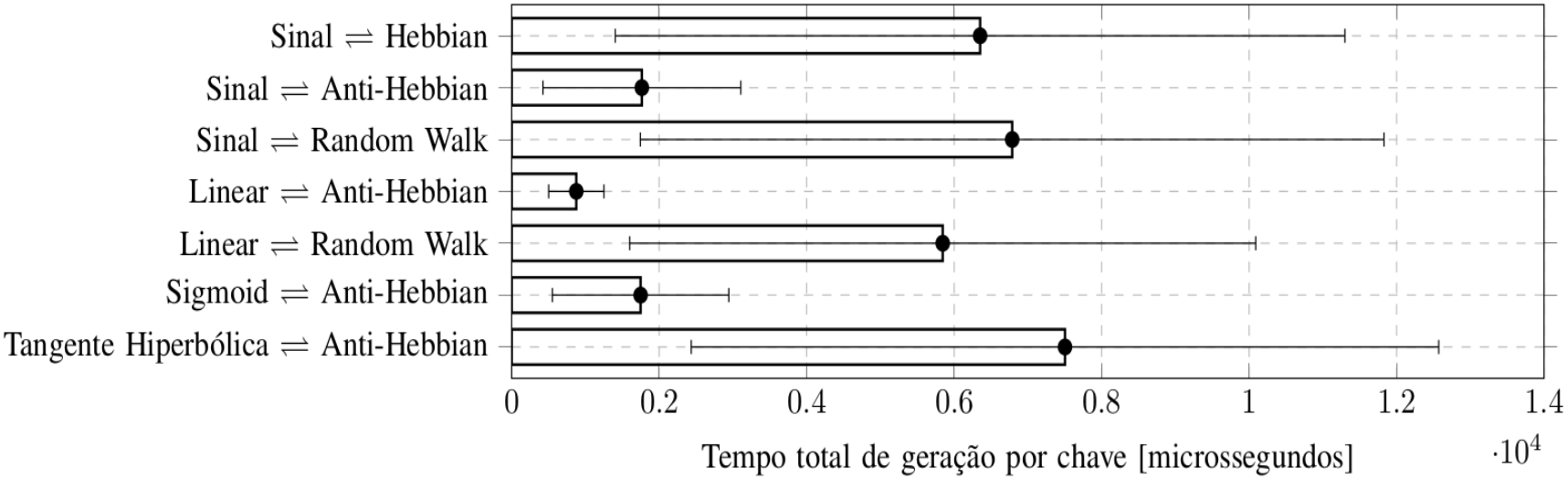
Experimento 1

Inatel
Instituto Nacional de Telecomunicações



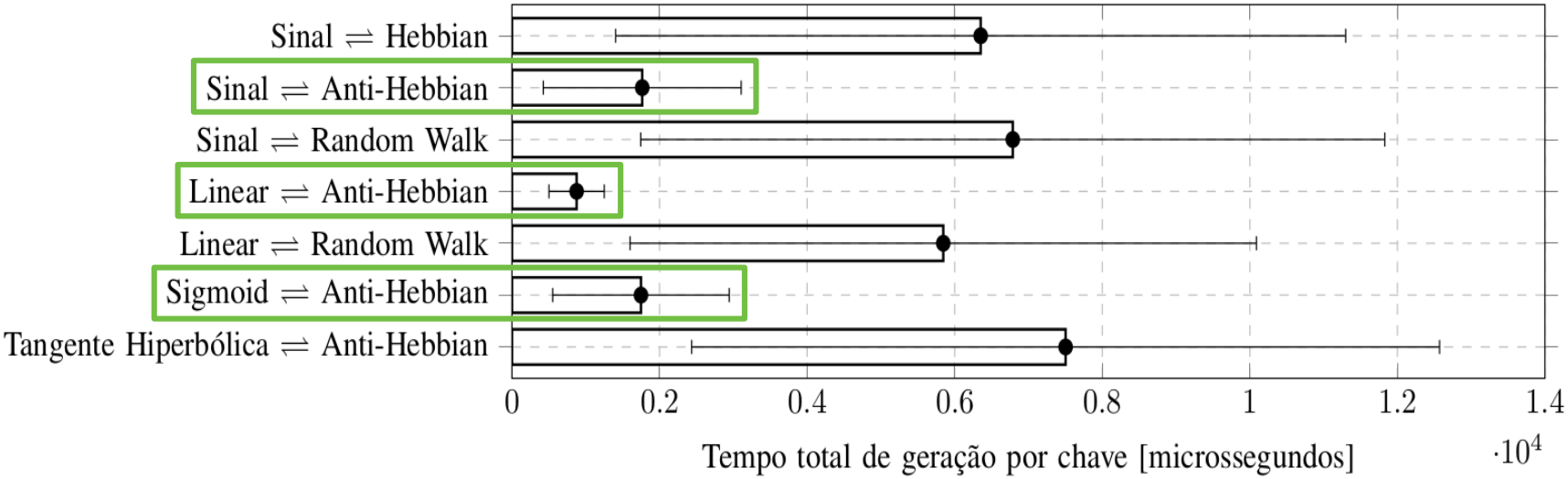
Experimento 1

Inatel
Instituto Nacional de Telecomunicações



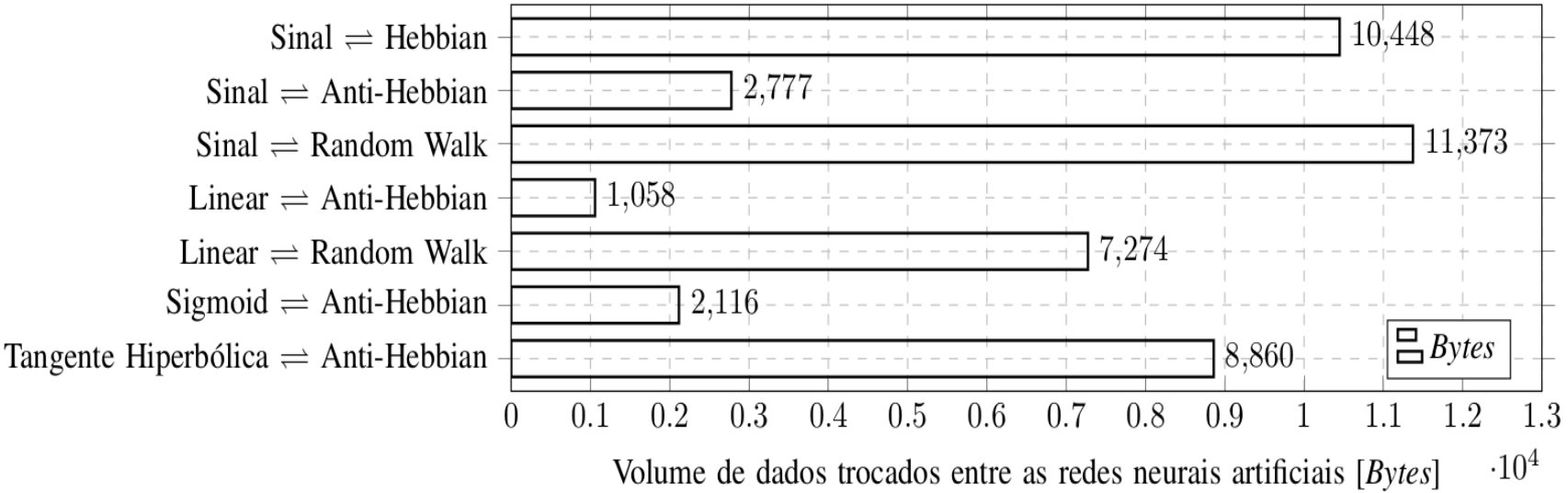
Experimento 1

Inatel
Instituto Nacional de Telecomunicações



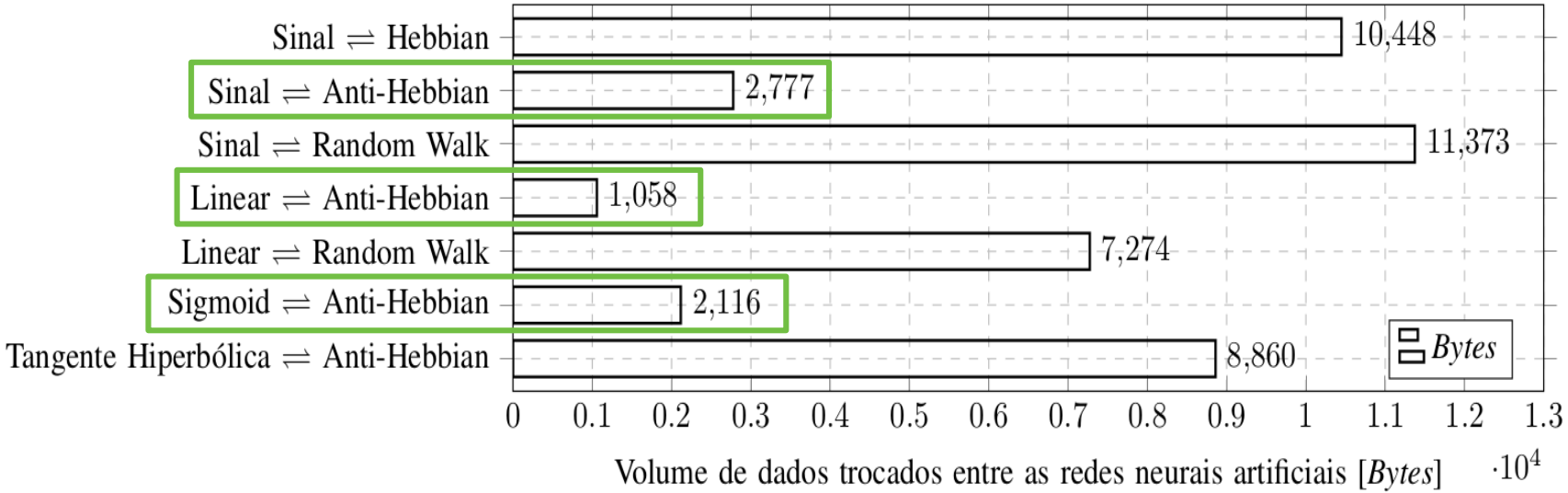
Experimento 1

Inatel
Instituto Nacional de Telecomunicações



Experimento 1

Inatel
Instituto Nacional de Telecomunicações



Experimento 1

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 1										
Função de Ativação	Regra de Aprendizado	Número de Épocas				Tempo [microssegundos]				Volume de Dados [*Bytes*]
		min	max	médio	σ	min	max	médio	σ	
Sinal	*Hebbian*	45	118	79	16.6	4007	12284	6352	1404.7	10448
	Anti-Hebbian	10	32	21	5	1085	4027	1765	423.9	2777
	Random Walk	45	178	86	22.2	3743	13932	6787	1745.2	11373
Linear	*Anti-Hebbian*	4	12	8	1.9	449	2969	876	501.6	1058
	Random Walk	30	95	55	14	3149	11533	5845	1600.6	7274
Sigmóide	*Anti-Hebbian*	9	26	16	3.9	1003	4453	1748	551.9	2116
Tangente Hiperbólica	*Anti-Hebbian*	32	141	67	21.5	3611	15981	7503	2434.7	8860

Experimento 1

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 1										
Função de Ativação	Regra de Aprendizado	Número de Épocas				Tempo [microssegundos]				Volume de Dados [*Bytes*]
		min	max	médio	σ	min	max	médio	σ	
Sinal	*Hebbian*	45	118	79	16.6	4007	12284	6352	1404.7	10448
	Anti-Hebbian	10	32	21	5	1085	4027	1765	423.9	2777
	Random Walk	45	178	86	22.2	3743	13932	6787	1745.2	11373
Linear	*Anti-Hebbian*	4	12	8	1.9	449	2969	876	501.6	1058
	Random Walk	30	95	55	14	3149	11533	5845	1600.6	7274
Sigmóide	*Anti-Hebbian*	9	26	16	3.9	1003	4453	1748	551.9	2116
Tangente Hiperbólica	*Anti-Hebbian*	32	141	67	21.5	3611	15981	7503	2434.7	8860

Experimento 1

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 1										
Função de Ativação	Regra de Aprendizado	Número de Épocas				Tempo [microssegundos]				Volume de Dados [*Bytes*]
		min	max	médio	σ	min	max	médio	σ	
Sinal	*Hebbian*	45	118	79	16.6	4007	12284	6352	1404.7	10448
	Anti-Hebbian	10	32	21	5	1085	4027	1765	423.9	2777
	Random Walk	45	178	86	22.2	3743	13932	6787	1745.2	11373
Linear	*Anti-Hebbian*	4	12	8	1.9	449	2969	876	501.6	1058
	Random Walk	30	95	55	14	3149	11533	5845	1600.6	7274
Sigmóide	*Anti-Hebbian*	9	26	16	3.9	1003	4453	1748	551.9	2116
Tangente Hiperbólica	*Anti-Hebbian*	32	141	67	21.5	3611	15981	7503	2434.7	8860

Experimento 1

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 1										
Função de Ativação	Regra de Aprendizado	Número de Épocas				Tempo [microssegundos]				Volume de Dados [*Bytes*]
		min	max	médio	σ	min	max	médio	σ	
Sinal	*Hebbian*	45	118	79	16.6	4007	12284	6352	1404.7	10448
	Anti-Hebbian	10	32	21	5	1085	4027	1765	423.9	2777
	Random Walk	45	178	86	22.2	3743	13932	6787	1745.2	11373
Linear	*Anti-Hebbian*	4	12	8	1.9	449	2969	876	501.6	1058
	Random Walk	30	95	55	14	3149	11533	5845	1600.6	7274
Sigmóide	*Anti-Hebbian*	9	26	16	3.9	1003	4453	1748	551.9	2116
Tangente Hiperbólica	*Anti-Hebbian*	32	141	67	21.5	3611	15981	7503	2434.7	8860

Experimento 1

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 1										
Função de Ativação	Regra de Aprendizado	Número de Épocas				Tempo [microssegundos]				Volume de Dados [*Bytes*]
		min	max	médio	σ	min	max	médio	σ	
Sinal	*Hebbian*	45	118	79	16.6	4007	12284	6352	1404.7	10448
	Anti-Hebbian	10	32	21	5	1085	4027	1765	423.9	2777
	Random Walk	45	178	86	22.2	3743	13932	6787	1745.2	11373
Linear	*Anti-Hebbian*	4	12	8	1.9	449	2969	876	501.6	1058
	Random Walk	30	95	55	14	3149	11533	5845	1600.6	7274
Sigmóide	*Anti-Hebbian*	9	26	16	3.9	1003	4453	1748	551.9	2116
Tangente Hiperbólica	*Anti-Hebbian*	32	141	67	21.5	3611	15981	7503	2434.7	8860

Experimento 1

Inatel
Instituto Nacional de Telecomunicações

→ Conjuntos selecionados

[Sinal, Anti-Hebbian]

[Linear, Anti-Hebbian]

[Sigmóide, Anti-Hebbian]

Experimento 1

Inatel
Instituto Nacional de Telecomunicações

→ Conjuntos selecionados

[Sinal,	Anti-Hebbian]
[Linear,	Anti-Hebbian]
[Sigmóide,	Anti-Hebbian]

Regra de aprendizado mais eficiente

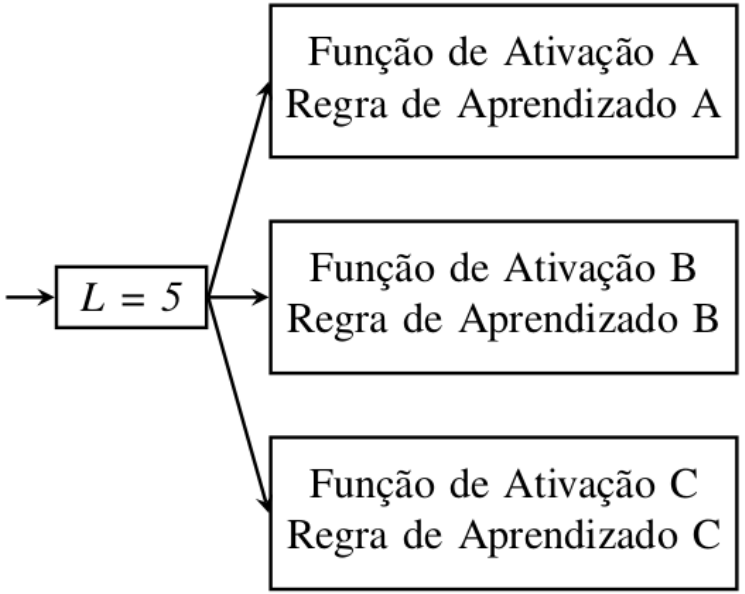
Anti-Hebbian

Experimento 2

Experimento 2

→ **Aferir influência de K e N**

$C_i[k_i, n_i]$	
k_i	n_i
1	1024
2	512
4	256
8	128
16	64
32	32
64	16
128	8
256	4
512	2
1024	1



Experimento 2

Inatel
Instituto Nacional de Telecomunicações

Configurações descartadas nas análises		
Função de Ativação	Regra de Aprendizado	Motivo do Descarte
Sigmóide	*Anti-Hebbian*	Não convergiu
Linear	*Anti-Hebbian*	Chaves repetidas

Experimento 2

Inatel
Instituto Nacional de Telecomunicações

→ Parâmetros ótimos

→ Regra de aprendizado: **Anti-Hebbian**

→ Função de ativação: **Sinal**

Função de ativação mais eficiente

Sinal

Experimento 2

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 2						
$C_i[k_i, n_i]$		Épocas		Tempo [micro]		Volume de Dados [B]
k_i	n_i	médio	σ	médio	σ	
1	1024	15	3.8	1188	308.8	1925
2	512	16	3.1	1210	209.9	2056
4	256	18	3.9	1263	305.2	2317
8	128	18	3.6	1325	306.8	2455
16	64	19	4.5	1570	427.9	2605
32	32	21	5	1453	309	2645
64	16	21	5.2	1575	350.4	2861
128	8	23	5.4	1751	411	3317
256	4	22	5.9	2010	413	3685
512	2	23	5.4	2485	506.7	4421
1024	1	15	3	2431	440.9	3843

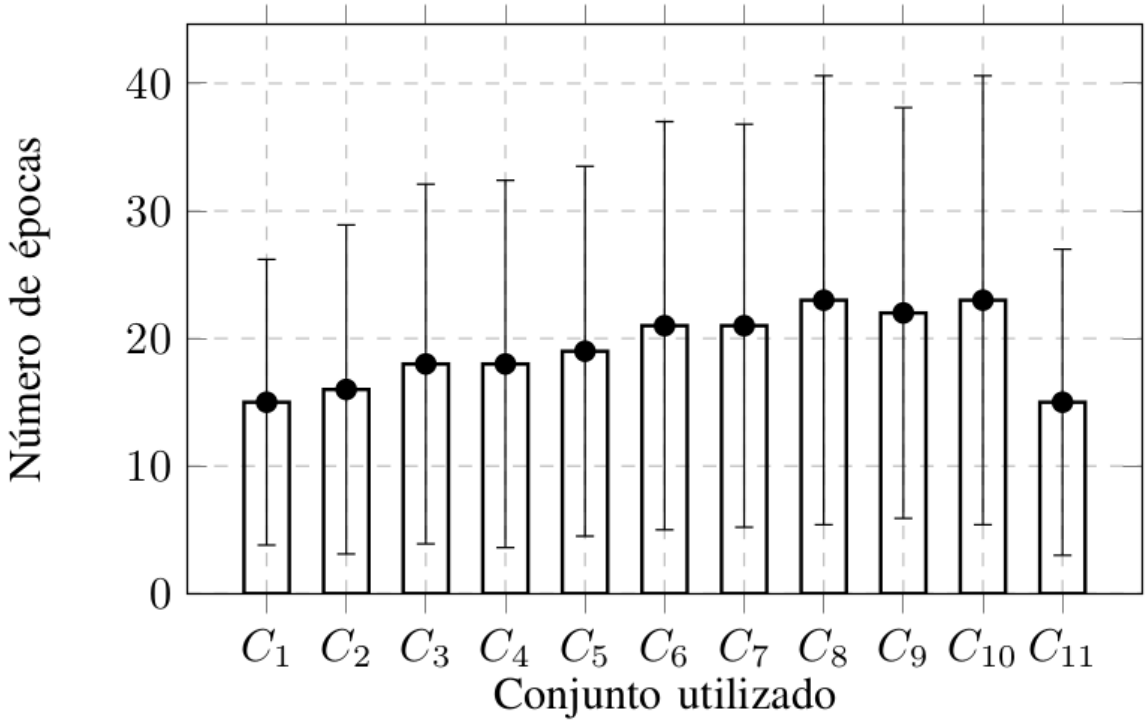
Experimento 2

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 2						
$C_i[k_i, n_i]$		Épocas		Tempo [micro]		Volume de Dados [B]
k_i	n_i	médio	σ	médio	σ	
1	1024	15	3.8	1188	308.8	1925
2	512	16	3.1	1210	209.9	2056
4	256	18	3.9	1263	305.2	2317
8	128	18	3.6	1325	306.8	2455
16	64	19	4.5	1570	427.9	2605
32	32	21	5	1453	309	2645
64	16	21	5.2	1575	350.4	2861
128	8	23	5.4	1751	411	3317
256	4	22	5.9	2010	413	3685
512	2	23	5.4	2485	506.7	4421
1024	1	15	3	2431	440.9	3843

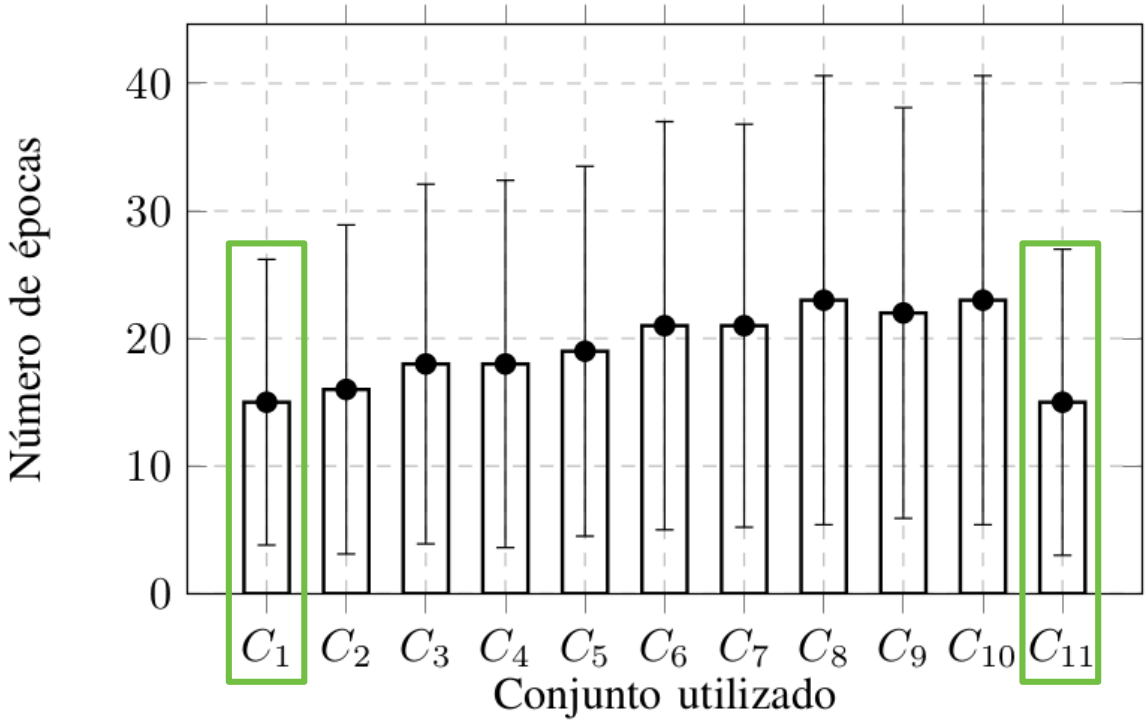
Experimento 2

Inatel
Instituto Nacional de Telecomunicações



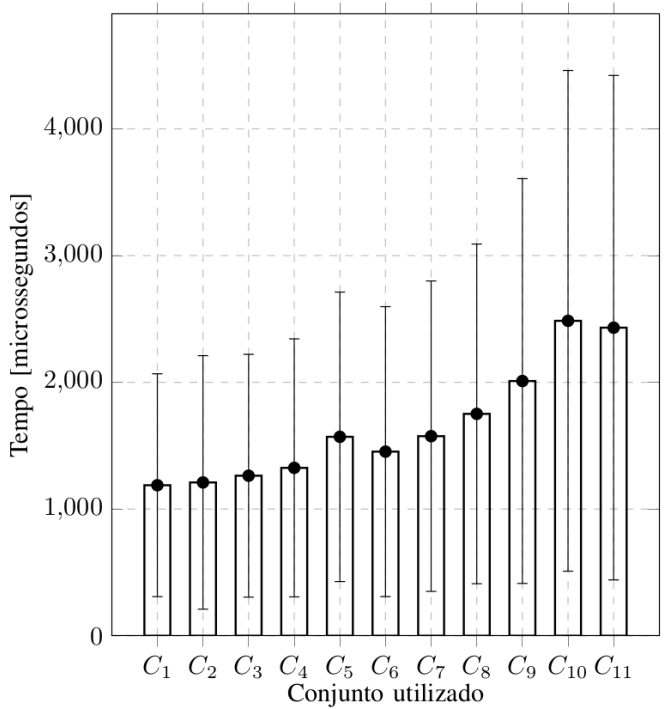
Experimento 2

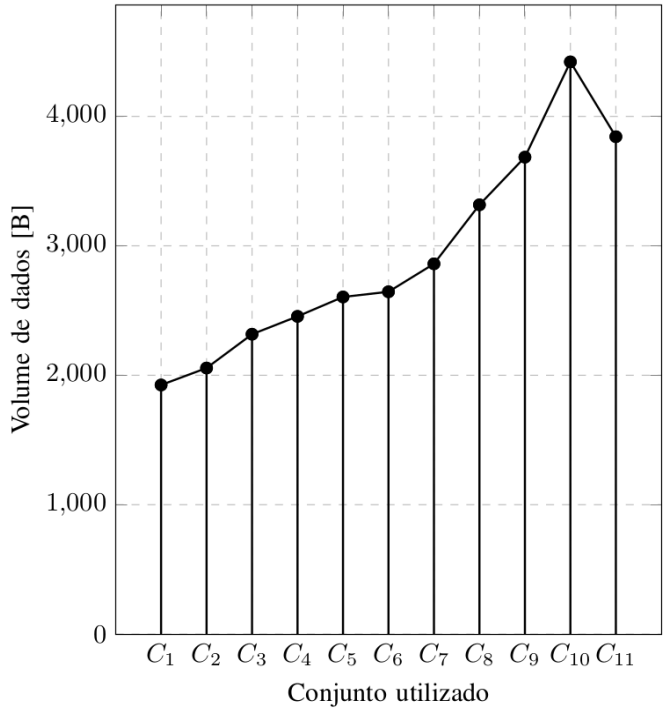
Inatel
Instituto Nacional de Telecomunicações



Experimento 2

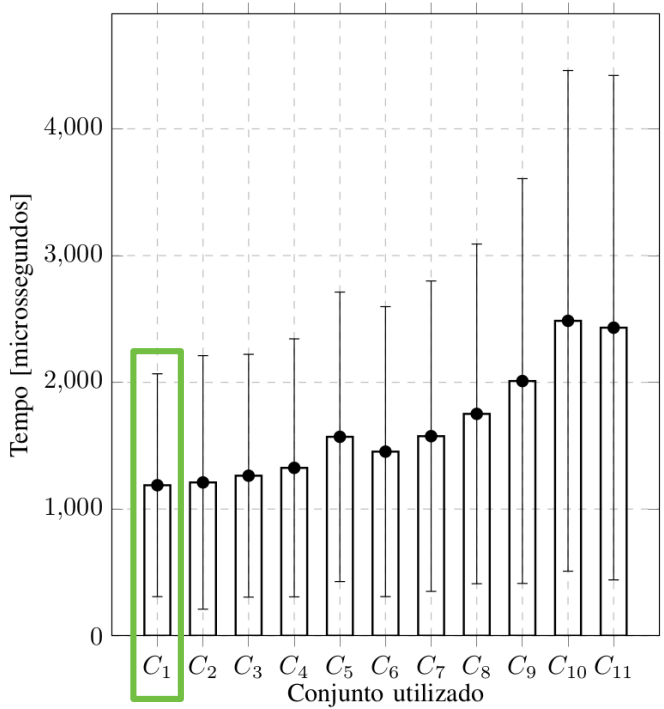
Inatel
Instituto Nacional de Telecomunicações

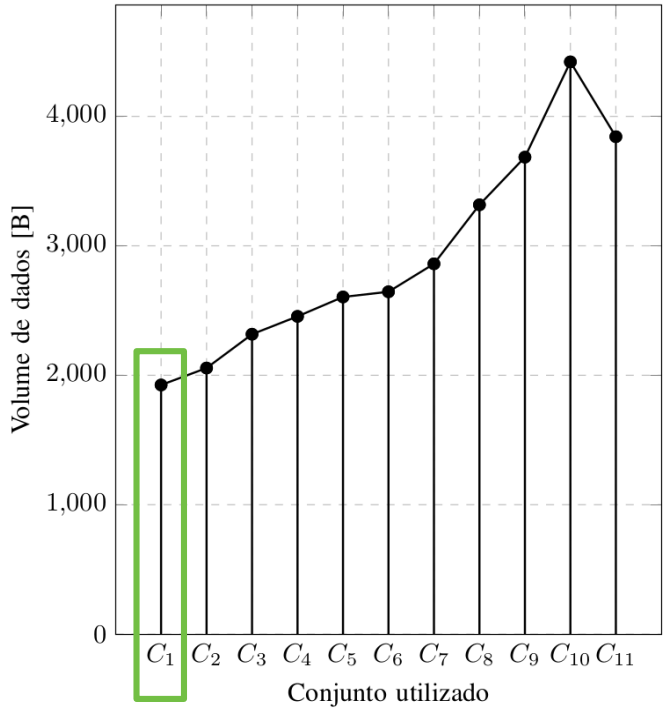




Experimento 2

Inatel
Instituto Nacional de Telecomunicações





Experimento 2

Inatel
Instituto Nacional de Telecomunicações

→ Influência do BIAS

$$I_{[K,N]} = (K \times N) + K$$

$$I_{[1,1024]} = (1024 \times 1) + 1 = 1025$$

$$I_{[1024,1]} = (1 \times 1024) + 1024 = 2048$$

Experimento 2

Inatel
Instituto Nacional de Telecomunicações

→ Influência do BIAS

$$V[Bytes] = \frac{epochs\_avg \times [(K \times N) + K + 2]}{8}$$

$$V_{[1,1024]} = \frac{15 \times [(1 \times 1024) + 1 + 2]}{8} = 1925[B]$$

$$V_{[1024,1]} = \frac{15 \times [(1024 \times 1) + 1024 + 2]}{8} = 3843[B]$$

Experimento 2

Inatel
Instituto Nacional de Telecomunicações

→ Parâmetros ótimos

→ Regra de aprendizado: **Anti-Hebbian**
→ Função de ativação: **Sinal**
→ K: **1**
→ N: **1024** (Comprimento da chave)

Parâmetro **K** mais eficiente: **1**

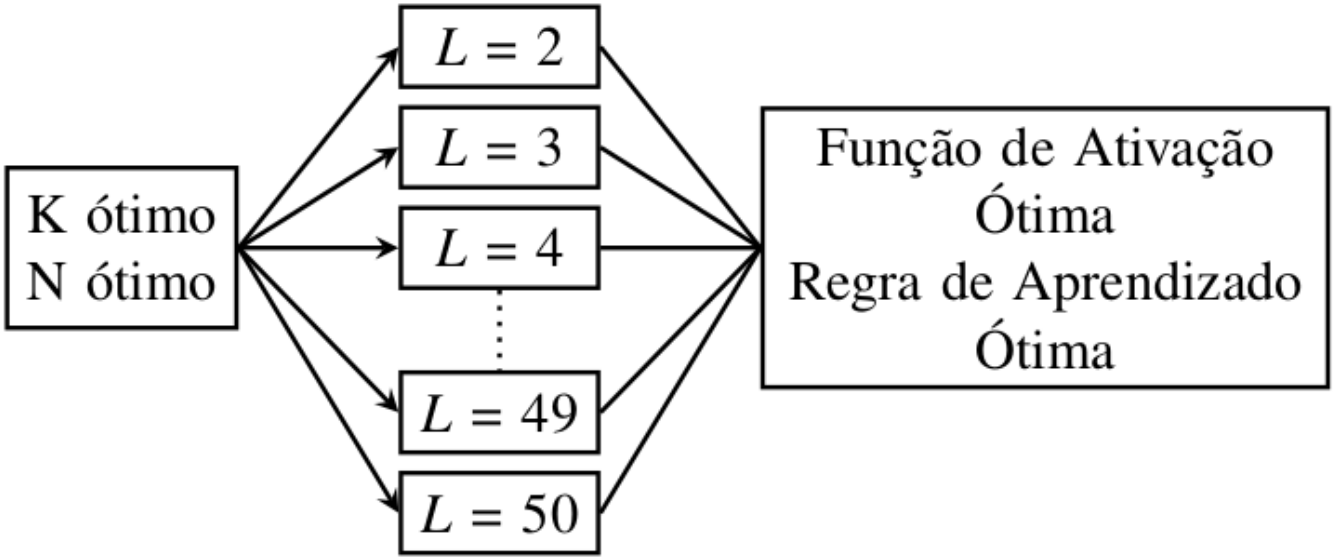
Parâmetro **N** mais eficiente: **1024**

Experimento 3

Experimento 3

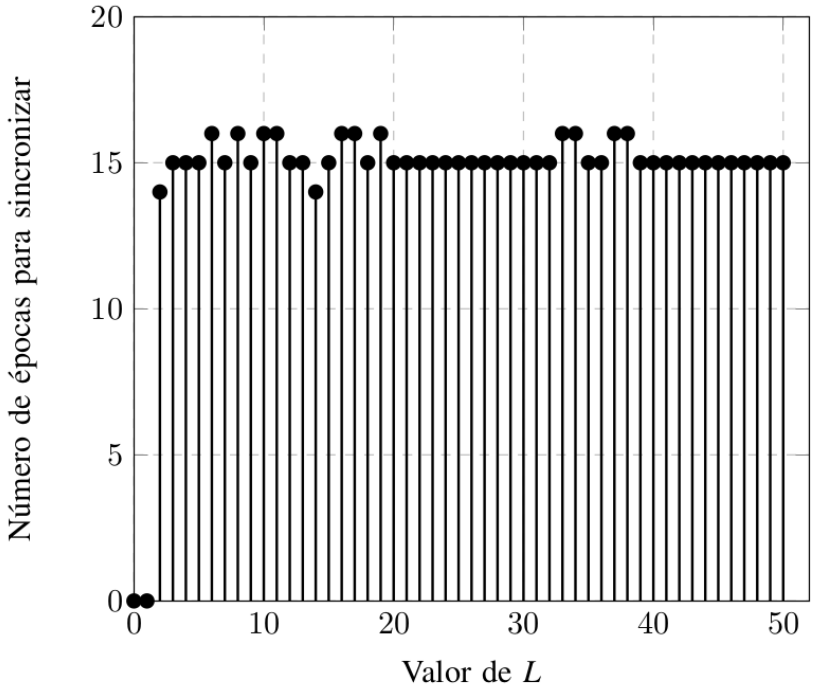
Inatel
Instituto Nacional de Telecomunicações

→ **Aferir influência de L**



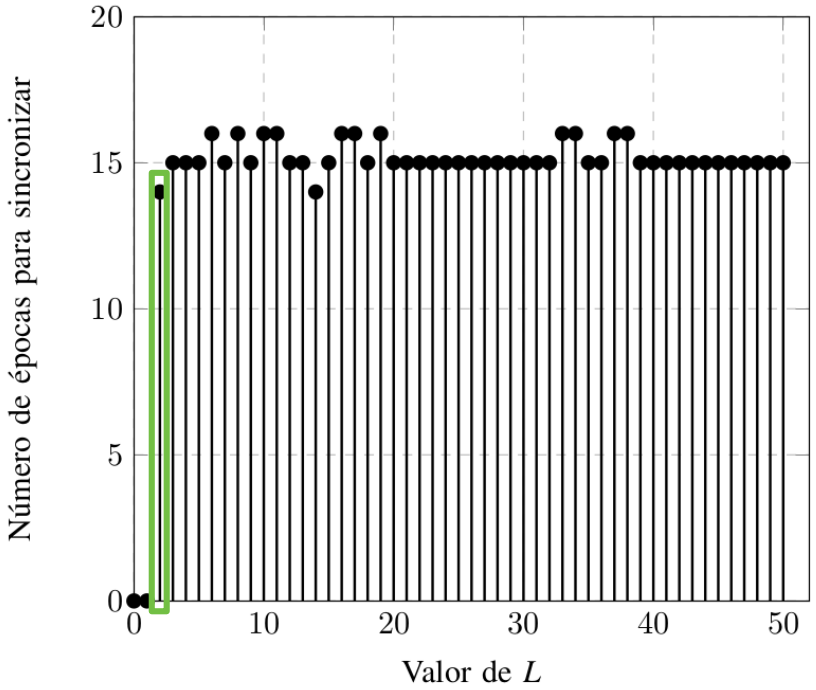
Experimento 3

Inatel
Instituto Nacional de Telecomunicações



Experimento 3

Inatel
Instituto Nacional de Telecomunicações



Experimento 3

Inatel
Instituto Nacional de Telecomunicações

→ Parâmetros ótimos

→ Regra de aprendizado: **Anti-Hebbian**
→ Função de ativação: **Sinal**
→ K: **1**
→ N: **1024** (Comprimento da chave)
→ L: **2**

Parâmetro **L** adotado: **2**

Experimento 4

Experimento 4

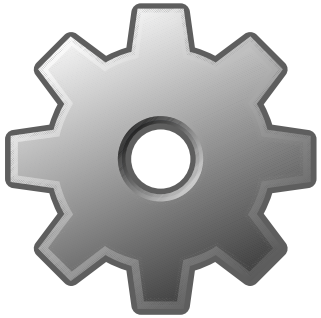
Inatel
Instituto Nacional de Telecomunicações

→ Parâmetros já foram individualmente analisádos

→ Gerar chaves criptográficas binárias de **10Kib** (10.240 bits)

→ Grupo 1 de **1.000 chaves**

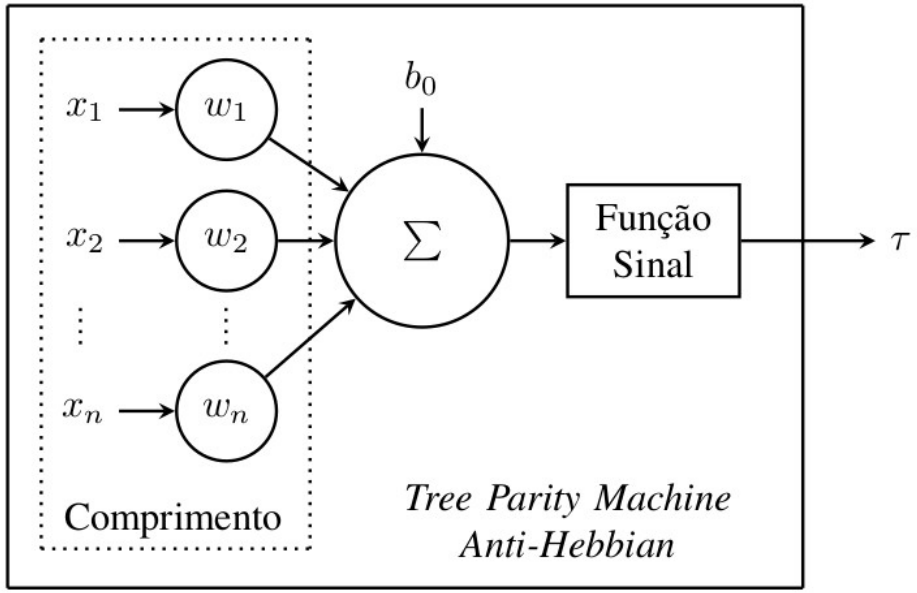
→ Grupo 2 de **10.000 chaves**



Experimento 4

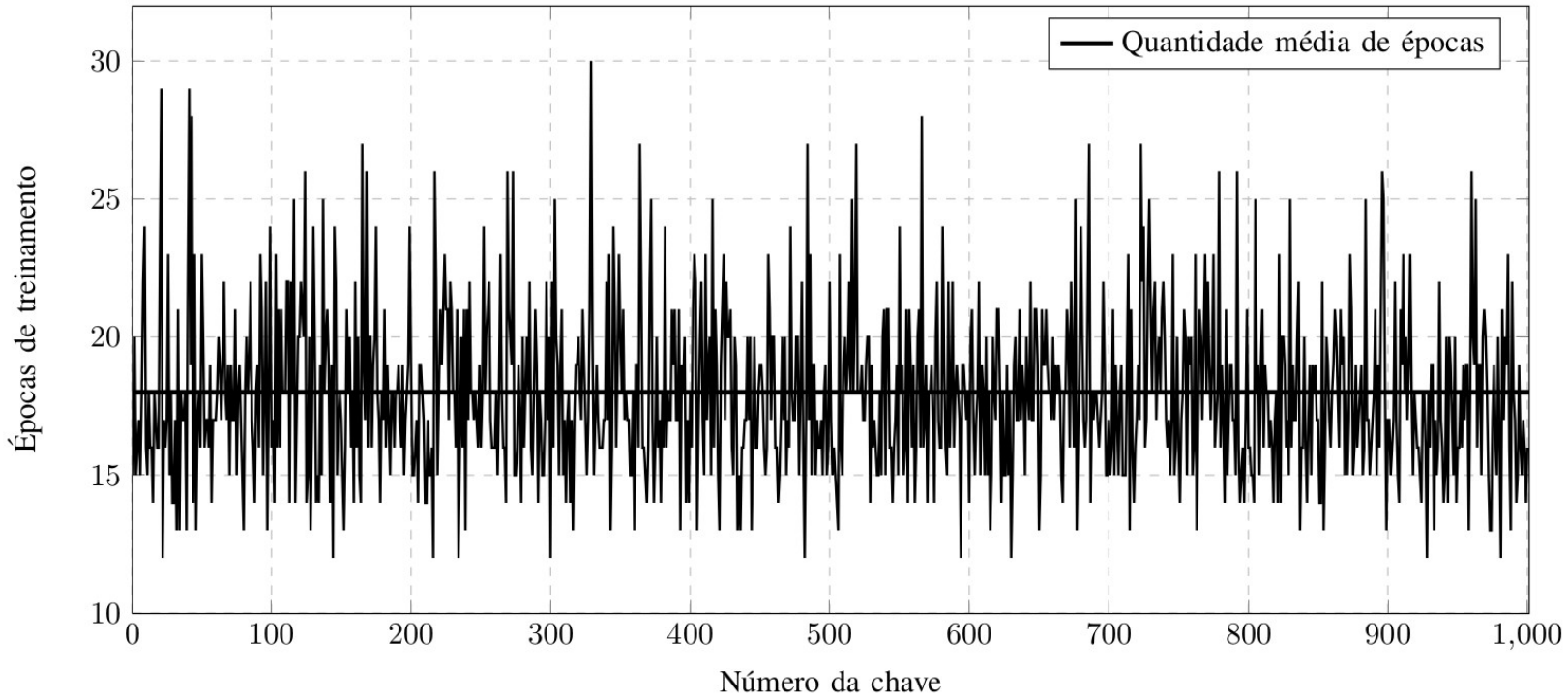
Inatel
Instituto Nacional de Telecomunicações

→ Estrutura ótima



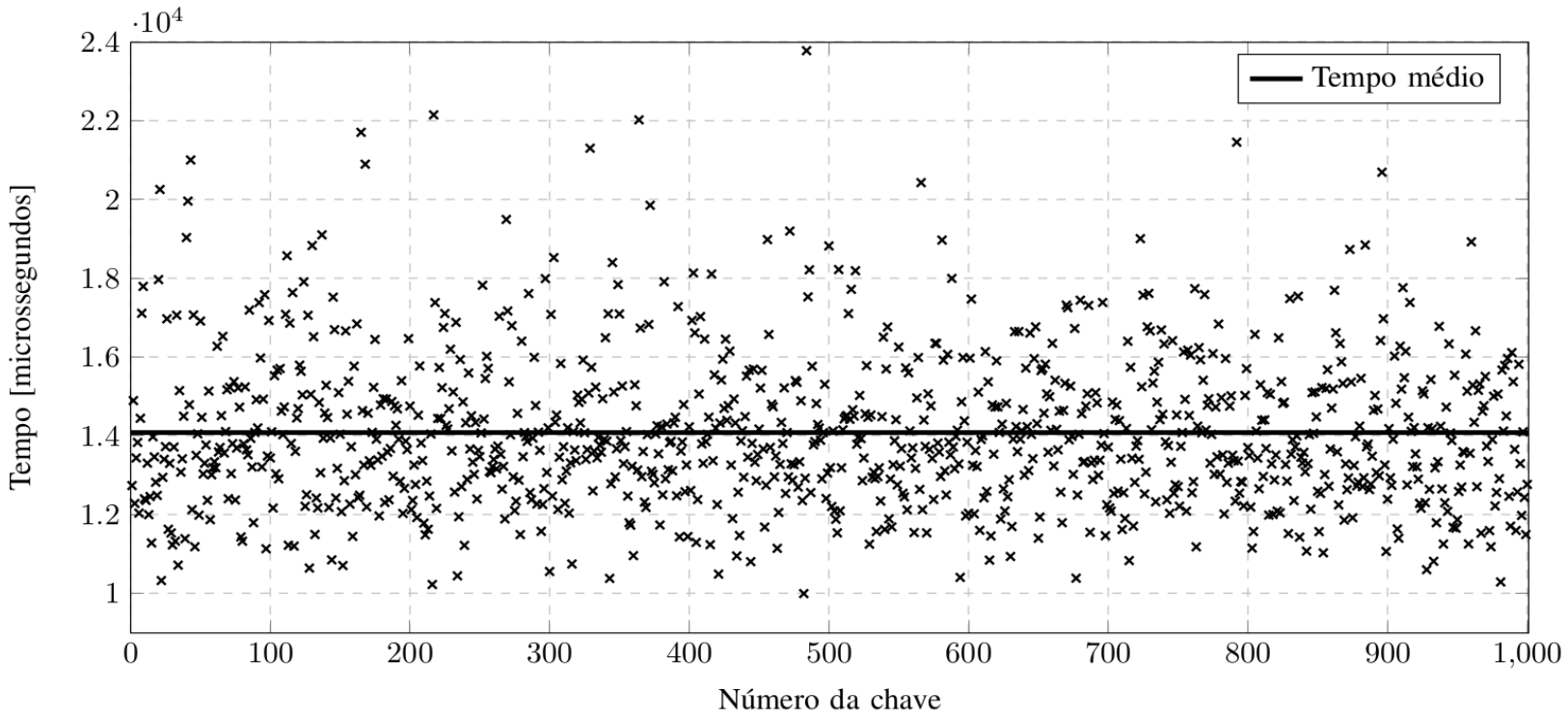
Experimento 4

Inatel
Instituto Nacional de Telecomunicações



Experimento 4

Inatel
Instituto Nacional de Telecomunicações



Experimento 4

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 4											
Configuração Ótima	Número de Chaves	Número de Épocas				Tempo [microssegundos]				Volume de Dados [B]	Chaves Repetidas
		min	max	médio	σ	min	max	médio	σ		
$K = 1$ $N = 10240$ $L = 2$ Sinal *Anti-Hebbian*	1000	12	30	18	3	9991	23778	14080	1928.6	23046	0
	10000	11	42	18	3	9673	24824	14016	1865	23046	0

Experimento 4

Inatel
Instituto Nacional de Telecomunicações

Resultados do Experimento 4											
Configuração Ótima	Número de Chaves	Número de Épocas				Tempo [microssegundos]				Volume de Dados [B]	Chaves Repetidas
		min	max	médio	σ	min	max	médio	σ		
$K = 1$ $N = 10240$ $L = 2$ Sinal *Anti-Hebbian*	1000	12	30	18	3	9991	23778	14080	1928.6	23046	0
	10000	11	42	18	3	9673	24824	14016	1865	23046	0

Experimento 4

Inatel
Instituto Nacional de Telecomunicações

Experimento 4

Inatel
Instituto Nacional de Telecomunicações

A2709E6F57D99F5E39FF8FF3E3F5FEBDB57F76DF6A16BFFF3B1D87CF510FB9FC6FEE06F6EA8EF7DB1EF7FFCF3F393FC32BFEE7FF6E3D75A8F
B2E8C77DEF113F7D7FD95FF4C63D5FBDBFEFE7F8E49D4CF7DF6FF6F9DBFFEE667C1DF7ADCEE38F7FAB9F46FFFED75FBDEDBFFB0CC3EDBF
7BF77E5F9EDBDF727FFF8BB6FB257CF2BDF9C86D3CAED9EDEF88FFD09FFF573C7977CEA9FE7B8F039EDF7ADBC427E8EABC8AECFDF97F6D
AFF66FDFBFFB6DAB7F9FD077B079F6FD49D7CD9B3377A33CA725FFEFDB25FFCFFFFCD779A5A13B97F77DDE595C6F9DD5C163E6FBA5FA7F1
BB9F6F054FE339EE7F7DDFC545CBDED30F7ECD33FA56F27F7F6D3FE28F678FFDB77AFD67BDD4FBBA77DF5DCBF8FFDEFFED7B76BAD2CFE7
FE677EBBDCE7FCCE67CF64DEEFF1FFFE77873FB8F19EDBC5655DEAEEB4951EAFFD9BD5769E7C59DDF62FDFFFB32FFDF4725FEDF7DFEBBF
B9EBEBBF71F1FE7D83D8FFD5BCB75F0AE6F3AF6EEAFCEBD0EFD3A6CBECB3AC4ECED17CE67F7F852B441F5B9DBB9D636CE7DFDBDD3EFBE
BBA654DD7B7BE4D763DBFD777BEFE7F6DE2AD47155ED514F3C3C987D2D7DDB6FABF58BB5E949F9AF2BEBFA6BE3D536C79FDDD5BBD6BFFC
F1F2DF49DAF6B0775D685B977FA57B55CE9CFBDBDB67F1ADAC8D67EA2B6ED8DD59B2ED5FFFBA9B2FEAC87EF25FFC5ACF15FFBE72FFBFF9
C35EA6EE2EEEC956DEFED5359FDB49B7CB1CB58E7F53E279F387FFDAA5FF5146FF5DEEFFBA96BBB7B19C0CDFCEF657E17E999D57DD7A7E6
2AD3FB6E57F5EB2F475B35F6FCA79ABFB7F378D42F93FF49FF79655FFBEA67655F6F53BBB8FACE116C9F70FCEDBCB59EFBF7FEEDEBAAF00E
7E57BF8F17F5F75D4C59FF4AD7BEFDB7EBBE74876DADF5DF69532FEA09EFF36DB85953BE82E3BBBF2337BFC976F9E787097B2CBBF7FF7E6EF
39F3FF5B3ED5B5AD8E3F31FDA7371F50C77B3BFEFDE77156E778E4FF4794FBA667BEF01B3DA1EB54DFFFBCEBF5B3DFD0C7F7F7FDC36ADFC
FFD7F5FE27DEEDEFAAF8FD3CA76DC75C7055398EB5EF8BEDFD7493F4FD73C7914E7F3F75BBEFEA533ACE4EBEFBEFEBB2FDB92BB29F3B868
FFD3DB697AFFFF713BCFD661FB174FBE7FD4AFBCFAE5F3BF845D97DDBBD14A4BEAFEE62F5E7A2D44B5F67FD7AAF6F5BF73D7FEE6BCFB6D5
3B66F87AA463BFDBFE34CFBBFA7B6FBE4BC393BFDB1FDEE6F635DEE63B76ABFD2F4B37FFEF978DD34973379325FCF792FDCF5E3E7A65FD72
DE4B7747614D377D8A8D97D7BD9FD6C5D7B37F8635D7B4B5FAB957E77ECDFFBFC53CF9F8BAEFA4E5B13CDAAAFFF7C0A2DFFF5BDDFE7CB8
D3C15AB7FFAE2174EF5DB7B9E745FAE6DFFF9E588FF6FB4CF7F3DFEEFAB2EDF5F2F389EC1FFE6E7EFD6B7D9277D4606793CBBA7AF77FEE86
B74DE86B5FEFDBBB59CFEFC7D77666703F7F376D9F5BDFDFCFFBDBFF76BBBEAB25DADF4EF9775AAD12B5BDBD1F6E01D2E63336F2795A45D
11EBF3F9DDF226EFD3BED79E5DFFFACFFD53FE5E2AFFBFE5BE742F83DFC5B9E83FDD4C53FA2BC03EBBB36FBEFFF4FF7F65CE76F2B562EDF
E779C83EDFAF91FD771FF9E2F5A5FC07BF75A7BC3FBC7EA2F3FDA9F37AE7D33FF225C79F9FBF593DE32FEF8F59DEB442BFBF9E6AB0B7FD65
F3F0F7BDBD7C9B7FDFBB3F6DAFACBFAB9FB3398BEF7F5FC2E9DCF4EDF1F763AD30F37DFB71CD66BFDCFF6362B77EAF3D9E7BDF8EC3EF56
9E9B3FC0BFD0BF1F7B5ECE16777FCB97C772DF45FBFEB23B75FEDF1FFFB3CD3F27B7387A9DFC50C59EBDCD2FED47F1B9FBF6F6960DBF7F7
3E7FF6DF9

Conclusão

Conclusão

Inatel
Instituto Nacional de Telecomunicações

→ O **patrimônio intelectual** vêm sendo a propriedade mais **valiosa** nas empresas

→ Os principais **algoritmos** criptográficos são ***open source***

→ As **chaves** criptográficas **garantem** a segurança dos dados

→ A **geração** e **troca** de chaves em sistemas reduzidos podem ser **ineficientes**

→ Uma **configuração ótima** para esta implementação foi alcançada

→ Geração de **10.000** chaves de **10Kib consecutivas distintas** em **14ms** por chave

Trabalhos Futuros

Trabalhos Futuros

Inatel
Instituto Nacional de Telecomunicações

→ Estudo de **vulnerabilidade**

→ Submeter a técnica aos **ataques** clássicos:
  → Ataque simples
  → Ataque geométrico
  → Ataque de maioria
  → Ataque genético

→ Implementar mecanismo de **realimentação** (*feedback*)

Redes Neurais Artificiais Aplicadas à Geração de Chaves Criptográficas Binárias

Gustavo Pasqua de Oliveira Celani
Marcelo Vinícius Cysneiros Aragão