Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

Estudo e aplicação de um circuito de criptografia analógico baseado em caos

Tiago Pereira Neves

TRABALHO DE GRADUAÇÃO

ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Brasília

2022

Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

Estudo e aplicação de um circuito de criptografia analógico baseado em caos

Tiago Pereira Neves

Trabalho de Graduação submetido como requisito parcial para obtenção do grau de Engenheiro de Controle e Automação.

Orientador: Prof. Dr. José Alfredo Ruiz Vargas

Brasília
2022

Pereira Neves, Tiago.
P436e Estudo e aplicação de um circuito de criptografia analógico baseado em caos / Tiago Pereira Neves; orientador José Alfredo Ruiz Vargas. –– Brasília, 2022.
55 p.

Trabalho de Graduação em Engenharia de Controle e Automação –– Universidade de Brasília, 2022.

1. Sistema caótico. 2. Eletrônica analógica. 3. Controle não-linear. 4. Circuito de Chua. 5. Criptografia analógica. 6. Análise de Lyapunov. I. Ruiz Vargas, José Alfredo, orient. II. Título

Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

Estudo e aplicação de um circuito de criptografia analógico baseado em caos

Tiago Pereira Neves

Trabalho de Graduação submetido como requisito parcial para obtenção do grau de Engenheiro de Controle e Automação.

Trabalho aprovado. Brasília, 4 de maio de 2022:

Prof. Dr. José Alfredo Ruiz Vargas,
UnB/FT/ENE
Orientador

Prof. Dr. Max Eduardo Vizcarra Melgar,
UFC
Examinador externo

Dr. Kevin Herman Muraro Gularte
Examinador externo

Brasília
2022

Agradecimentos

Agradeço toda minha família pelo apoio incondicional que sempre me deram. E em especial agradeço à minha mãe Marlene, meu pai Jerônimo, minha madrasta Leilian e minha noiva Nicole.

Agradeço também meus amigos que estiveram comigo nessa jornada, e aos meus colegas e professores.

Agradeço ao meu orientador, professor Dr. José Alfredo Ruiz Vargas, pela oportunidade e ao Dr. Kevin Herman Muraro Gularte por todo o auxílio prestado no decorrer do desenvolvimento deste trabalho.

Por fim, agradeço a Deus por estar comigo e aos que de alguma forma fizeram parte dessa caminhada.

Muito Obrigado!

Resumo

Este trabalho estuda um esquema de sincronização subatuado para o circuito de Chua com aplicação em criptografia. Com base na teoria de estabilidade de Lyapunov, é apresentado um estudo sobre um esquema de controle, o qual, em contraste com o mais comumente encontrado na literatura, utiliza um controle em apenas uma das equações de estado do sistema escravo. As principais vantagens do esquema de sincronização estudado são sua simplicidade e sua robustez contra distúrbios internos e externos. Essas diferenças são de grande importância na aplicação prática em criptografia analógica. Para validar a abordagem estudada, considerou-se a sincronização de dois circuitos caóticos de Chua usando componentes reais e na presença de distúrbios. A validação foi realizada por meio de simulações nos *Software* Matlab/Simulink e Multisim.

Palavras-chave: Sistema caótico. Eletrônica analógica. Controle não-linear. Circuito de Chua. Criptografia analógica. Análise de Lyapunov.

Abstract

This work studies an under-actuated synchronization scheme for Chua's circuit with application in analog cryptography. Based on Lyapunov's theory, a study on a control scheme is presented, which in contrasts to the most commonly found in literature, uses a control signal in only one of the state equations of the slave system. The main advantages of the synchronization scheme studied are its simplicity and strength against internal and external disturbance. These differences are of great significance in the practical application of cryptography applied. To validate the studied approach, we considered the synchronization of two chaotic Chua's circuit using real components in the presence of disturbances. The validation was performed through simulations in the Matlab/Simulink and Multisim software.

Keywords: Chaotic system. analog electronics. Nonlinear control. Chua circuit. Analog encryption. Lyapunov analysis.

Lista de ilustrações

Sumário

1 INTRODUÇÃO

1.1 REVISÃO DA LITERATURA

Ao longo da história do estudo das ciências foram identificados sistemas que apresentavam um comportamento de difícil análise. E por muitos anos a dinâmica dos sistemas foi classificada como de curso estável, oscilação periódica ou de quasi-periódica, semelhante ao movimento da lua e dos planetas, mesmo que já fosse de conhecimento que determinados sistemas não apresentavam uma dinâmica que se encaixava nessa classificação. No século XIX Henri Poincaré quando estudava a estabilidade do sistema solar, foi quem primeiro descreveu essa dinâmica (POINCARÉ; MAITLAND, 2003). Poincaré percebeu que as órbitas apresentavam grandes variações de comportamento a partir de pequenas variações das condições iniciais. E em um de seus estudos sobre essa dinâmica, apontou que os sistemas observados que apresentavam esse comportamento tinham no mínimo três dimensões.

James Clerk Maxwell, que nos anos de 1860 estudava a trajetória de movimento e colisão das moléculas de gases, já compreendia que mudanças muito pequenas no movimento inicial das partículas resultaria em grandes mudanças nas trajetórias das moléculas, ainda que essas moléculas fossem consideradas esferas rígidas (ALLIGOOD; SAUER; YORKE, 1996). Contudo, foi somente no século XX que os estudiosos classificaram essa dinâmica de movimento, que atualmente é conhecida por meio da teoria do caos.

Hoje está estabelecido que a dinâmica do caos é uma propriedade dos sistemas determinísticos, que apresentam um comportamento aleatório sem uma compreensão profunda de sua causa (SPROTT, 2010). O comportamento de sistemas que exibem caos, também conhecidos como sistemas não-lineares, é pautado pela imprevisibilidade ao longo do tempo e pela alta dependência das suas condições iniciais (MANGIAROTTI et al., 2020).

Com a maior compreensão acerca de sistemas não-lineares, por meio da análise desenvolvida por Lyapunov e considerando o nível de complexidade apresentada, estabeleceu-se uma divisão desses sistemas em dois tipos, os sistemas denominados caóticos e os hipercaóticos, mesmo que todo sistema hipercaótico seja um sistema caótico. Como característica os sistemas caóticos apresentam um expoente de Lyapunov positivo. Já em sistemas hipercaóticos, são pelo menos dois expoentes positivos (STANKEVICH et al., 2019), o que indica maior complexidade.

Uma característica particular dos sistemas não-lineares é o fenômeno observado quando é realizada a exposição gráfica de uma dimensão do sistema em função de outra dimensão do mesmo sistema, onde tal feito faz formar figuras gráficas chamadas de atratores. Tais figuras gráficas são comumente associadas à presença de caos (SPROTT, 2010).

Os sistemas dinâmicos caóticos e hipercaóticos estão presentes nos diversos campos de estudo das ciências, como nas finanças (MOUTSINGA; PINDZA; MARÉ, 2020) (ZHAO; LI, Z.; LI, S., 2011) (VARGAS; GRZEIDAK; HEMERLY, 2015), biologia (SCHARF, 2017) (HUESO et al., 2018), medicina (KESIĆ; SPASIĆ, 2016), redes neurais (WANG, R.; ZHANG; CHEN, Y., 2020) (CHAI; LIM, 2016), química (AWAL; BULLARA; EPSTEIN, 2019) (VARAN; AKGUL, 2018), criptografia de informações (ZHOU; WANG, C., 2020) (WEN; WEI; ZHANG, 2020) (FARAH et al., 2020) (HANIF et al., 2020), entre outros como pode ser verificado em (ALLIGOOD; SAUER; YORKE, 1996).

Devido a característica de imprevisibilidade dos sistemas não-lineares, esse tipo de sistema é amplamente utilizado em criptografia de informações para comunicação segura como pode ser observado em (VASEGHI et al., 2021) (LUO et al., 2019) (BUTKEVICH; AFANASIEV; LOGINOV, 2021) (CHEN, Y.-J. et al., 2020). Para que seja possível realizar a criptografia de uma informação pelo transmissor e posteriormente realizar descriptografia pelo receptor, é necessário primeiro realizar a sincronização entre dois sistemas não-lineares, o sistema mestre (sistema transmissor) e o sistema escravo (sistema receptor). É no sistema escravo que o sincronizador atua forçando a convergência dos estados desse sistema para o estados do sistema mestre. Depois que é feita a sincronização dos sistemas, é possível transmitir por um canal público de maneira segura uma mensagem criptografada do sistema mestre para o sistema escravo, onde é realizada a descriptografia da informação transmitida.

Existe uma variedade de tipos de controladores para realizar a sincronização de sistemas não-lineares, como controle adaptativo (ASIAIN; GARRIDO, 2021), controle por modo deslizante (MODIRI; MOBAYEN, 2020), controle ativo (WANG, S. et al., 2020), etc. Além disso o controlador é classificado quanto a sua atuação nas equações de estado do sistema, portanto, quando o sinal de controle está presente em todas equações de estado do sistema é denominado completamente atuado e subatuado caso contrário.

Nesse trabalho, diferentemente do normalmente encontrado na literatura como em (CAPLIGINS et al., 2021) (ZHILONG et al., 2019) (VAIDYANATHAN; RASAPPAN, 2014) (KOCAMAZ; CEVHER; UYAROĞLU, 2017), é considerado a presença de distúrbios nas equações de estado do sistema. Além disso, é utilizado um esquema de controle simples, do tipo proporcional e subatuado, o que facilita a implementação com componentes eletrônicos e diminui os custo da implementação, já que possibilita a utilização de componentes de baixo custo.

Portanto, as vantagens da sincronização e aplicação em criptografia analógica do sistema estudado neste trabalho em relação a outros trabalhos normalmente encontrados na literatura, são:

- Esquema de sincronização mais simples, por se tratar de um controlador do tipo proporcional aplicado em apenas um estado do sistema.

- Maior robustez a distúrbios limitados, já que são considerados matematicamente distúrbios atuando sobre o sistema e que são inerentes a implementação prática de circuitos eletrônicos.
- Capacidade de transmissão de duas mensagens distintas criptografadas, dado que dois estados do sistema estará livre, possibilitando assim a transmissão simultânea de duas mensagens.
- Baixo custo de implementação pois terá a utilização de elementos da eletrônica analógica comuns, como amplificadores operacionais, resistores, capacitores e indutores, com tolerância padrão de 5% ao contrário de (MOBAYEN; FEKIH et al., 2021). Neste caso, a validação do circuito eletrônico ocorrerá em simulações no *software* Multisim.

1.2 CARACTERÍSTICAS DO TRABALHO

As principais características deste trabalho estão concentradas no estudo de uma nova metodologia de baixa complexidade para sincronização de sistemas caóticos. Em particular, neste trabalho é considerado o circuito gerador de sinal caótico de Chua e sua aplicação em criptografia analógica. Sendo que as principais vantagens obtidas, em comparação ao que é encontrado nos diversos estudos presente na literatura, são:

- Alta simplicidade do sincronizador estudado por utilizar apenas um sinal de controle do tipo proporcional atuando apenas na primeira equação de estado. Diferentemente de (MOBAYEN; J., 2018) e (MOBAYEN, 2018) que têm lei de controle mais complexa.
- O sincronizador possui robustez na presença de ruídos e distúrbios limitados, já que este estudo leva em consideração a presença de distúrbios na análise de estabilidade, ao contrário de (KUETCHE MBE et al., 2014) que não considera tais distúrbios.
- Implementação eletrônica em *software* de simulação com componentes reais, ou seja, componentes com tolerância operacional, diferentemente de (WANG, N. et al., 2021), onde todos componentes considerados no circuito, são ideais.

1.3 OBJETIVOS

Este trabalho tem como objetivo propor um esquema de sincronização para o circuito gerador de sinal caótico de Chua com aplicação em criptografia analógica.

1.3.1 OBJETIVOS ESPECÍFICOS

Com condições iniciais distintas e na presença de distúrbios limitados, a sincronização deverá ser realizada entre dois circuitos de Chua, sendo um denominado mestre e o outro

escravo, utilizando um controle do tipo proporcional subatuado. O controle do circuito deve ter lei de descrição simples, e aplicação apenas na primeira equação de estado do sistema que descreve o funcionamento do circuito escravo. O sistema deve ser capaz de realizar a criptografia analógica utilizando a segunda e/ou terceira equação(ões) de estado para criptografar uma ou duas mensagens simultaneamente. A sincronização e a robustez do sistema devem ser asseguradas pela prova que fará uso da teoria de estabilidade de Lyapunov. Por fim, a validação do esquema estudado deve ser realizada por meio de simulações nos *software* Matlab/Simulink e Multisim.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado da seguinte forma:

- Capítulo 1: Motivação para a realização do presente trabalho e uma breve revisão da literatura.
- Capítulo 2: Definições e conceitos necessários para a compreensão do trabalho.
- Capítulo 3: Formulação do problema, proposição de uma lei de controle e prova a partir da teoria de estabilidade de Lyapunov.
- Capítulo 4: Validação do esquema estudado por meio dos resultados obtidos nas simulações realizadas nos *software* Matlab/Simulink e Multisim.
- Capítulo 5: Principais conclusões alcançadas neste trabalho de conclusão de curso.

2 CONCEITOS E DEFINIÇÕES PRELIMINARES

Neste capítulo são apresentados os conceitos e principais definições necessárias para a compreensão do presente trabalho.

2.1 SISTEMAS DINÂMICOS

Um sistema dinâmico consiste em um conjunto de estados possíveis, juntamente com uma regra que determina o estado atual em termos de estados passados (ALLIGOOD; SAUER; YORKE, 1996). Portanto, seguindo esse conceito o sistema dinâmico definido como (KHALIL; GRIZZLE, 2002):

$$\dot{x} = f(t, x, u) \tag{2.1}$$

está na forma de equação de estado com referência ao estado x, em que t é a variável temporal e u uma entrada. Um sistema de n dimensão:

$$\begin{aligned}
\dot{x}_1 &= f_1\left(t, x_1, \dots, x_n, u_1, \dots, u_p\right) \\
\dot{x}_2 &= f_2\left(t, x_1, \dots, x_n, u_1, \dots, u_p\right) \\
\dot{x}_3 &= f_3\left(t, x_1, \dots, x_n, u_1, \dots, u_p\right) \\
&\vdots \qquad \vdots \\
\dot{x}_n &= f_n\left(t, x_1, \dots, x_n, u_1, \dots, u_p\right)
\end{aligned} \tag{2.2}$$

apresenta uma quantidade n finita de equações diferenciais ordinárias em que $\dot{x}_i$ refere-se à derivada de x_i em relação à variável temporal t; $u_1, u_2, \dots, u_p$ são variáveis de entrada e $x_1, x_2, \dots, x_n$ são variáveis de estado.

Duas variações importantes na estrutura apresentada de sistemas dinâmicos são definidas a seguir. A primeira refere-se a ausência da entrada u, que transforma a equação de estado do sistema na forma:

$$\dot{x} = f(t, x) \tag{2.3}$$

tornando a equação de estado de um sistema forçado na equação de estado de um sistema não forçado quando u está ausente. A segunda refere-se a ausência de u e t, que transforma a equação de estado do sistema na forma:

$$\dot{x} = f(x) \tag{2.4}$$

tornando a equação de estado do sistema na equação de estado de um sistema não forçado e, se a parte da direita da equação (2.4) não depende do tempo, invariante no tempo. Além disso, outra forma comumente encontrada na literatura para representar u é apresentada na seguinte equação:

$$u = g(t, x) \tag{2.5}$$

Portanto, a equação (2.1) pode ser representada como:

$$\dot{x} = f(t, x, g(t, x)) = f(t, x) \tag{2.6}$$

Um conceito importante que ainda não foi abordado nesta seção é o conceito de ponto de equilíbrio. Dado um sistema dinâmico qualquer, definido como (2.1) e para $x = x^*$ em um certo ponto de sua trajetória, x^* é dito ponto de equilíbrio do sistema se sua variação nesse ponto for nula, ou seja:

$$\left[\frac{dx}{dt}\right]_{x=x^*} = 0 \tag{2.7}$$

É importante destacar que, os sistemas tendem a se manter em um ponto de equilíbrio na ausência e perturbações.

Na presença de sistemas não-lineares, a depender da aplicação, com frequência são feitas tentativas de linearização da dinâmica desses sistemas em torno de algum ponto de operação, e isso ocorre devido uma maior facilidade de compreensão do comportamento de sistemas lineares. Por essa razão, geralmente não se realiza a linearização de sistemas caóticos quando a aplicação desejada é em criptografia analógica, já que sistemas lineares não exibem caos.

2.2 ESCALONAMENTO

O escalonamento é utilizado para fazer alterações no sistema de equações diferenciais com o objetivo de alterar sua curva, seja por razões de projeto como, por exemplo, limitação da faixa de operação de componentes eletrônicos ou simplesmente por requisitos de projeto. O escalonamento pode ser realizado de duas maneiras, como apresentado a seguir.

2.2.1 ESCALONAMENTO DE AMPLITUDE

O escalonamento de amplitude, como o próprio nome sugere, é utilizado para variar a amplitude das equações de estado. O escalonamento de amplitude é aplicado quando se deseja diminuir a faixa de operação da tensão do sistema que descreve um circuito eletrônico, possibilitando a sua implementação prática, por exemplo.

Para diminuir a amplitude em n vezes, em que n é um número real, uma nova variável X é definida em cada equação de estado como:

$$X = \frac{x}{n} \tag{2.8}$$

e então as equações diferenciais tornam-se:

$$\dot{X} = \frac{\dot{x}}{n} \tag{2.9}$$

assim, o sistema dinâmico original deve ser reescrito substituindo as novas variáveis. Com o escalonamento realizado, as condições iniciais também devem ser escalonadas na mesma proporção n, já que o sistema resultante do escalonamento, pode não comportar as condições iniciais anteriores.

2.2.2 ESCALONAMENTO DE FREQUÊNCIA

O escalonamento de frequência é aplicado quando se deseja aumentar a frequência de processos muito lentos ou diminuir a frequência em sistemas que podem levar a desgaste no caso de execução em alta frequência. Além disso, com o escalonamento de frequência é possível obter uma convergência mais rápida dos sistemas.

Para tornar a simulação de um sistema m vezes mais lenta, basta realizar a seguinte alteração nas equações de estado:

$$\dot{x} = \frac{f(x)}{m} \tag{2.10}$$

e caso o desejado seja tornar o sistema mais rápido, basta fazer o inverso de (2.10).

2.3 TEORIA DE ESTABILIDADE DE LYAPUNOV

Esta seção contém conceitos e definições retirados de (IOANNOU; SUN, 2012) sobre a teoria da estabilidade de Lyapunov.

2.3.1 CONCEITOS SOBRE ESTABILIDADE

Seja o seguinte sistema modelado por equações diferenciais ordinárias

$$\dot{x} = f(t,x), \quad x(t_0) = x_0 \tag{2.11}$$

em que $x \in \Re^n, f : \tau \times B(r) \to \Re, \tau = [t_0, \infty)$ e $B(r) = \left\{x \in \Re^n | \|x\| < r\right\}$. Assume-se que f é de tal natureza que, para cada $x_0 \in B(r)$ e cada $t_0 \in \Re^+$, (2.11) possui uma, e somente uma solução $x(t, t_0, x_0)$.

Definição 2.2.1.1: Um estado x_e é chamado de **estado de equilíbrio** para o sistema descrito por (2.11) se $f(t, x_s) \equiv 0$ para todo $t \geq t_0$.

Definição 2.2.1.2 . Um estado de equilíbrio x_s é chamado de **estado de equilíbrio isolado** se existir uma constante $k > 0$ tal que $B(x_e, k) := \{x | \|x - x_s\| < k\} \subset R^n$.

Definição 2.2.1.3: O estado de equilíbrio x_e é considerado estável (no sentido de Lyapunov) se para um t_o arbitrário e $\varepsilon > 0$ existir um $\delta(\varepsilon, t_0)$ tal que $\|x_0 - x_e\| < \delta$ implica $\|x(t, t_0, x_0) - x_e\| < \varepsilon$ para todo $t \geq t_0$.

Definição 2.2.1.4: O estado de equilíbrio x_e é considerado **uniformemente estável** se ele for estável e se $\delta(\varepsilon, t_0)$ na definição 2.2.1.3 não for dependente de t_o.

Definição 2.2.1.5 :O estado de equilíbrio x_e é considerado **assintoticamente estável** se

- (i) ele for estável e
- (ii) existir um $\delta(t_0)$ tal que $\|x_0 - x_e\| < \delta(t_0)$ implica em $\lim_{t \to +\infty} \|x(t, t_0, x_0) - x_s\| = 0$.

Se a condição (ii) for satisfeita, então o estado de equilíbrio x_e é **atrativo**.

Definição 2.2.1.6: O conjunto de todos $x_0 \in \Re^n$ tal que $x(t, t_0, x_0) \to x_e$ quando $t \to \infty$ para qualquer $t_0 \geq 0$ é chamado de **região de atração** do estado de equilíbrio x_e.

Definição 2.2.1.7: O estado de equilíbrio x_e é chamado de **uniformemente assintoticamente estável** se

- (i) ele for uniformemente estável e
- (ii) para cada $\varepsilon > 0$ e qualquer t_0 em $\Re^+$, existe um $\delta_0 > 0$, independente de t_0, ε e um $T(\varepsilon) > 0$, independente de t_0, tal que $\|x(t, t_0, x_0) - x_\varepsilon\| < \varepsilon$ para todo $t \geq t_0 + T(\varepsilon)$ sempre que $\|x_0 - x_\varepsilon\| < \delta_0$.

Definição 2.2.1.8: O estado de equilíbrio x_e é chamado de **exponencialmente estável** se, para cada $\varepsilon > 0$ existe um $\delta(\varepsilon) > 0$, tal que $\|x(t, t_0, x_0) - x_e\| < \varepsilon e^{-\alpha(t-t_0)}$ para todo $t \geq t_0$ sempre que $\|x_0 - x_\varepsilon\| < \delta(\varepsilon)$, em que $\alpha > 0$.

Definição 2.2.1.9: O estado de equilíbrio x_e é chamado de **instável** se ele não for estável.

Quando a equação em (2.11) possui somente uma única solução para cada $x_0 \in \Re^n$ e $t_0 \in \Re^+$, são necessárias as seguintes definições para se realizar uma caracterização global de soluções.

Definição 2.2.1.10: Uma solução $x(t, t_0, x_0)$ de (2.11) é **limitada** se existe algum $\beta > 0$ tal que $\|x(t, t_0, x_0) - x_e\| < \beta$ para todo $t > t_0$, em que β pode ser dependente de cada solução.

Definição 2.2.1.11: As soluções de (2.11) são **uniformemente limitadas** se para quaisquer $\alpha > 0$ e $t_0 \in \Re^+$, existir um $\beta = \beta(\alpha)$, independente de t_0, tal que se $\|x_0\| < \alpha$, então $\|x(t, t_0, x_0) - x_e\| < \beta$ para todo $t > t_0$.

Definição 2.2.1.12: As soluções de (2.11) são **uniformemente finalmente limitadas** (com limitante B) se existir algum $B > 0$ e se para quaisquer $\alpha \geq 0$ e $t_0 \in \Re^+$, existir um $T = T(\alpha) > 0$ (independente de t_0) tal que $\|x_0\| < \alpha$ implica $\|x(t, t_0, x_0)\| < B$ para todo $t > t_0 + T$.

Definição 2.2.1.13: Se $x(t, t_0, x_0)$ é uma solução de $\dot{x} = f(t, x)$, então a trajetória $x(t, t_0, x_0)$ é chamada de **estável** se o ponto de equilíbrio $z_e = 0$ da equação diferencial $\dot{z} = f(t, z + x(t, t_0, x_0)) - f(t, x(t, t_0, x_0))$ for estável.

2.4 SISTEMAS CAÓTICOS E HIPERCAÓTICOS

Ainda que não se tenha uma definição universal para descrever sistemas caóticos, três características importantes e necessárias que o sistema deve ter para que seja considerado caótico são (STROGATZ, 2018) (DEVANEY, 2008):

- **Sistema determinístico:** regido por leis determinísticas, não possui entradas ou parâmetros aleatórios.
- **Sensibilidade às condições iniciais:** as trajetórias se separam a uma taxa exponencial para diferentes condições iniciais.
- **Comportamento não linear e aperiódico:** órbitas periódicas ou quase-periódicas, trajetórias que não se acomodam com o passar do tempo em pontos fixos.

O cálculo dos expoentes de Lyapunov de um sistema é utilizado para caracterizar a separação das trajetórias desse sistema ao longo do tempo. Seja $\delta(t)$ a distância entre duas trajetórias em termos do tempo e δ_0 a distância no tempo inicial t_0, o sistema apresenta sensibilidade às condições iniciais se $\delta(t)$ crescer exponencialmente com o passar do tempo. Desta forma $\delta(t)$ pode ser representada como:

$$\delta(t) = \delta_0 e^{\gamma(t-t_0)} \tag{2.12}$$

em que γ é chamado de expoente de Lyapunov. Os expoentes de Lyapunov são calculados para avaliar a previsibilidade de um determinado sistema. Um sistema caótico tem no mínimo um expoente de Lyapunov maior que zero. Já sistemas hipercaóticos têm quatro ou mais dimensões e pelo menos dois expoentes de Lyapunov positivos.

2.5 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS

Em (BOCCALETTI et al., 2002) a sincronização de sistemas caóticos é definida como um fenômeno em que dois ou mais sistemas ajustam propriedades de seu movimento para obter um comportamento comum.

Como já mencionado, os sistemas caóticos possuem alta sensibilidade as condições iniciais, em que pequenas variações levam a diferenças exponenciais. Essa característica torna a sincronização de sistemas caóticos mais desafiante. Em sistemas práticos como circuitos eletrônicos, por possuírem elementos que de armazenamento de energia como capacitores, é impossível saber quais são as condições iniciais desses circuitos e, assim, dificultando a sincronização entre dois circuitos, já que possuem condições diferentes.

A seguir é apresentado um problema genérico de sincronização para um sistema dinâmico. Seja o sistema caótico representado por:

$$\dot{x}_m = f_m(x_m, d_m(t)) \tag{2.13}$$

em que f_m é um mapa conhecido, x_m é o estado do sistema mestre e d_m é um distúrbio desconhecido. E seja um sistema escravo representado por:

$$\dot{x}_s = f_s(x_s, u, d_s(t)) \tag{2.14}$$

em que f_s é um mapa conhecido, x_s é o estado do sistema escravo, u é a entrada do controlador e d_s é um distúrbio desconhecido. Pode-se definir o erro dinâmico baseando-se em (2.13) e (2.14) como:

$$\dot{e} = \dot{x}_s - \dot{x}_m = f_s(x_s, u, d_s(t)) - f_m(x_m, d_m(t)) \tag{2.15}$$

em que

$$e = x_s - x_m \tag{2.16}$$

é definido como sendo o erro de sincronização. Em geral, $e(t) \to 0$ quando $t \to \infty$, ou seja, se o sistema escravo convergir para os valores do sistema mestre, podemos considerar que os sistemas descritos pelas equações (2.13) e (2.14) estão perfeitamente sincronizados. Neste

trabalho também se considera a sincronização para o caso em que $e(t)$ se manter em valores limitados e próximos de zero quando $t \to \infty$.

3 SINCRONIZAÇÃO SUBATUADA DE UM SISTEMA CAÓTICO BASEADA EM CONTROLE PROPORCIONAL PARA APLICAÇÃO EM CRIPTOGRAFIA ANALÓGICA

3.1 INTRODUÇÃO

Neste capítulo é apresentado o estudo de um esquema de sincronização (GULARTE et al., 2021) para o circuito caótico de Chua (KUETCHE MBE et al., 2014) (MKAOUAR; BOUBAKER, 2012) para aplicação em criptografia analógica de informações.

3.2 FORMULAÇÃO DO PROBLEMA

Considere o sistema não-linear a seguir:

$$\begin{aligned} C_1\frac{dV_1}{dt} &= \frac{V_2 - V_1}{R} - f(V_1) \\ C_2\frac{dV_2}{dt} &= \frac{V_1 - V_2}{R} - I_L \\ \frac{dI_L}{dt} &= -\frac{V_2}{L} - \frac{R_L I_L}{L} \end{aligned} \tag{3.1}$$

O sistema (3.1) é obtido por meio da aplicação das leis de Kirchhoff no circuito de Chua em que $f(V_1) = m_0 V_1 + \frac{1}{2}(m_1 - m_0)[|V_1 + B_p| - |V_1 - B_p|]$ e representa a corrente caracterizada pela resistência não linear do circuito de Chua. As constantes m_0, m_1 e B_p são, respectivamente, $-0{,}7879S$, $-1{,}4357S$ e $1V$; a constante R_L, que caracteriza a resistência interna do indutor do circuito, é 2Ω; C_1, C_2, L, R são, respectivamente, $15nF$, $150nF$, $10mH$, 1070Ω. Para maiores detalhes vide (KUETCHE MBE et al., 2014) e (LING; LU; LAM, 2009). Nos circuitos dos sistemas mestre e escravo apresentados é importante destacar que o indutor foi implementado utilizando amplificadores operacionais, isso se dá devido ao valor de indutância, nesse caso, não ser comumente encontrado comercialmente.

A partir do sistema (3.1) fazendo escalonamento e mudanças das variáveis originais para as variáveis de estado $x(t) = V_1, y(t) = V_2$ e $z(t) = I_L$, tem-se (KUETCHE MBE et al., 2014);

Sistema mestre:

$$\begin{aligned} \dot{x}_m &= \frac{\alpha}{\beta_1}(y_m - x_m) - \frac{f(x_m)}{\beta_1} \\ \dot{y}_m &= \frac{\alpha}{\beta_2}(x_m - y_m) + \frac{z_m}{\beta_2} \\ \dot{z}_m &= -\frac{y_m}{\gamma} - \frac{R_L z_m}{\gamma} \end{aligned} \tag{3.2}$$

Sistema escravo:

$$\begin{aligned} \dot{x}_s &= \frac{\alpha}{\beta_1}(y_s - x_s) - \frac{f(x_s)}{\beta_1} + h_1(t) + u_1 \\ \dot{y}_s &= \frac{\alpha}{\beta_2}(x_s - y_s) + \frac{z_s}{\beta_2} + h_2(t) \\ \dot{z}_s &= -\frac{y_s}{\gamma} - \frac{R_L z_s}{\gamma} + h_3(t) \end{aligned} \tag{3.3}$$

em que $\alpha = 0{,}9346, \beta_1 = 0{,}15, \beta_2 = 1{,}50$ e $\gamma = 0{,}10$; os estados do sistema mestre são x_m, y_m e z_m; os estados do sistema escravo são x_s, y_s e z_s; os distúrbios presentes no sistema escravo são h_1, h_2 e h_3; e o sinal de controle é u_1.

Então, o objetivo é obter a sincronização dos sistemas (3.2) e (3.3), independentemente das perturbações e condições iniciais, na qual o sistema escravo sofrerá a influência de somente um sinal de controle atuando apenas na primeira equação de estado.

Comentário 1: Uma peculiaridade deste trabalho é que no sistema (3.3) é apresentado com distúrbios explicitamente, ao contrário da maioria dos trabalhos na literatura, o que nos permite considerar na análise que o sistema (3.2) é diferente do sistema (3.3), e a influência destas incertezas na limitação e convergência dos erros de sincronização. Os distúrbios são inevitáveis em implementações práticas devido às tolerâncias dos componentes, condições ambientais e ruído eletromagnético, entre outros.

Hipótese 1: Assume-se que os distúrbios são limitados. Mais precisamente, se:

$$
\begin{aligned}
|h_1(t)| &\leq \bar{h}_1 \\
|h_2(t)| &\leq \bar{h}_2 \\
|h_3(t)| &\leq \bar{h}_3
\end{aligned}
\tag{3.4}
$$

Sendo $\bar{h}_1, \bar{h}_2$ e $\bar{h}_3$ constantes desconhecidas para todo $t > 0$.

Comentário 2: O controle foi adicionado na primeira equação de estado do sistema escravo por ser o estado em que foi verificado, por meio da teoria de estabilidade de Lyapunov, que a lei de controle permitiria assegurar a convergência entre os dois sistemas. Essa escolha foi resultado de diferentes tentativas de prova, com o controle atuando em apenas uma equação de estado, concluiu-se que o lugar mais adequado para o controle atuar é no primeiro estado.

3.3 ERRO DE SINCRONIZAÇÃO E SINAL DE CONTROLE ESTUDADO

Uma vez que já foi caracterizado o sistema a ser utilizado, o seguinte passo é definir os erros de sincronização, pois esses erros são fundamentais para a prova de estabilidade. Então, os erros de sincronização dos sistemas são definidos como:

$$
\begin{aligned}
e_1 &= x_s - x_m \\
e_2 &= y_s - y_m \\
e_3 &= z_s - z_m
\end{aligned}
\tag{3.5}
$$

Assim, as equações dinâmicas dos erros podem ser obtidas usando os sistemas (3.2) e (3.3). Portanto:

$$
\begin{aligned}
\dot{e}_1 &= \frac{\alpha}{\beta}_1 (e_2 - e_1) - \frac{f(x_s) - f(x_m)}{\beta_1} + h_1 + u_1 \\
\dot{e}_2 &= \frac{\alpha}{\beta}_2 (e_1 - e_2) + \frac{e_3}{\beta_2} + h_2 \\
\dot{e}_3 &= -\frac{e_2}{\gamma} - \frac{R_L e_3}{\gamma} + h_3
\end{aligned}
\tag{3.6}
$$

Teorema 1: Considere os sistemas mestre e escravo descritos em (3.2) e (3.3) e a lei de controle proporcional descrita por:

$$u_1 = -\psi e_1 \tag{3.7}$$

em que ψ é uma constante positiva definida pelo usuário que se $\psi > \frac{\alpha}{\beta_1} + m_0 + \frac{1}{2} + \left(\frac{3\alpha}{\beta_1}\right)^2$, então o erro de sincronização converge em tempo finito para o conjunto compacto $\Omega = \{e \in \Re^3 \| \|e\| \leq \theta\}, \theta > 0$.

Prova:

Considere a seguinte candidata a função de Lyapunov:

$$V = \frac{1}{2}e_1^2 + e_2^2 + \frac{\gamma}{\beta_2}e_3^2 \tag{3.8}$$

Derivando (3.8) em relação ao tempo resulta:

$$\dot{V} = e_1\dot{e_1} + 2e_2\dot{e_2} + \frac{2\gamma}{\beta_2}e_3\dot{e_3} \tag{3.9}$$

Substituindo-se (3.6) em (3.9), tem-se:

$$\dot{V} = e_1\left[\frac{\alpha}{\beta_1}(e_2 - e_1) - \frac{f(x_s) - f(x_m)}{\beta_1} + h_1 + u_1\right] + 2e_2\left[\frac{\alpha}{\beta_2}(e_1 - e_2) + \frac{e_3}{\beta_2} + h_2\right] + \frac{2\gamma}{\beta_2}e_3\left(-\frac{e_2}{\gamma} - \frac{R_L e_3}{\gamma} + h_3\right) \tag{3.10}$$

Note que $-2 \leq |\lambda| - 1 - |\lambda| - 1 \leq |\lambda + 1| - |\lambda - 1| \leq |\lambda| + 1 - |\lambda| + 1 \leq 2$, para todo λ. Desse modo, $f(x_m) - f(x_s) \leq -m_0 e_1 + 2(m_0 - m_1)$. Substituindo-se (3.7) em (3.10), implica:

$$\dot{V} \leq -e_1^2\left(\psi + \frac{\alpha}{\beta_1} + \frac{m_0}{\beta_1}\right) - e_2^2\frac{2\alpha}{\beta_2} - e_3^2\frac{2R_L}{\beta_2} + e_1\left[\bar{h}_1 + \frac{2}{\beta_1}(m_0 - m_1)\right] + e_1e_2\frac{\alpha\beta_2 + 2\alpha\beta_1}{\beta_1\beta_2} + 2e_2\bar{h}_2 + e_3\frac{2\gamma\bar{h}_3}{\beta_2} \tag{3.11}$$

Perceba que $e_1\left[\bar{h}_1 + \frac{2}{\beta_1}(m_0 - m_1)\right] \leq \frac{1}{2}\left\{e_1^2 + \left[\bar{h}_1 + \frac{2}{\beta_1}(m_0 - m_1)\right]^2\right\}$, $e_1e_2\frac{\alpha\beta_2 + 2\alpha\beta_1}{\beta_1\beta_2} \leq \frac{1}{2}\left\{\left[\frac{\alpha\beta_2 + 2\alpha\beta_1}{\beta_1\beta_2}\right]^2 e_1^2 + e_2^2\right\}$, $2e_2h_2 \leq \frac{1}{2}\left[e_2^2 + (2\bar{h}_2)^2\right]$, $e_3\frac{2\gamma\bar{h}_3}{\beta_2} \leq \frac{1}{2}\left[e_3^2 + \left(\frac{2\bar{h}_3\gamma}{\beta_2}\right)^2\right]$, assim:

$$\dot{V} \leq -e_1^2\left[\psi + \frac{\alpha}{\beta_1} + \frac{m_0}{\beta_1} - \frac{1}{2} - \frac{1}{2}\left(\frac{\alpha\beta_2 + 2\alpha\beta_1}{\beta_1\beta_2}\right)^2\right] - e_2^2\left(\frac{2\alpha}{\beta_2} - 1\right) - e_3^2\left(\frac{2R_L}{\beta_2} - \frac{1}{2}\right) + \frac{1}{2}\left\{\left[\bar{h}_1 + \frac{2}{\beta_1}(m_0 - m_1)\right]^2 + 2\bar{h}_2^2 + 2\left(\frac{\gamma\bar{h}_3}{\beta_2}\right)^2\right\} \tag{3.12}$$

Considere que $\rho_1 = \psi + \frac{\alpha}{\beta_1} + \frac{m_0}{\beta_1} - \frac{1}{2} - \frac{1}{2}\left(\frac{\alpha\beta_2+2\alpha\beta_1}{\beta_1\beta_2}\right)^2$, $\rho_2 = \frac{2\alpha}{\beta_2} - 1$, $\rho_3 = \frac{2R_L}{\beta_2} - \frac{1}{2}$ e $\beta = \frac{1}{2}\left\{\left[\bar{h}_1 + \frac{2}{\beta_1}(m_0 - m_1)\right]^2 + 2\bar{h}_2^2 + 2\left(\frac{\gamma\bar{h}_3}{\beta_2}\right)^2\right\}$, então:

$$\dot{V} \leq -e_1^2\rho_1 - e_2^2\rho_2 - e_3^2\rho_3 + \beta \tag{3.13}$$

Note que $\rho_2 > 0$ e $\rho_3 > 0$ e que ψ escolhido pelo projetista é suficientemente grande, de modo que ρ_1 seja positivo. Definindo $\rho = min\{\rho_1, \rho_2, \rho_3\}$ (3.13), pode ser escrita como:

$$\dot{V} \leq -\rho||e||^2 + \beta \tag{3.14}$$

Definindo também o conjunto compacto $\Omega = \{e \in \Re^3 | ||e|| \leq \theta\}$, busca-se a partir de (3.14) a situação em que $\dot{V} < 0$, que ocorre em $||e|| > \sqrt{\frac{\beta}{\rho}} := \theta$, como θ é constante, pode-se afirmar que o erro de sincronização é limitado. Em outras palavras, pode-se afirmar que se por qualquer razão $||e||$ deixar o conjunto residual Ω, $\dot{V}$ se torna negativo definido e força a convergência do erro de sincronização para o conjunto residual Ω, conforme (3.14). Ou seja, se $\dot{V} < 0$ for satisfeito, a norma do erro somente poderá diminuir com o decorrer do tempo. Conclui-se então que o erro de sincronização é limitado e converge para uma bola com raio igual a θ.

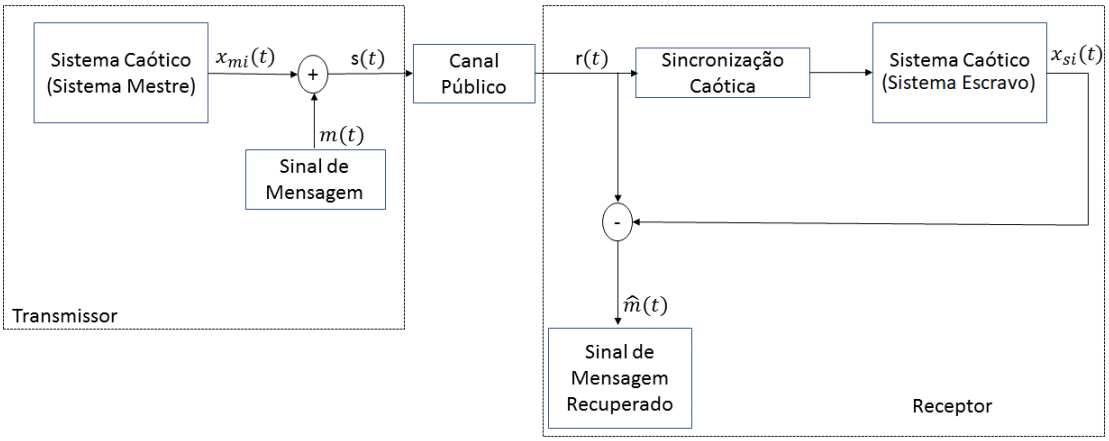
Comentário 3: Pode-se notar pela prova que distúrbios limitados estão sendo considerados. Assim, a partir da escolha de parâmetros de projeto do controlador pode se levar a um erro de sincronização próximo de zero, ainda que na presença de distúrbios limitados.

4 SIMULAÇÕES

Para validar a lei de controle (3.7) para o sistema (3.3) foram realizadas simulações computacionais utilizando o *software* MATLAB/Simulink. Com as simulações em Matlab/Simulink é possível verificar o comportamento do sistema, o erro de sincronização e a robustez do controle estudado na presença de distúrbios, além de mostrar a possibilidade de criptografar e transmitir até duas mensagens simultâneas. E para as implementações circuitais, foi utilizado o *software* Multisim onde foram realizadas as implementações dos circuitos dos sistemas mestre e escravo, e um esquema para criptografia analógica onde é possível criptografar até duas mensagens simultâneas. Convém ressaltar que a implementação no Multisim é crucial para verificar a implementação e calibração dos circuitos caóticos com elementos de eletrônica analógica de baixo custo, tornando possível se aproximar de situações reais em que os componentes apresentam tolerâncias.

Na figura (1) é apresentado um esquemático do sistema de sincronização e comunicação. No esquema deste trabalho, o primeiro estado do sistema mestre ($x_m(t)$) é transmitido sem o acréscimo de nenhuma informação ou mensagem, para que seja possível realizar a sincronização do sistema escravo com o sistema mestre. Assim, a mensagem pode ser transmitida acrescendo seu sinal no segundo ($y_m(t)$) ou terceiro ($z_m(t)$) estado, e para o caso de transmissão simultânea de duas mensagens, as mensagens são acrescentadas no segundo e terceiro estados do sistema mestre.

Figura 1 – Esquemático do sistema de sincronização e comunicação.



4.1 SIMULAÇÃO USANDO O MATLAB/SIMULINK

A simulação presente nesta seção foi realizada utilizando-se o *software* MATLAB R2016a (9.0.0.341360) 64-bit (win64), em um computador HP ProBook 6465b com processa-

dor AMD A6-3410MX APU com Radeon(tm) HD *Graphics* 1.60GHz, 6GB de memória RAM e sistema operacional Windows 10. Os códigos dos sistemas encontram-se nos Apêndices A e B.

As condições iniciais para o sistema mestre foram: $x_m(0) = 0{,}1$, $y_m(0) = 0{,}1$ e $z_m(0) = 0{,}0$. E as condições iniciais consideradas para o sistema escravo foram: $x_s(0) = 0{,}2$, $y_s(0) = 0{,}0$ e $z_s(0) = 0{,}2$. As simulações nesse *software* foram realizadas com o método de resolução $ode113$ e passo variável.

Para representar a presença de distúrbios limitados, foram considerados os seguintes sinais de distúrbio atuando, respectivamente, na primeira, segunda e terceira equação de estado do sistema escravo:

$$\begin{aligned} disturbio1(t) &= 0{,}05 * sen(2 * \pi * 20 * t) + 0{,}1 * square(2 * \pi * 3 * t) \\ disturbio2(t) &= 0{,}1 * cos(0{,}5 * \pi * 30 * t) - 0{,}05 * square(2 * \pi * 9 * t) \\ disturbio3(t) &= 0{,}15 * sen(\pi * 100 * t) - 0{,}15 * sawtooth(2 * \pi * 14 * t) \end{aligned} \tag{4.1}$$

em que $disturbio1 = h_1(t)$, $disturbio2 = h_2(t)$ e $disturbio3 = h_3(t)$. As equações de (4.1) foram escolhidas de maneira aleatória na tentativa de expressar diferentes formatos de distúrbios. Portanto, os distúrbios podem possuir sinal com diferentes formatos desde que estejam de acordo com (3.4).

4.1.1 SINCRONIZAÇÃO DO SISTEMA ESCRAVO COM O SISTEMA MESTRE

Nas figuras (2 a 4) é apresentado o resultado da sincronização, onde mostra o desempenho da sincronização dos estados do sistema escravo com os estados do sistema mestre.

Figura 2 – Desempenho de sincronização $x_s(t)$.

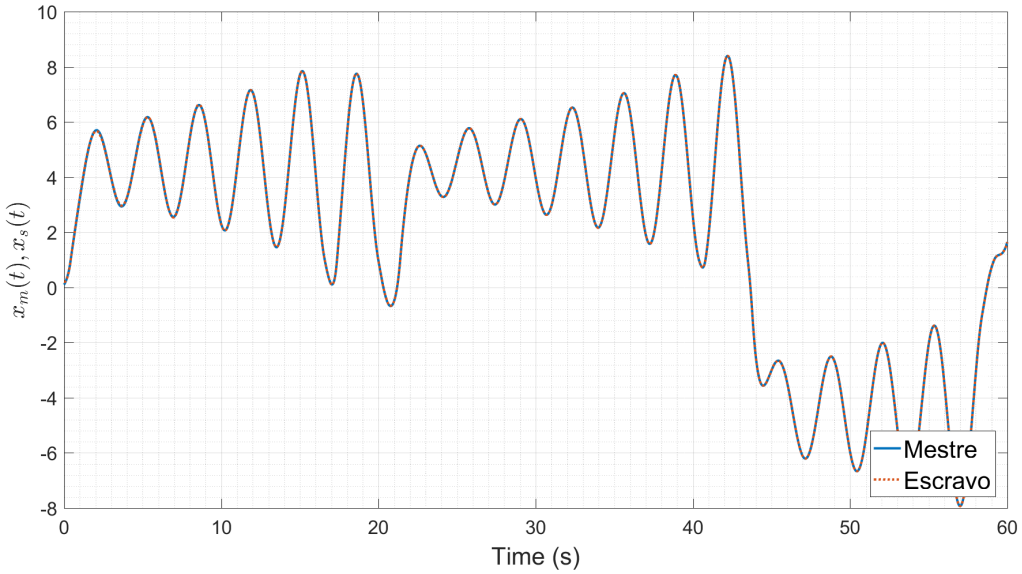


Figura 3 – Desempenho de sincronização $y_s(t)$.

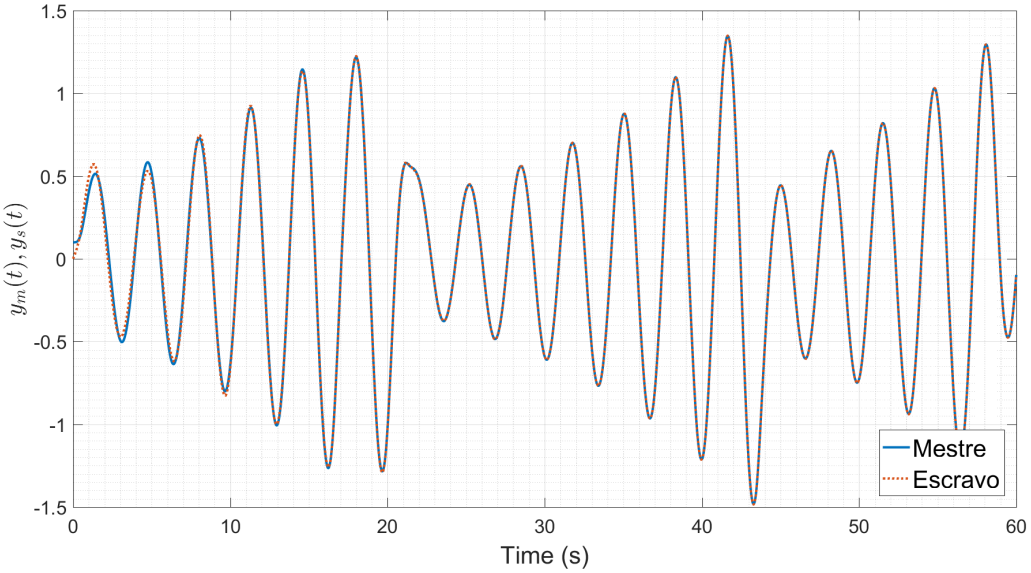
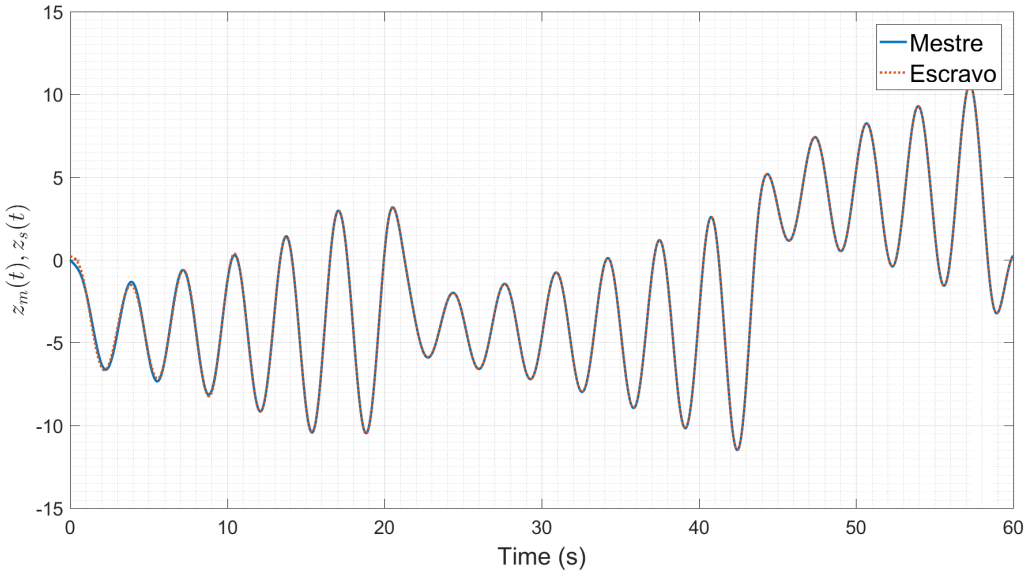


Figura 4 – Desempenho de sincronização $z_s(t)$.



Observe que a sincronização ocorre mais rapidamente no primeiro estado do sistema, onde o sinal de controle atua, mas apesar de demorar um pouco mais nos demais estados do sistema, a sincronização é realizada de forma bem sucedida. Mais adiante, como será mostrado, nos primeiros instantes de execução da sincronização o erro presente no segundo e terceiro estado do sistema escravo pode prejudicar a transmissão de mensagens, já que o erro nesse momento é maior. Porém, por ser um intervalo muito curto de sincronização, pode-se evitar a transmissão de mensagens nesse período.

4.1.2 ERRO DE SINCRONIZAÇÃO

As próximas figuras (5 a 7) mostram os erros de sincronização dos três estados do sistema escravo x_s, y_s e z_s, respectivamente.

Figura 5 – Erro de sincronização entre $x_s(t)$ e $x_m(t)$.

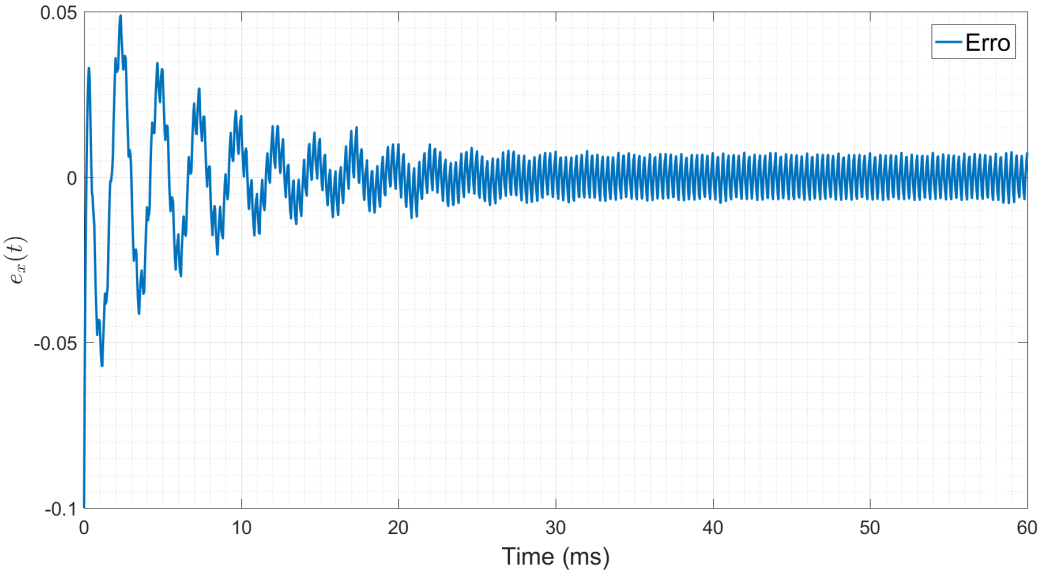


Figura 6 – Erro de sincronização entre $y_s(t)$ e $y_m(t)$.

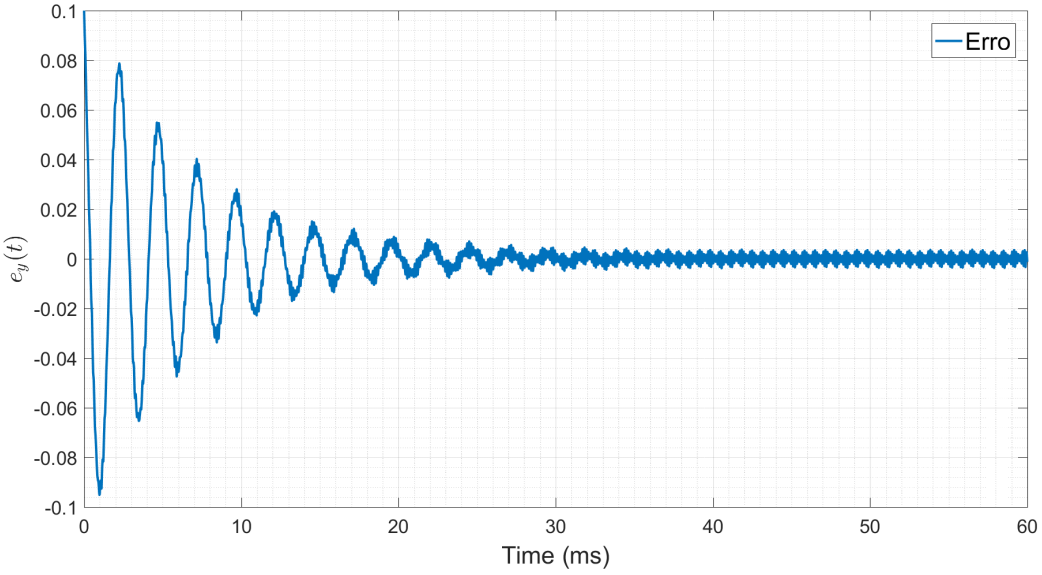
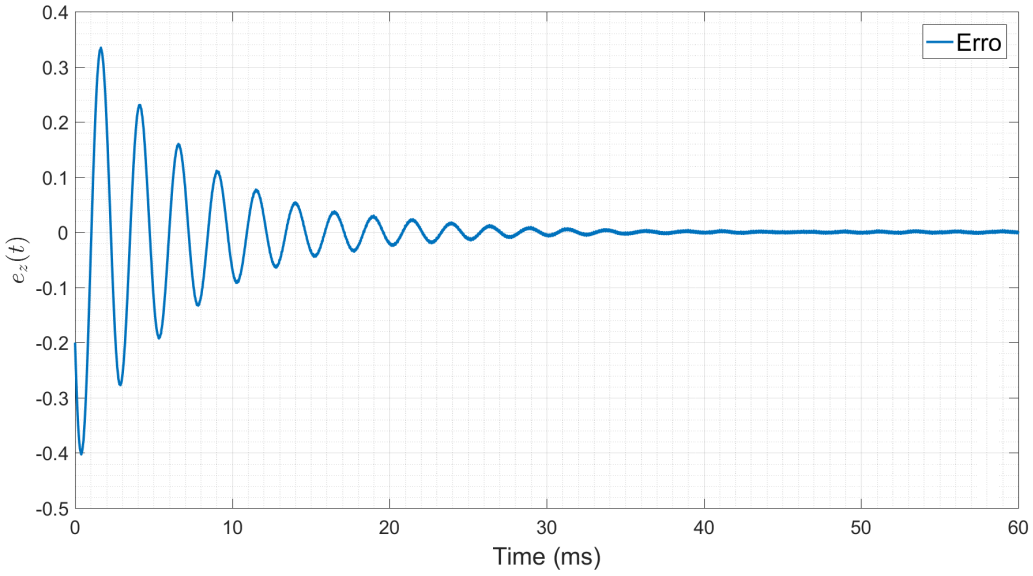


Figura 7 – Erro de sincronização entre $z_s(t)$ e $z_m(t)$.



Note que os erros de sincronização são limitados e convergem para uma região na vizinhança da origem, ou seja uma região na proximidade de zero. Este resultado valida o que foi demonstrado no capítulo 3 onde, pela teoria de estabilidade de Lyapunov, o erro de sincronização se mantém em valores limitados com o passar do tempo.

4.1.3 MENSAGENS ORIGINAIS E MENSAGENS CRIPTOGRAFADAS

Nas figuras a seguir são mostrados os sinais propostos como sinais de mensagem. A figura (8) mostra a mensagem $m_1(t)$ e a respectiva mensagem codificada que é resultado do acréscimo da mensagem $m_1(t)$ ao segundo estado $y_m(t)$. Já a figura (9) mostra a mensagem $m_2(t)$ e a respectiva mensagem codificada que é resultado do acréscimo da mensagem $m_2(t)$ ao terceiro estado $z_m(t)$.

Figura 8 – Mensagem codificada (laranja) e sinal $m_1(t)$ (azul) da mensagem inserida em $y_m(t)$.

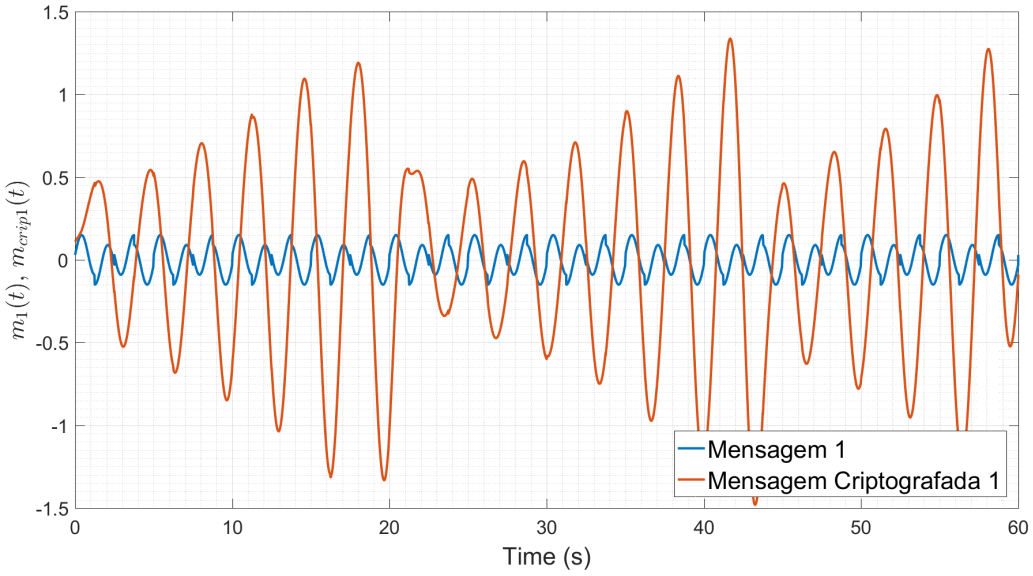
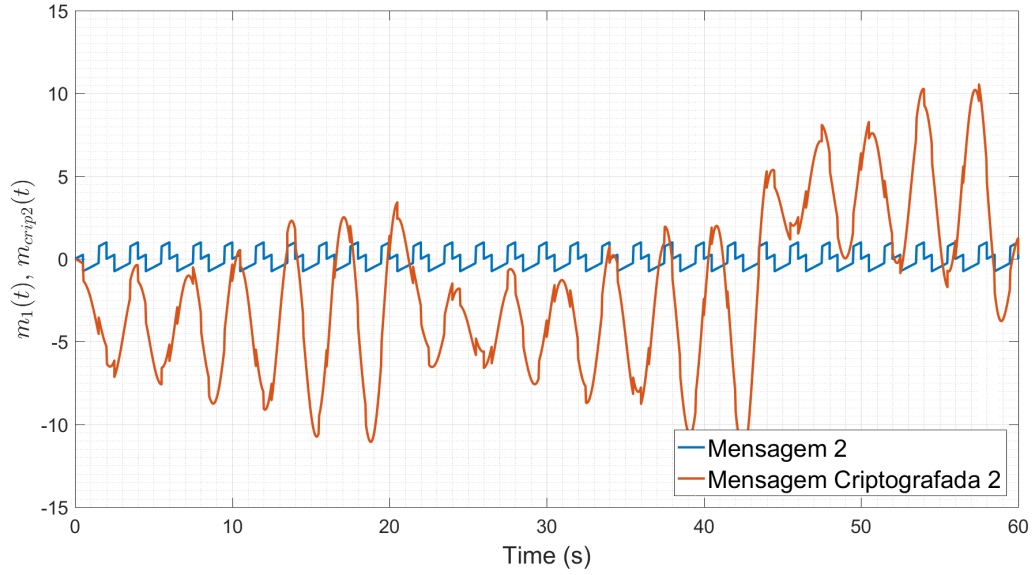


Figura 9 – Mensagem codificada (laranja) e sinal $m_2(t)$ (azul) da mensagem inserida em $z_m(t)$.



Note que os sinais das mensagens criptografadas são bem distintos dos sinais das mensagens originais. Portanto, tornando, imperceptível visualmente a natureza comportamental dos sinais de mensagem, como era esperado.

4.1.4 MENSAGENS ORIGINAIS E MENSAGENS RECUPERADAS

Figura 10 – Mensagem original $m_1(t)$ (azul) e mensagem recuperada $m_{1R}(t)$ (laranja).

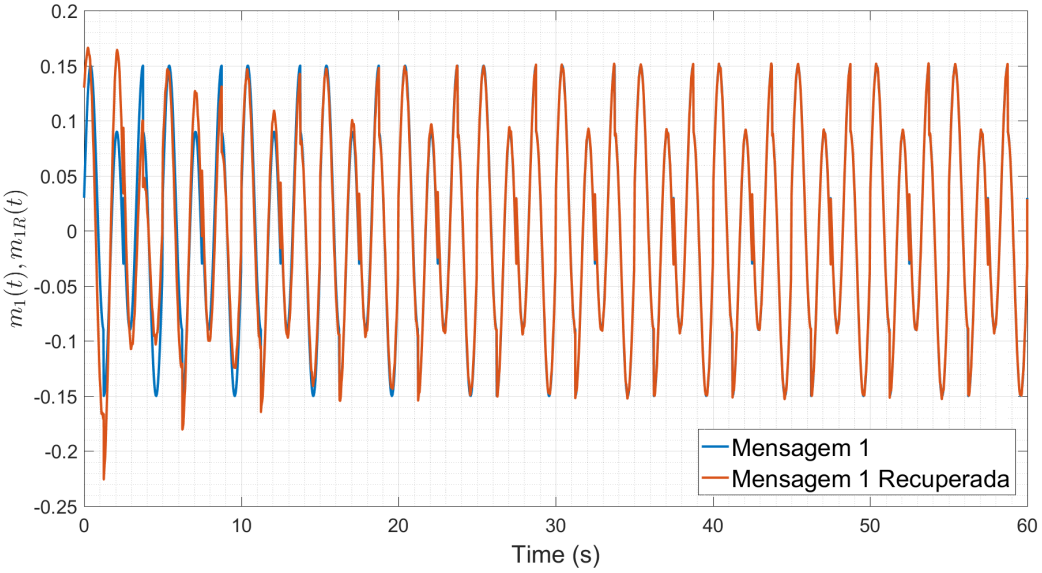
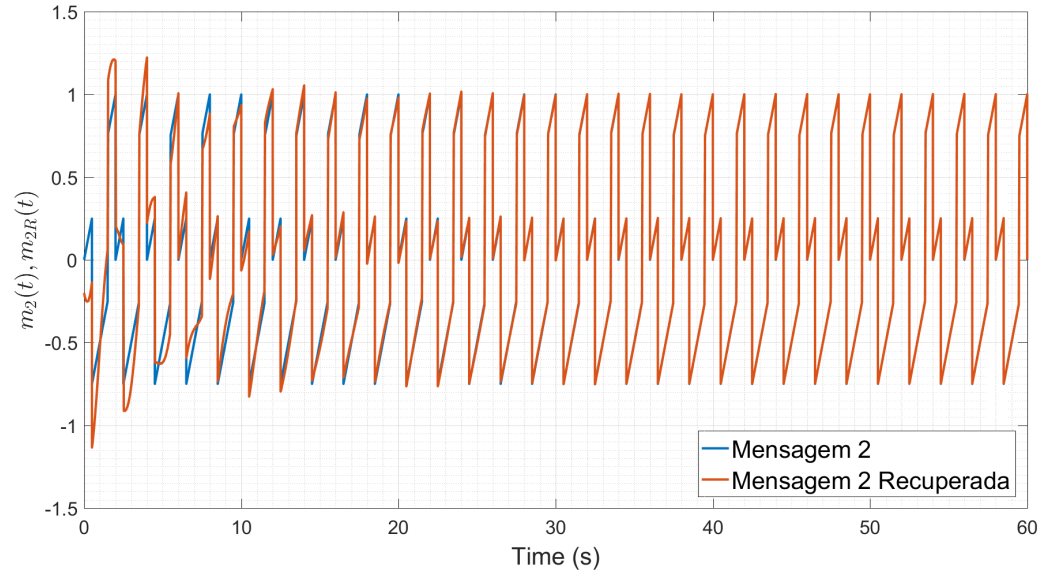


Figura 11 – Mensagem original $m_2(t)$ (azul) e mensagem recuperada $m_{2R}(t)$ (laranja).



4.1.5 ERRO DAS MENSAGENS RECUPERADAS

Figura 12 – Erro entre a mensagem original $m_1(t)$ e a mensagem recuperada $m_{1R}(t)$.

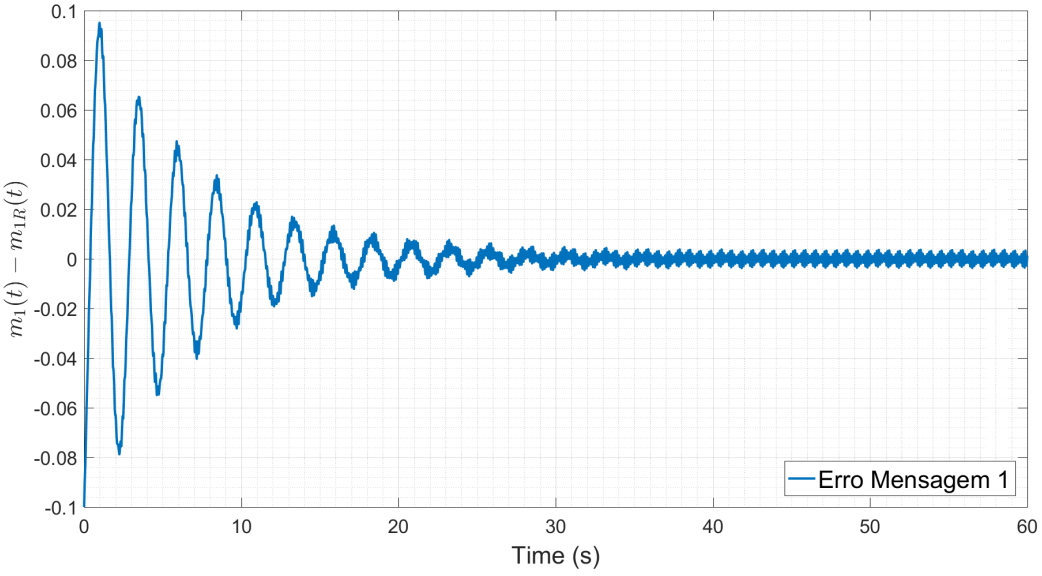
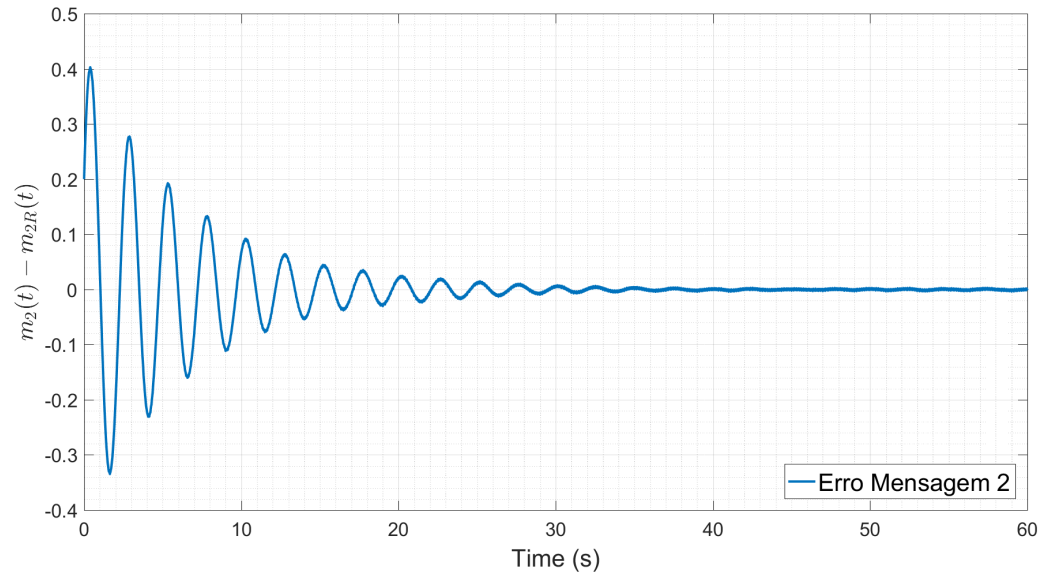


Figura 13 – Erro entre a mensagem original $m_2(t)$ e a mensagem recuperada $m_{2R}(t)$.



4.2 SIMULAÇÃO USANDO O MULTISIM

Nesta plataforma, foi utilizado um passo variável, método de integração trapezoidal e tolerância absoluta de erro de tensão igual a 0,001. Por ser uma das considerações desse trabalho o uso de elementos da eletrônica analógica de baixo custo, todos os componentes discretos apresentam uma tolerância de 5% emulando, portanto, a presença de distúrbios.

4.2.1 CIRCUITOS DOS SISTEMAS

Nas figuras (14 a 16) a seguir, são apresentados os circuitos do sistema mestre, do sistema escravo e para obtenção do erro e_1, sendo o erro entre o estado x_s e x_m.

Figura 14 – Circuito do sistema mestre.

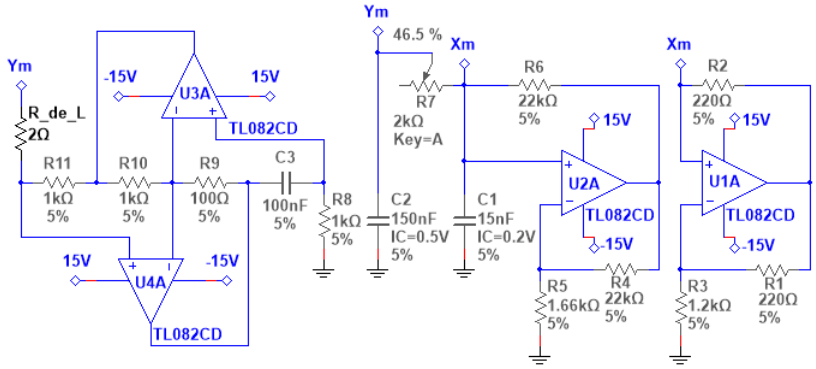


Figura 15 – Circuito do sistema escravo.

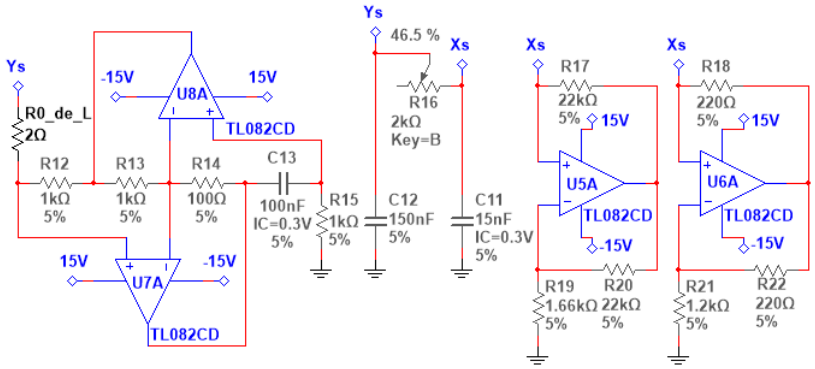
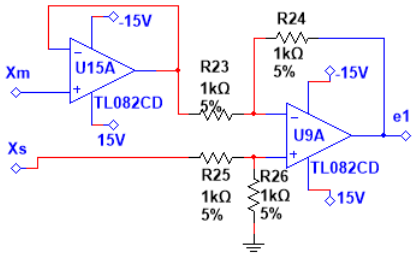
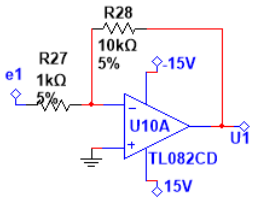


Figura 16 – Circuito do erro entre x_s e x_m.



Observe que na figura (14) as escritas "Xm", "Ym" e "Zm", referem-se aos estados $x_m(t)$, $y_m(t)$ e $z_m(t)$. Já na figura (15) as escritas "Xs", "Ys" e "Zs", referem-se aos estados $x_s(t)$, $y_s(t)$ e $z_s(t)$. Na figura (16) a escrita "e1", refere-se ao erro de sincronização $e_1(t)$ entre os estados $x_s(t)$ e $x_m(t)$. A seguir tem-se o circuito gerador do sinal de "U1", que refere-se a $u_1(t)$, a partir do erro.

Figura 17 – Circuito do sinal de controle.



Note que $u_1(t) = -10e_1$, que é obtido com um amplificador operacional em um circuito multiplicador inversor.

Figura 18 – Circuito de criptografia.

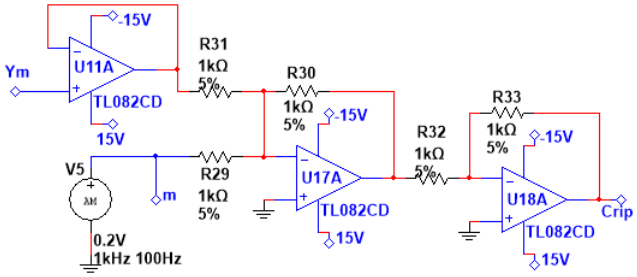
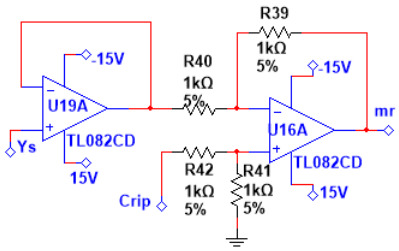


Figura 19 – Circuito de recuperação da mensagem.



Como sinal de mensagem tem-se uma fonte de tensão com variação de amplitude denominada *AM*, presente no Multisim. Por praticidade de implementação e diferentemente das simulações em Matlab/Simulink, nas simulações no Multisim a criptografia é aplicada na transmissão de apenas uma mensagem, porém como já demonstrado em tópicos anteriores, é possível transmissão simultânea de até duas mensagens criptografadas.

4.2.2 SINCRONIZAÇÃO DO CIRCUITO ESCRAVO COM O CIRCUITO MESTRE

Nas figuras (20 a 22) é apresentado o resultado e desempenho da sincronização do circuito escravo com o circuito mestre no Multisim.

Figura 20 – Desempenho de sincronização de $x_s(t)$ (vermelho) com $x_m(t)$ (azul).

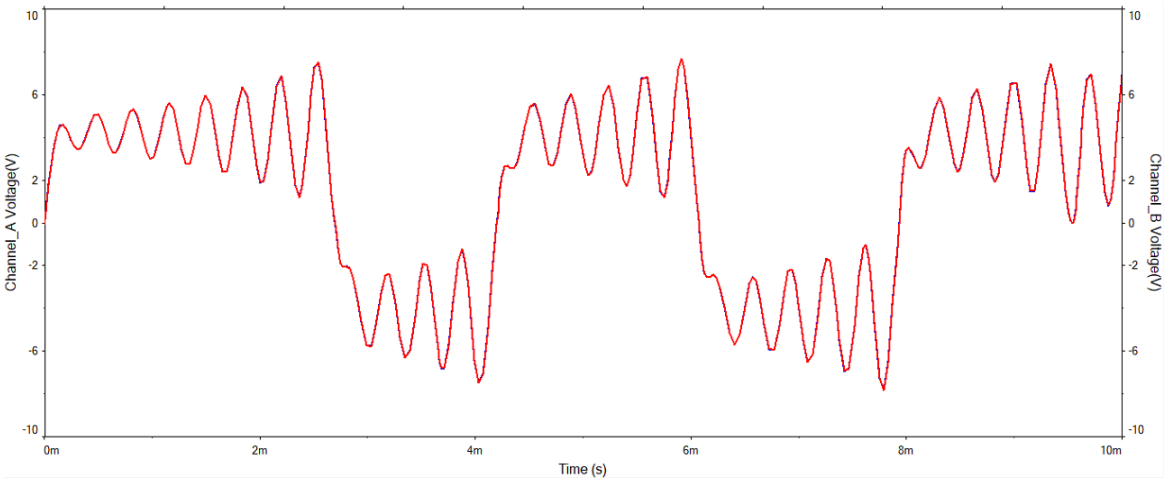


Figura 21 – Desempenho de sincronização de $y_s(t)$ (vermelho) com $y_m(t)$ (azul).

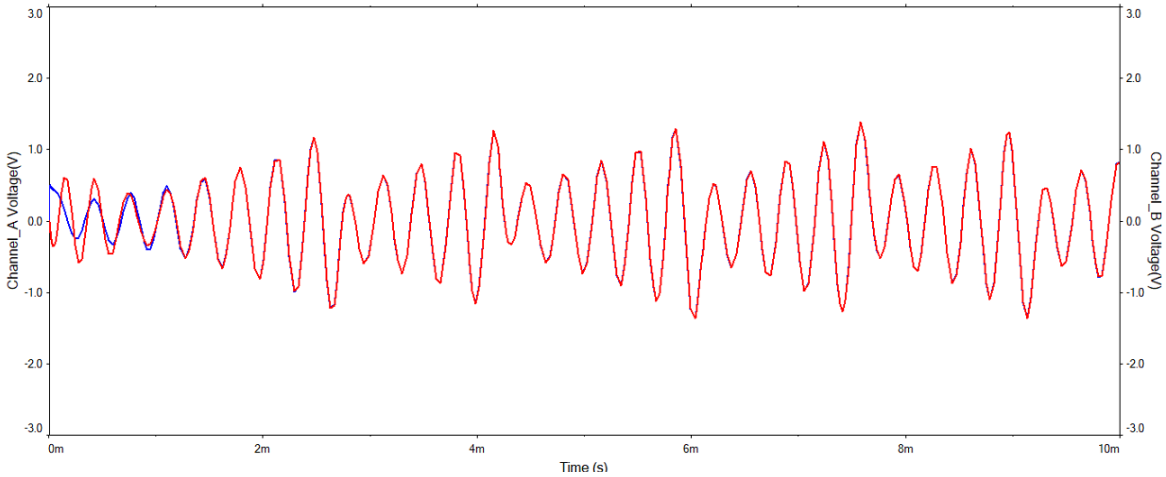
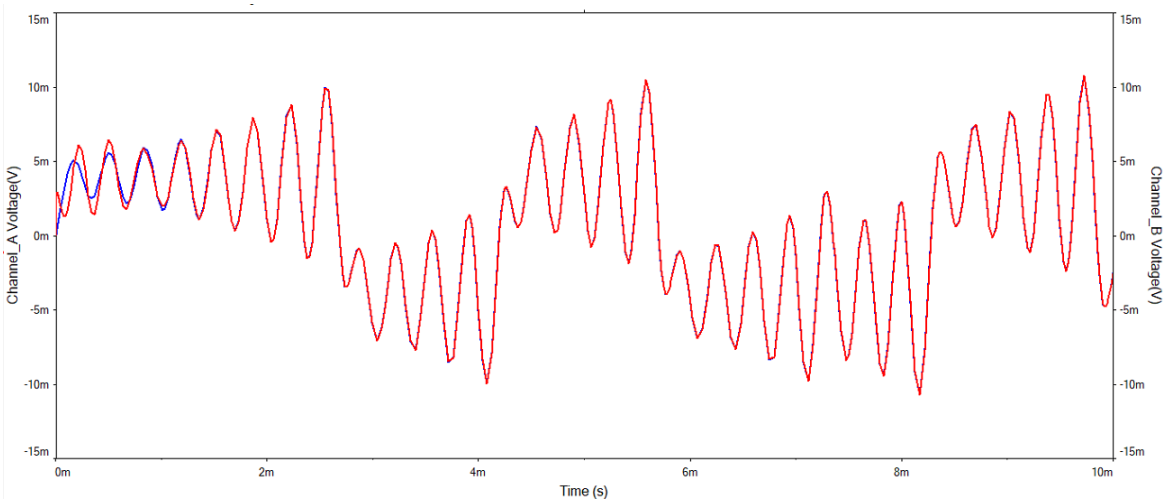


Figura 22 – Desempenho de sincronização de $z_s(t)$ (vermelho) com $z_m(t)$ (azul).



A exemplo da sincronização em Matlab/Simulink, a sincronização ocorre mais rapidamente no primeiro estado do sistema, onde o sinal de controle atua, mas também ocorre

de maneira satisfatória nos demais estados.

4.2.3 ERRO DE SINCRONIZAÇÃO

As próximas figuras (23 a 25) mostram os erros de sincronização dos três estados do sistema escravo x_s, y_s e z_s, respectivamente.

Figura 23 – Erro de sincronização entre $x_s(t)$ e $x_m(t)$.

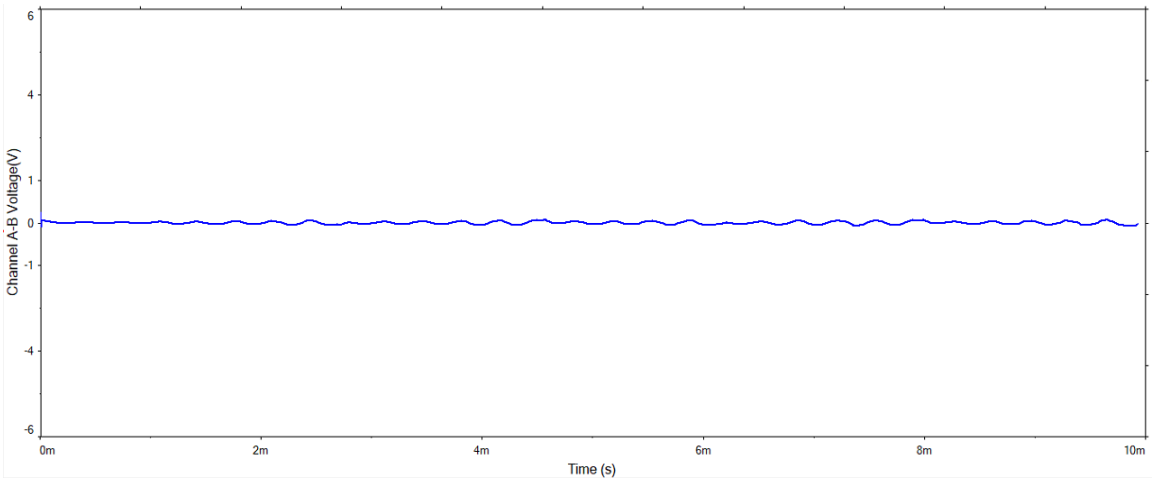


Figura 24 – Erro de sincronização entre $y_s(t)$ e $y_m(t)$.

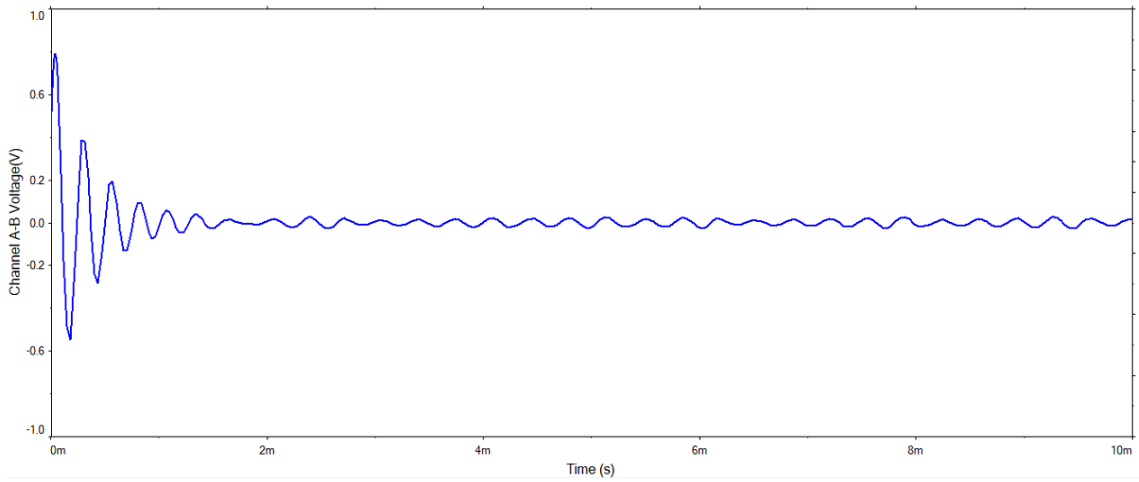
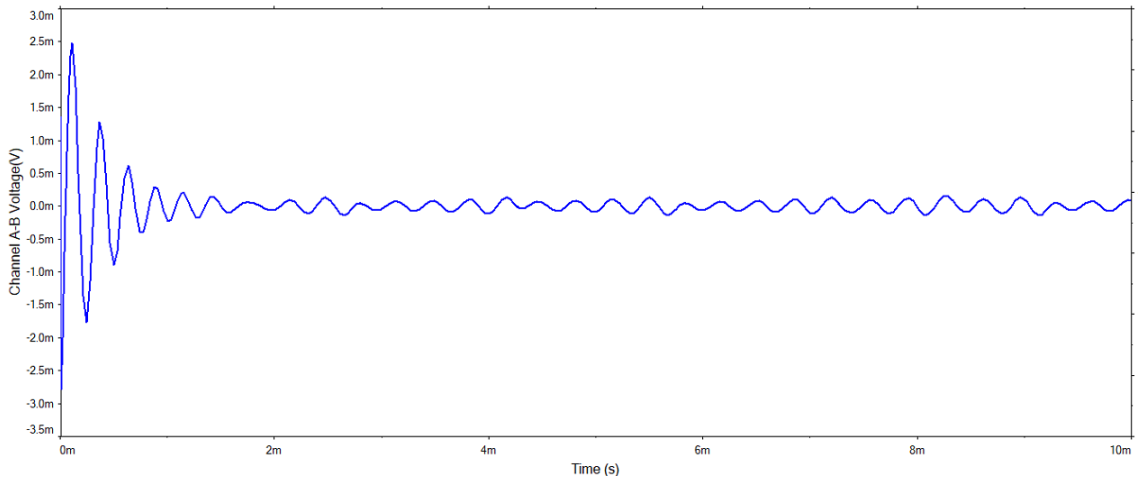


Figura 25 – Erro de sincronização entre $z_s(t)$ e $z_m(t)$.

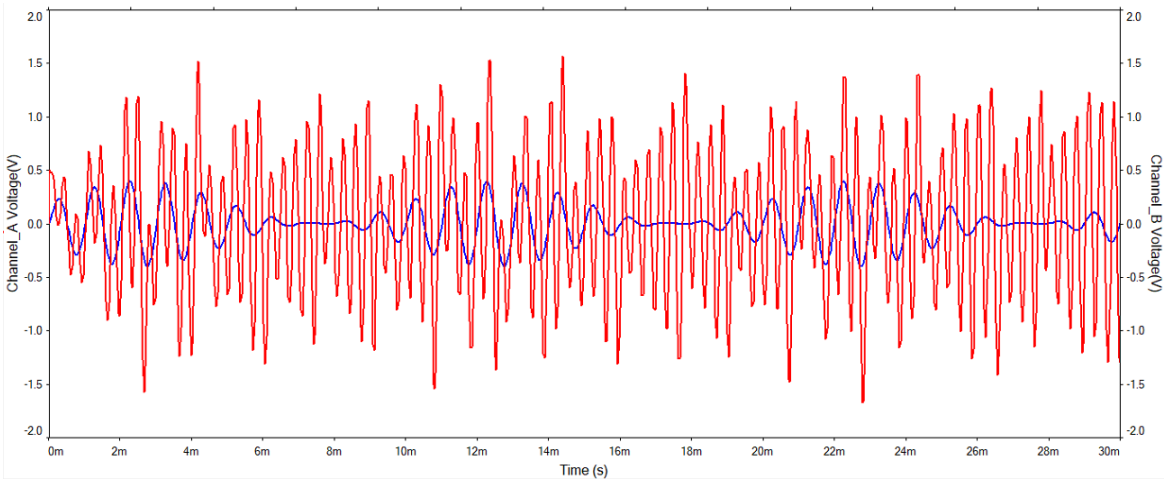


Como pode ser observado o erro de sincronização é limitado, como esperado pela teoria apresentada.

4.2.4 MENSAGEM ORIGINAL E MENSAGEM CRIPTOGRAFADA

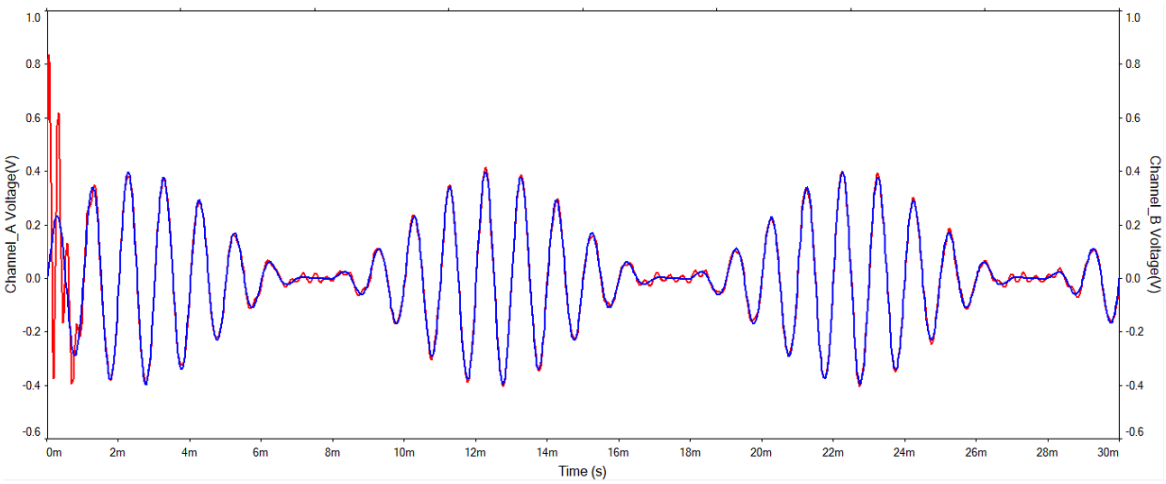
Na figura (26) a seguir é mostrado o sinal proposto como sinal de mensagem e o sinal da mensagem criptografada. A figura (27) mostra a mensagem $m(t)$ e a mensagem recuperada $m_R(t)$. Já em (28) está o erro referente a recuperação da mensagem transmitida.

Figura 26 – Mensagem original $m(t)$ (azul) e a mensagem criptografada $m_{crip}(t)$ (vermelho).



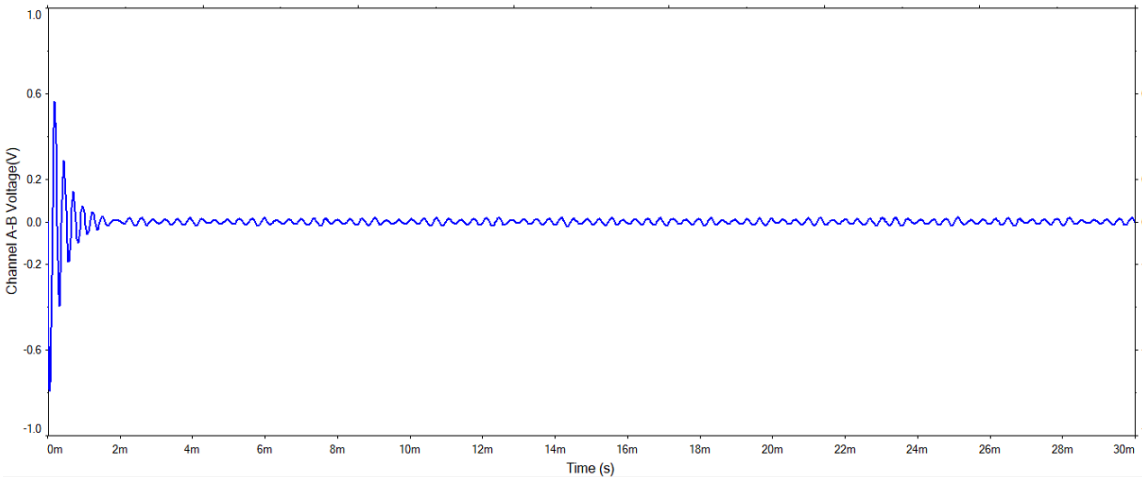
4.2.5 MENSAGEM ORIGINAL E MENSAGEM RECUPERADA

Figura 27 – Mensagem original $m(t)$ (azul) e a mensagem recuperada $m_R(t)$ (vermelho).



4.2.6 ERRO DA MENSAGEM RECUPERADA

Figura 28 – Erro entre a mensagem original $m(t)$ e a mensagem recuperada $m_R(t)$.



Note que por praticidade não foi implementado o envio simultânio de duas mensagens como realizado em MATLAB/Simulink. Note ainda que mesmo sendo considerado todos os componentes do circuito como não ideais com tolerância de 5%, o resultado da sincronização e recuperação da mensagem transmitida foi satisfatório, semelhante ao resultado obtido em MATLAB/Simulink.

5 CONCLUSÕES

Com base na teoria de estabilidade de Lyapunov, este trabalho de graduação estudou uma metodologia para a sincronização de sistemas caóticos e sua aplicação para comunicação segura, em particular foi considerado uma aplicação para o circuito caótico de Chua com controle subatuado e sujeito a distúrbios. As principais peculiaridades do esquema estudado são sua simplicidade, pois é baseado em um controle proporcional, e robustez, já que foi projetado considerando-se de maneira explícita a presença de distúrbios.

Para ressaltar sua aplicabilidade a situações práticas de interesse foi também estudado um esquema de comunicação segura. Ficou provado através da teoria de estabilidade de Lyapunov que somente é necessária a atuação na primeira equação de estado do sistema escravo para realizar a sincronização completa do circuito mestre/escravo. Foi validada a eficácia do sinal de controle a partir de simulações computacionais em MATLAB/Simulink e Multisim.

Como recomendação de trabalhos futuros fica a implementação prática do circuito apresentado desenvolvido no Multisim, uma possível utilização de redes neurais no sistema escravo para melhoria da confidencialidade e um sistema de sincronização subatuada de um sistema hipercaótico de Chua.

Esse trabalho foi apresentado em um estágio menos amadurecido no 24º Congresso de Iniciação Científica da Universidade de Brasília e 15º Congresso de Iniciação Científica do Distrito Federal, pelo programa de PIBIC/UnB 2017-2018 com titulação de “SINCRONIZAÇÃO DO CIRCUITO DE CHUA COM APLICAÇÃO PARA CRIPTOGRAFIA ANALÓGICA”, e foi agraciado com uma Menção Honrosa.

Referências

ALLIGOOD, T.; SAUER, D.; YORKE, A. **CHAOS: An Introduction to Dynamical Systems**. Springer, 1996. ISBN 0-387-94677-2. Citado nas pp. 10, 11, 14.

ASIAIN, E.; GARRIDO, R. Anti-Chaos control of a servo system using nonlinear model reference adaptive control. **Chaos, Solitons & Fractals**, Elsevier, v. 143, p. 110581, 2021. Citado na p. 11.

AWAL, N. M.; BULLARA, D.; EPSTEIN, I. R. The smallest chimera: Periodicity and chaos in a pair of coupled chemical oscillators. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP Publishing LLC, v. 29, n. 1, p. 013131, 2019. Citado na p. 11.

BOCCALETTI, S.; KURTHS, J.; OSIPOV, G.; VALLADARES, D.; ZHOU, C. The synchronization of chaotic systems. **Physics reports**, Elsevier, v. 366, n. 1-2, p. 1–101, 2002. Citado na p. 19.

BUTKEVICH, Y. R.; AFANASIEV, V. V.; LOGINOV, S. S. Communication System Based on Chaotic Masking Binary Phase Manipulation and Nonlinear Filtering. **SYNCHROINFO**, IEEE, v. 9, p. 1–4, 2021. Citado na p. 11.

CAPLIGINS, F.; LITVINENKO, A.; ABOLTINS, A.; KOLOSOVS, D. FPGA Implementation and Study of Synchronization of Modified Chua's Circuit-Based Chaotic Oscillator for High-Speed Secure Communications. **IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)**, IEEE, p. 1–6, 2021. Citado na p. 11.

CHAI, S. H.; LIM, J. S. Forecasting business cycle with chaotic time series based on neural network with weighted fuzzy membership functions. **Chaos, Solitons & Fractals**, Elsevier, v. 90, p. 118–126, 2016. Citado na p. 11.

CHEN, Y.-J.; CHOU, H.-G.; WANG, W.-J.; TSAI, S.-H.; TANAKA, K.; WANG, H. O.; WANG, K.-C. A polynomial-fuzzy-model-based synchronization methodology for the multi-scroll Chen chaotic secure communication system. **Engineering Applications of Artificial Intelligence**, Elsevier, v. 87, p. 103251, 2020. Citado na p. 11.

DEVANEY, R. **An introduction to chaotic dynamical systems**. Westview press, 2008. Citado na p. 18.

FARAH, M. B.; GUESMI, R.; KACHOURI, A.; SAMET, M. A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. **Optics & Laser Technology**, Elsevier, v. 121, p. 105777, 2020. Citado na p. 11.

GULARTE, K. H. M.; GÓMEZ, J. C. G.; VIZCARRA MELGAR, M. E.; VARGAS, J. A. R. Chaos Synchronization and its Application in Parallel Cryptography. **IEEE 5th Colombian Conference on Automatic Control (CCAC)**, IEEE, p. 198–203, 2021. Citado na p. 21.

HANIF, M.; ALI, R. A.; ABBAS, S.; KHAN, M. A.; IQBAL, N. A Novel and Efficient 3D Multiple Images Encryption Scheme Based on Chaotic Systems and Swapping Operations. **IEEE Access**, IEEE, v. 8, p. 123536–123555, 2020. Citado na p. 11.

HUESO, M.; CRUZADO, J. M.; TORRAS, J.; NAVARRO, E. ALUminating the path of atherosclerosis progression: chaos theory suggests a role for Alu repeats in the development of atherosclerotic vascular disease. **International journal of molecular sciences**, Multidisciplinary Digital Publishing Institute, v. 19, n. 6, p. 1734, 2018. Citado na p. 11.

IOANNOU, P. A.; SUN, J. **Robust adaptive control**. Courier Corporation, 2012. Citado na p. 16.

KESIĆ, S.; SPASIĆ, S. Z. Application of Higuchi's fractal dimension from basic to clinical neurophysiology: A review. **Computer Methods and Programs in Biomedicine**, Elsevier, v. 133, p. 55–70, 2016. Citado na p. 11.

KHALIL, H. K.; GRIZZLE, J. W. **Nonlinear systems**. Prentice hall Upper Saddle River, NJ, 2002. v. 3. Citado na p. 14.

KOCAMAZ, U. E.; CEVHER, B.; UYAROĞLU, Y. Control and synchronization of chaos with sliding mode control based on cubic reaching rule. **Chaos, Solitons & Fractals**, Elsevier, v. 105, p. 92–98, 2017. Citado na p. 11.

KUETCHE MBE, E.; FOTSIN, H.; KENGNE, J.; WOAFO, P. Parameters estimation based adaptive Generalized Projective Synchronization (GPS) of chaotic Chua's circuit with application to chaos communication by parametric modulation. **Chaos, Solitons & Fractals**, Elsevier, v. 61, p. 27–37, 2014. Citado nas pp. 12, 21, 22.

LING, B. W.; LU, H. H.; LAM, H. **Control of Chaos in Nonlinear Circuits and Systems**. World Scientific, 2009. ISBN 978-981-279-056-9. Citado na p. 21.

LUO, Y.; LIN, J.; LIU, J.; WEI, D.; CAO, L.; ZHOU, R.; CAO, Y.; DING, X. A robust image encryption algorithm based on Chua's circuit and compressive sensing. **Signal Processing**, Elsevier, v. 161, p. 227–247, 2019. Citado na p. 11.

MANGIAROTTI, S.; PEYRE, M.; ZHANG, Y.; HUC, M.; ROGER, F.; KERR, Y. Chaos theory applied to the outbreak of Covid-19: an ancillary approach to decision-making in pandemic context. **Epidemiology & Infection**, Cambridge University Press, p. 1–29, 2020. Citado na p. 10.

MKAOUAR, H.; BOUBAKER, O. Chaos synchronization for master slave piecewise linear systems: Application to Chua's circuit. **Communications in Nonlinear Science and Numerical Simulation**, Elsevier, v. 17, p. 1292–1302, 2012. Citado na p. 21.

MOBAYEN, S. Chaos synchronization of uncertain chaotic systems using composite nonlinear feedback based integral sliding mode control. **ISA Transactions**, Elsevier, v. 77, p. 100–111, 2018. Citado na p. 12.

MOBAYEN, S.; FEKIH, A.; VAIDYANATHAN, S.; SAMBAS, A. Chameleon Chaotic Systems With Quadratic Nonlinearities: An Adaptive Finite-Time Sliding Mode Control Approach and Circuit Simulation. **IEEE Access**, IEEE, v. 9, p. 64558–64573, 2021. Citado na p. 12.

MOBAYEN, S.; J., M. Robust finite-time composite nonlinear feedback control for synchronization of uncertain chaotic systems with nonlinearity and time-delay. **Chaos, Solitons & Fractals**, Elsevier, v. 114, p. 46–54, 2018. Citado na p. 12.

MODIRI, A.; MOBAYEN, S. Adaptive terminal sliding mode control scheme for synchronization of fractional-order uncertain chaotic systems. **ISA Transactions**, Elsevier, v. 105, p. 33–50, 2020. Citado na p. 11.

MOUTSINGA, C. R. B.; PINDZA, E.; MARÉ, E. A robust spectral integral method for solving chaotic finance systems. **Alexandria Engineering Journal**, Elsevier, v. 59, p. 601–611, 2020. Citado na p. 11.

POINCARÉ, H.; MAITLAND, F. **Science and method**. Courier Corporation, 2003. Citado na p. 10.

SCHARF, Y. A chaotic outlook on biological systems. **Chaos, Solitons & Fractals**, Elsevier, v. 95, p. 42–47, 2017. Citado na p. 11.

SPROTT, J. C. **Elegant Chaos, Algebraically Simple Chaotic Flows**. World Scientific, 2010. ISBN 981-283-881-3. Citado na p. 10.

STANKEVICH, N.; KUZNETSOV, A.; POPOVA, E.; SELEZNEV, E. Chaos and hyperchaos via secondary Neimark-Sacker bifurcation in a model of radiophysical generator. **Nonlinear dynamics**, Springer, v. 97, n. 4, p. 2355–2370, 2019. Citado na p. 10.

STROGATZ, S. H. **Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering**. CRC Press, 2018. Citado na p. 18.

VAIDYANATHAN, S.; RASAPPAN, S. Global Chaos Synchronization of n-Scroll Chua Circuit and Lur 'e System using Backstepping Control Design with Recursive Feedback. **Arabian Journal for Science and Engineering**, Springer, v. 39, p. 3351–3364, 2014. Citado na p. 11.

VARAN, M.; AKGUL, A. Control and synchronisation of a novel seven-dimensional hyperchaotic system with active control. **Pramana**, Springer, v. 90, n. 4, p. 54, 2018. Citado na p. 11.

VARGAS, J. A.; GRZEIDAK, E.; HEMERLY, E. M. Robust adaptive synchronization of a hyperchaotic finance system. **Nonlinear Dynamics**, Springer, v. 80, n. 1-2, p. 239–248, 2015. Citado na p. 11.

VASEGHI, B.; MOBAYEN, S.; HASHEMI, S. S.; FEKIH, A. Fast Reaching Finite Time synchronization Approach for Chaotic Systems With Application in Medical Image Encryption. **IEEE Access**, IEEE, v. 9, p. 25911–25925, 2021. Citado na p. 11.

WANG, N.; ZHANG, G.; KUZNETSOV N, V.; BAO, H. Hidden attractors and multistability in a modified Chua's circuit. **Communications in Nonlinear Science and Numerical Simulation**, Elsevier, v. 92, p. 105494, 2021. Citado na p. 12.

WANG, R.; ZHANG, Y.; CHEN, Y. Fuzzy neural network-based chaos synchronization for a class of fractional-order chaotic systems: an adaptive sliding mode control approach. **Nonlinear Dynamics**, Springer, v. 90, p. 1275–1287, 2020. Citado na p. 11.

WANG, S.; BEKIROS, S.; YOUSEFPOUR, A.; HE, S.; CASTILLO, O.; JAHANSHAHI, H. Synchronization of fractional time-delayed financial system using a novel type-2 fuzzy active control method. **Chaos Solitons & Fractals**, v. 136, p. 109768, 2020. Citado na p. 11.

WEN, W.; WEI, K.; ZHANG, Y. Colour light field image encryption based on DNA sequences and chaotic systems. **Nonlinear Dynamics**, Springer, v. 99, p. 1587–1600, 2020. Citado na p. 11.

ZHAO, X.; LI, Z.; LI, S. Synchronization of a chaotic finance system. **Applied Mathematics and Computation**, Elsevier, v. 217, p. 6031–6039, 2011. Citado na p. 11.

ZHILONG, L.; MA, J.; ZHANG, G.; ZHANG, Y. Synchronization control between two Chua 's circuits via capacitive coupling. **Applied Mathematics and Computation**, Elsevier, v. 360, p. 94–106, 2019. Citado na p. 11.

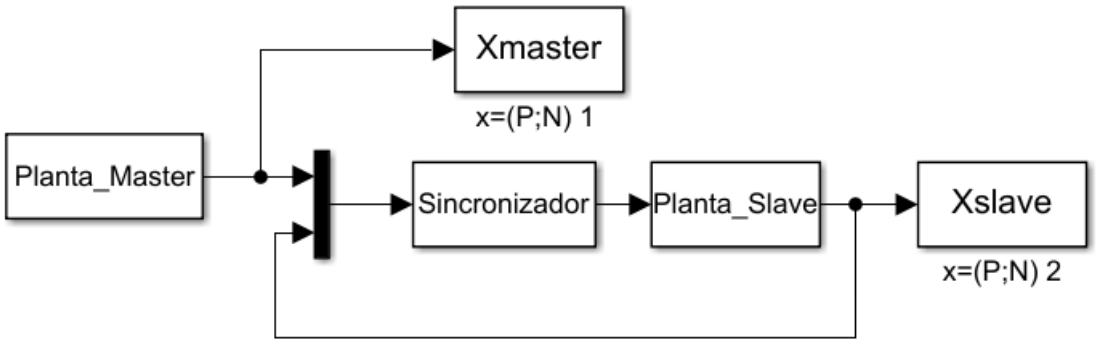
ZHOU, M.; WANG, C. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. **Signal Processing**, Elsevier, v. 171, p. 107484, 2020. Citado na p. 11.

Apêndices

APÊNDICE A – Diagrama de blocos do Simulink

Diagrama de blocos no Simulink para a simulação do esquema de sincronização para telecomunicação segura.

Figura 29 – Diagrama de blocos no Simulink.



APÊNDICE B – Códigos de programação

B.1 Código da Planta Mestre

Código B.1 – Código de Matlab

```
function [sys,x0,str,ts] = Planta_Master(t,x,u,flag)

G=0.9346; %Constantes
C1=0.15;
C2=1.5;
L=0.10;
m1=-1.4357;
m0=-0.7879;
r=0.002;

mensagem1 = 0.03*(4*sin(2*pi*0.6*t)+square(2*pi*0.4*t));
mensagem2 = 0.5*(square(cos(pi*t))+sawtooth(pi*t));

switch flag,
   %%%%%%%%%%%%%%%%%
   % Inicializacao %
   %%%%%%%%%%%%%%%%%
case 0,
  sizes = simsizes;
    sizes.NumContStates = 3; %Numero de estados constantes
    sizes.NumDiscStates = 0; %Numero de estados discretos
    sizes.NumOutputs = 3;    %Numero de saidas
    sizes.NumInputs = 0;     %Numero de entradas
    sizes.DirFeedthrough = 1;
    sizes.NumSampleTimes = 1;
    sys = simsizes(sizes);
    x0=[0.1 0.1 0]; %Condicoes iniciais
  str=[];
  ts=[0 0];
   %%%%%%%%%%%%%%
   % Diretivas  %
   %%%%%%%%%%%%%%
case 1,      %Sistema
    sys = [(G/C1)*(x(2) - x(1)) - (1/C1)*(m0*x(1) +
       ((m1-m0)*(abs(x(1)+1)-abs(x(1)-1))/2));
           (G/C2)*(x(1) - x(2)) + x(3)/C2;
           (-x(2)- r*x(3))/L];
   %%%%%%%%%%
   % Saidas %
```

```
39     %%%%%%%%%%
40 case 3,
41     sys = [x(1); x(2) + mensagem1; x(3) + mensagem2];
42     %%%%%%%%%
43     %  End  %
44     %%%%%%%%%
45 case {2,4,9},
46     sys = []; % Nao faz nada
47  otherwise
48     error(['unhandled flag = ',num2str(flag)]);
49 end
```

B.2 Código da Planta Escravo

Código B.2 – Código de Matlab

```
1  function [sys,x0,str,ts] = Planta_Slave(t,x,u,flag)
2
3  G=0.9346; %Constantes
4  C1=0.15;
5  C2=1.5;
6  L=0.10;
7  m1=-1.4357;
8  m0=-0.7879;
9  r=0.002;
10
11 disturbio1 = 0.05*sin(2*pi*20*t) + 0.1*square(2*pi*3*t);
12 disturbio2 = 0.1*cos(0.5*pi*30*t) - 0.05*square(2*pi*9*t);
13 disturbio3 = 0.15*sin(pi*100*t) - 0.15*sawtooth(2*pi*14*t);
14
15 switch flag,
16    %%%%%%%%%%%%%%%%%
17    % Inicializacao %
18    %%%%%%%%%%%%%%%%%
19 case 0,
20   sizes = simsizes;
21     sizes.NumContStates = 3; %Numero de estados constantes
22     sizes.NumDiscStates = 0; %Numero de estados discretos
23     sizes.NumOutputs = 3;    %Numero de saidas
24     sizes.NumInputs = 3;     %Numero de entradas
25     sizes.DirFeedthrough = 1;
26     sizes.NumSampleTimes = 1;
27     sys = simsizes(sizes);
28     x0=[0.2 0 0.2]; %Condicoes iniciais
29   str=[];
30   ts=[0 0];
31    %%%%%%%%%%%%%%
32    % Diretivas  %
33    %%%%%%%%%%%%%%
34 case 1,      %Sistema
```

```
35      sys = [(G/C1)*(x(2) - x(1)) - (1/C1)*(m0*x(1) +
           ((m1-m0)*(abs(x(1)+1)-abs(x(1)-1))/2)) + disturbio1 + u(1);
36              (G/C2)*(x(1) - x(2)) + x(3)/C2 + disturbio2;
37              (-x(2)- r*x(3))/L + disturbio3];
38    %%%%%%%%%%
39    % Saidas %
40    %%%%%%%%%%
41  case 3,
42    sys = x;
43    %%%%%%%%%
44    %  End  %
45    %%%%%%%%%
46  case {2,4,9},
47      sys = []; % Nao faz nada
48   otherwise
49    error(['unhandled flag = ',num2str(flag)]);
50  end
```

B.3 Código do Sincronizador

Código B.3 – Código de Matlab

```
1   function [sys,x0,str,ts] = Sincronizador(t,x,u,flag)
2
3   psi1 = 10;
4   psi2 = 20;
5   psi3 = 30;
6
7   switch flag,
8     %%%%%%%%%%%%%%%%%
9     % Inicializacao %
10    %%%%%%%%%%%%%%%%%
11  case 0,
12
13    sizes = simsizes;
14      sizes.NumContStates  = 3;   %Numero de estados constantes
15      sizes.NumDiscStates  = 0;   %Numero de estados discretos
16      sizes.NumOutputs     = 3;   %Numero de saidas
17      sizes.NumInputs      = 6;   %Numero de entradas
18      sizes.DirFeedthrough = 1;
19      sizes.NumSampleTimes = 1;
20      sys = simsizes(sizes);
21      x0=zeros(3,1);              %Condicoes iniciais
22    x0(1)=0;
23      x0(2)=0;
24      x0(3)=0;
25          str=[];
26    ts=[0 0];
27     %%%%%%%%%%%%%%
28     % Diretivas  %
```

```
29     %%%%%%%%%%%%%%
30 case 1,
31       sys = [0;
32              0;
33              0];
34     %%%%%%%%%%
35     % Saidas %
36     %%%%%%%%%%
37   case 3,     %controlador
38       sys =  [-1*(psi1*(u(4) - u(1)));
39               -0*(psi2*(u(5) - u(2)));
40               -0*(psi3*(u(6) - u(3)))];
41
42    case {2,4,9},
43    sys = [];
44
45  otherwise
46    error(['unhandled flag = ',num2str(flag)]);
47 end
```

B.4 Código dos Gráficos

Código B.4 – Código de Matlab

```
1  %Executando esse arquivo --> automaticamente mostra os graficos da
2  %simulacao e salva na pasta em formato png (poderia ser escolhido
3  %formato jpg tambem)
4  clc
5  fsize=20;
6
7  mensagem1 = 0.03*(4*sin(2*pi*0.6*t)+square(2*pi*0.4*t));
8  mensagem2 = 0.5*(square(cos(pi*t))+sawtooth(pi*t));
9
10 %Figura 1
11 fig=figure;
12 plot(t,Xmaster(:,1),t,
      Xslave(:,1),':','LineWidth',2);set(0,'DefaultAxesFontSize',16);
13 grid on
14 grid minor
15 h=legend('Mestre','Escravo','Location','southeast');
16 set(h,'FontSize',fsize);
17 set(0,'DefaultAxesFontSize', 16);
18 xlabel('Time (s)','Fontsize',fsize);
19 ylabel('$$x_{m}(t),
      x_{s}(t)$$','Interpreter','Latex','Fontsize',fsize)
20 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
21 saveas(gcf,'20s_FIG1.png');
22 close(fig)
23
24 %Figura 2
```

```
fig=figure;
plot(t,Xmaster(:,2),t,
   Xslave(:,2),':','LineWidth',2);set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Mestre','Escravo','Location','southeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (s)','Fontsize',fsize);
ylabel('$$y_{m}(t),
   y_{s}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG2.png');
close(fig)

%Figura 3
fig=figure;
plot(t,Xmaster(:,3),t,
   Xslave(:,3),':','LineWidth',2);set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (s)','Fontsize',fsize);
ylabel('$$z_{m}(t),
   z_{s}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG3.png');
close(fig)

%Figura 4
fig=figure;
aux = Xmaster(:,1) - Xslave(:,1);
plot(t,aux,'LineWidth',2);set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Erro','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (ms)','Fontsize',fsize);
ylabel('$$e_x(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG4.png');
close(fig)

%Figura 5
fig=figure;
aux = Xmaster(:,2) - Xslave(:,2);
plot(t,aux,'LineWidth',2);
set(0,'DefaultAxesFontSize',16);
grid on
```

```
grid minor
h=legend('Erro','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (ms)','Fontsize',fsize);
ylabel('$$e_y(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG5.png');
close(fig)

%Figura 6
fig=figure;
aux = Xmaster(:,3) - Xslave(:,3);
plot(t,aux,'LineWidth',2);
set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Erro','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (ms)','Fontsize',fsize);
ylabel('$$e_z(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG6.png');
close(fig)

%Figura 7
fig=figure;
aux = Xmaster(:,1) - Xslave(:,1);
aux1 = Xmaster(:,2) - Xslave(:,2);
aux2 = Xmaster(:,3) - Xslave(:,3);
plot(t,aux,t,aux1,'--',t,aux2,':','LineWidth',2);
set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('e_x(t)','e_y(t)','e_z(t)','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (ms)','Fontsize',fsize);
ylabel('$$e(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG7.png');
close(fig)

%Figura 8
fig=figure;
plot(t,mensagem1,t,Xmaster(:,2),'LineWidth',2);
set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Mensagem 1','Mensagem Criptografada
   1','Location','southeast');
```

```
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (s)','Fontsize',fsize);
ylabel('$$m_1(t)$$,
   $$m_{crip1}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG8.png');
close(fig)

%Figura 9
fig=figure;
plot(t,mensagem2,t,Xmaster(:,3),'LineWidth',2);
set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Mensagem 2','Mensagem Criptografada
   2','Location','southeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (s)','Fontsize',fsize);
ylabel('$$m_1(t)$$,
   $$m_{crip2}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG9.png');
close(fig)

%Figura 10
fig=figure;
plot(t,mensagem1,t,Xmaster(:,2) -
   Xslave(:,2),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Mensagem 1','Mensagem 1
   Recuperada','Location','southeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', 16);
xlabel('Time (s)','Fontsize',fsize);
ylabel('$$m_1(t),
   m_{1R}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'20s_FIG10.png');
close(fig)

%Figura 11
fig=figure;
plot(t,mensagem2,t,Xmaster(:,3) -
   Xslave(:,3),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
grid on
grid minor
h=legend('Mensagem 2','Mensagem 2
   Recuperada','Location','southeast');
set(h,'FontSize',fsize);
```

```
168 set(0,'DefaultAxesFontSize', 16);
169 xlabel('Time (s)','Fontsize',fsize);
170 ylabel('$$m_2(t),
       m_{2R}(t)$$','Interpreter','Latex','Fontsize',fsize)
171 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
172 saveas(gcf,'20s_FIG11.png');
173 close(fig)
174
175 %Figura 12
176 fig=figure;
177 aux = mensagem1 - (Xmaster(:,2) - Xslave(:,2));
178 plot(t,aux,'LineWidth',2);set(0,'DefaultAxesFontSize',16);
179 grid on
180 grid minor
181 h=legend('Erro Mensagem 1','Location','southeast');
182 set(h,'FontSize',fsize);
183 set(0,'DefaultAxesFontSize', 16);
184 xlabel('Time (s)','Fontsize',fsize);
185 ylabel('$$m_1(t) -
       m_{1R}(t)$$','Interpreter','Latex','Fontsize',fsize)
186 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
187 saveas(gcf,'20s_FIG12.png');
188 close(fig)
189
190 %Figura 13
191 fig=figure;
192 aux = mensagem2 - (Xmaster(:,3) - Xslave(:,3));
193 plot(t,aux,'LineWidth',2);set(0,'DefaultAxesFontSize',16);
194 grid on
195 grid minor
196 h=legend('Erro Mensagem 2','Location','southeast');
197 set(h,'FontSize',fsize);
198 set(0,'DefaultAxesFontSize', 16);
199 xlabel('Time (s)','Fontsize',fsize);
200 ylabel('$$m_2(t) -
       m_{2R}(t)$$','Interpreter','Latex','Fontsize',fsize)
201 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
202 saveas(gcf,'20s_FIG13.png');
203 close(fig)
```