

## طراحی سیستم مخابراتی امن با استفاده از سنکرون کردن سیستم‌های آشوبی

محمد نیکخو<sup>\*</sup> \*\*\* مسعود شفیعی<sup>\*</sup> \*\*\* کوروش کیانی<sup>\*</sup>

\* دانشجوی کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر

\*\* استاد، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر

\*\*\* دانشجوی کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه سمنان

### چکیده

دانش را که "سیستم‌های یقینی دارای رفتاری قابل پیش‌بینی هستند" ، زیر سوال برد. سیستم‌های آشوبی دارای چندین خاصیت قابل توجه نظیر: ارگادیک بودن<sup>۱</sup> ، تصادفی بودن، غیر تناوبی بودن، حساسیت به شرایط اولیه و غیر قابل پیش‌بینی بودن، هستند<sup>[۲]</sup> ، که آنها را برای کاربرد رمزنگاری مساعد می‌سازد. محققین براین عقیده‌اند که این خاصیت‌ها می‌توانند چندین ویژگی اولیه نظیر پخش شدگی<sup>۲</sup> و درهم‌ریختگی<sup>۳</sup> که در رمزنگاری مدرن مورد نیاز است را برآورده سازند<sup>[۳] تا [۵]</sup>.

در چنددهه اخیر، ساخت سیستم‌های رمزنگار بر مبنای تئوری آشوب توجه بسیاری را به خود جلب کرده است. این سیستم‌ها را به دو دسته کلی، سیستم‌های رمزنگاری آشوبی زمان گستته و سیستم‌های رمزنگاری آشوبی زمان پیوسته تقسیم‌بندی می‌کنند. سیستم‌های رمزنگاری آشوبی زمان گستته برای رمزنگاری اطلاعات دیجیتال از سیستم‌های آشوبی زمان گستته، معمولاً به عنوان منبع تولید کننده بیت شبه رندم، استفاده می‌کنند. استفاده از سیستم‌های آشوبی زمان گستته برای هدف رمزکردن نخستین بار توسط آقای ماتیوس<sup>۴</sup> در[۶] انجام گرفت. در این روش، یک نگاشت آشوبی تک بعدی، که برای یک محدوده از شرایط اولیه و

در این مقاله ابتدا مفهوم سنکرون کردن امن سیستم‌های آشوبی با استفاده از تکنیک‌های کنترل تطبیقی و مقاوم مورد بحث قرار گرفته است. در ادامه یک طرح مخابراتی امن جدید بر مبنای سنکرون کردن امن یک کلاس عمومی از سیستم‌های آشوبی به نام سیستم لورنیز تعمیم یافته ارائه گردیده است. این طرح مخابراتی ترکیبی از روش‌های رمزنگاری مرسوم و روش مدولاسیون آشوبی است. نتایج تحلیل‌های تئوریک و شبیه‌سازی با استفاده از سیگنال سینوسی و سیگنال صوتی و با وجود تاخیر انتشار ثابت نامشخص بین فرستنده و گیرنده بررسی شده است. همچنین مقاومت این طرح در برابر نویز گوسی کانال با واریانس<sup>۵</sup> ۱۰ نیز بررسی شده و آنالیز امنیت این سیستم مخابراتی از نقطه نظر جستجوی بروت-فورس مورد ارزیابی قرار گرفته است. با استفاده از این طرح مخابراتی طول کلید بسیار مناسبی حاصل شده است.

**کلیدواژگان:** آشوب، سیستم‌های غیرخطی، سنکرون کردن، مشاهده‌گر، مخابرات امن

### ۱- مقدمه

یکی از این پدیده‌های بسیار جالب در مبحث سیستم‌های غیرخطی، "آشوب" است. کشف آشوب این اصل اساسی

▪ نویسنده عهده‌دار مکاتبات (Nickhoo\_m@yahoo.com)

1. ergodicity  
2. Diffusion  
3. Confusion  
4. Matthews

نه تنها سیگنال پیام با سیگنال کریر آشوبی جمع می گردد، بلکه حالت های سیستم آشوبی توسط سیگنال پیام از طریق یک روند معکوس پذیر مدوله می گردد به نحوی که سیگنال آشوبی تولید شده ذاتاً شامل اطلاعات سیگنال پیام است [۱۳و۱۶]. در روش سوم، که به نام سویچینگ آشوبی است نیازمند دو سیستم آشوبی برای بیت های صفر و یک هستیم. سیگنال ارسالی توسط سویچ بین این دو سیستم آشوبی بر اساس اینکه صفر یا یک سیگنال پیام منتقل می گردد انتخاب می گردد [۱۹و۲۰].

اگرچه بکارگیری سیستم های آشوبی به صورت شبیه سازی و ساخت افزاری با موفقیت انجام شد، ولی کاربردهای اولیه سیستم های آشوبی برای مخابرات امن دارای سطح پایینی از امنیت بودند از آنجایی که فرد مهاجم می توانست با بکارگیری تکنیک های مختلف برداشتن ماسک از سیگنال ارسالی سیگنال پیام را بازسازی نماید [۲۱]. برای چیز شدن بر این مسئله، روش های مختلف برای بهبود امنیت سیستم های رمز نگارانه شده است. برای مثال، یک طرح رمز نگاری پیشرفته با استفاده از سیگنال های آشوبی چند کانه در [۲۲] ارائه شده است و در [۲۰و۲۳] نویسندهاگان به یک ایده برای انتقال امن سیگنال پیام با در نظر گرفتن این نکته که رمز نگاری سیگنال آشوبی به اندازه رمز نگاری سیگنال پیام اهمیت دارد دست یافتند. برای این منظور روش رمز نگاری مرسوم و سنکرون کردن آشوب با یکدیگر برای طراحی سیستم رمز نگار آشوبی ترکیب شدند.

با این وجود، از آنجایی که همه سیستم های مخابراتی امن آشوبی، که در بالا اشاره گردید، بر مبنای ویژگی سنکرون کردن سیستم های آشوبی ساده هستند، نکته کلیدی برای این روش ها امنیت سنکرون کردن است. متاسفانه این مسئله در گذشته برای طرح های سنکرون کردن مورد توجه قرار نمی گرفت. برای مثال، در [۲۴]، محققین تئوری سنکرون کردن مقاوم و سنکرون کردن تطبیقی را برای رفتار کردن با مسائل مربوط به پارامترهای ناشناخته یا عدم تطبیق پارامترها در نظر گرفته اند. از آنجایی که مقدار پارامترهای سیستم آشوبی معمولاً به عنوان "کلید" محرمانه برای سنکرون کردن بین فرستنده و گیرنده در نظر گرفته می شوند، این روش های مقاوم و تطبیقی امکانی را برای اندازه گیری کلید به ما می دهند. به این معنا که با استفاده از تکنیک های تطبیقی و مقاوم، مهاجم قادر است بدون دانش دقیق از "کلید" یک سیستم گیرنده طراحی کند، و با فرستنده سنکرون کند. در این زمینه، مفهوم سنکرون کردن امن با توجه به روش های کنترل مقاوم و تطبیقی در [۲۵] توضیح داده است.

پارامترهای کنترلی دارای رفتار آشوبی است، برای تولید یک دنباله ای از اعداد شبه رندم برای رمز نگاری و رمز گشایی پیام مورد استفاده قرار می گیرد. اندکی بعد از آن، در سال ۱۹۹۰، یک سیستم رمز نگار بر مبنای نگاشت تن [۱ آشوبی تکمای خطی که توسط آقای هابوتسو<sup>۱</sup> و همکارانش توسعه یافت ایجاد گردید [۷]، در این مقاله پارامتر نگاشت تن به عنوان یک کلید محرمانه مورد استفاده قرار گرفت و رمز نگاری و رمز گشایی به ترتیب توسط تکرار معکوس و مستقیم نگاشت تن آشوبی حاصل می گشت. تعداد بسیار زیاد دیگری از الگوریتم های رمز نگاری آشوبی گشته در چند سال اخیر پیشنهاد شده اند، که برای نمونه می توان به مراجع [۸و۹] مراجعه کرد.

سیستم رمز نگار آشوبی زمان پیوسته، اساساً جهت تولید سیگنال آشوبی شبه نویز، غیر متناوب، باند وسیع برای مخابرات امن مورد استفاده قرار می گیرد، در حالیکه سیگنال های پیام معمولاً سیگنال های پیوسته بوده که درون سیگنال آشوبی در سمت فرستنده مخفی می گردد، و در سمت گیرنده این سیگنال های پیام توسط فرایند سنکرون کردن بازیابی می شوند.

ایده استفاده از سیستم های آشوبی سنکرون برای مخابرات امن ابتدا توسط پکورا و کارول ارائه گردید [۱۰]. این دو گزارش کردن که سیستم های آشوبی خاصی می توانند به دو زیر سیستم درایو و زیر سیستم پاسخ پایدار تجزیه گردند. این دو زیر سیستم با استفاده از یک سیگنال درایو مشترک با یکدیگر کوپل شده اند. بر طبق مفهوم درایو-پاسخ پکورا و کارول، چندین سیستم مخابراتی امن با موفقیت طراحی گردید [۱۱و۱۳]. به علاوه بر اساس تئوری پایداری لیاپانوف، روش فیدبک حالت خطی یا غیر خطی، روش مفید دیگری برای سنکرون کردن دو سیستم آشوبی ایزوله شده برای کاربرد مخابرات امن در مقاله [۱۴] پیشنهاد شد. روش طراحی مشاهده گر حالت غیر خطی برای مسئله سنکرون کردن آشوبی یک کلاس از سیستم های آشوبی در [۱۵و۱۶] ارائه شده است.

بر طبق این رهیافت ها، روش های مخابرات امن آشوبی را می توان به انواع ماسک زدن آشوبی<sup>۲</sup>، مدولاسیون آشوبی<sup>۳</sup> و سویچینگ آشوبی<sup>۴</sup> تقسیم بنده نمود. در روش اول، سیگنال پیام محرمانه فقط با سیگنال کریر آشوبی جمع می گردد [۱۷و۱۸]. در روش دوم،

1. Tent Map

2. Habutsu

3. Chaotic Masking

4. Chaotic Modulation

5. Chaotic Switching

$$\lim_{t \rightarrow \infty} \|x(t) - \hat{x}(t)\| \geq K(\bar{\mu} - \tilde{\mu}) \quad (4)$$

سپس سنکرون کردن امن به این صورت تعریف می‌گردد که، هم امن ضد تطبیقی و هم امن ضد مقاوم باشد. روشی است که، برای هر طرح سنکرون کردن، امن ضد تطبیقی نشان‌دهنده این است که، اگر پارامتر  $\mu$  به عنوان کلید محربانه در نظر گرفته شود، نبایستی هیچ راهی وجود داشته باشد که یک مهاجم بتواند با استفاده از تکنیک طراحی مشاهده‌گر تطبیقی به آن دست یابد. به علاوه، امن ضد مقاوم به این معناست که برای هر روش سنکرون کردن با استفاده از یک پارامتر کلید تخمین‌زده شده، یک عدم دقت به اندازه کافی بزرگ از پارامترهای تخمین بایستی منجر به خطای سنکرون کردن به اندازه کافی بزرگ گردد. بنابراین هر دو ویژگی امنیتی ضد مقاوم و ضد تطبیقی از طرح سنکرون کردن، برای مقاومت در برابر هجوم قاطع هستند. برای اینکه این دو ویژگی تضمین می‌کنند که فقط یک شخص که دقیقاً کلید محربانه را می‌شناسد قادر باشد یک مشاهده‌گر برای ساختن سیستم سنکرون - ساز طراحی نماید.

سیستم لورنز تعمیم یافته<sup>۳</sup> و شکل تبدیل شده آن، که به نام فرم کانونیکال مشاهده‌گر نامیده می‌شود را در نظر بگیرید [۲۵]:

$$\dot{\eta} = A\eta + F(\eta, y) \quad (5)$$

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \quad \text{که } \eta = [\eta_1 \quad \eta_2 \quad \eta_3]^T \text{ حالت سیستم و}$$

$$F(\eta, y) = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - 0.5(k+1)(\eta_1)^3 \\ K(k)(\eta_1)^2 \end{bmatrix}$$

$$K(k) = \frac{\lambda_3(k+1) - 2k\lambda_2 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}, \quad k \in (-1, \infty)$$

از آنجایی که نشان‌دهنده یک کلاس خیلی عمومی از سیستم‌های آشوبی با فقط یک پارامتر است، می‌خواهیم از آن برای طراحی سیستم مخابراتی بر مبنای سنکرون کردن امن استفاده کنیم.

اکنون سیستم (۵) با نمودار محدود شده آن ( $\eta(t)$  و  $y$  به  $t \geq t_0$ ) را به عنوان سیستم درایو و حالت اول  $\eta$  که به عنوان سیگنال درایو برای درایو کردن سیستم پاسخ انتخاب می‌شود را در نظر بگیرید.

سیستم درایو به صورت ذیل قابل نمایش است:

$$\begin{aligned} \dot{\eta} &= A\eta + F(\eta, y) \\ y &= C^T\eta \end{aligned} \quad (6)$$

در حالیکه  $C^T = [1 \quad 0 \quad 0]$ . توجه کنید که، برای سیستم درایو (۶)، جفت  $(C^T, A)$  مشاهده‌پذیر نیست اما آشکارا پذیر است، که

در ادامه این مقاله در بخش ۲ طرح سنکرون کردن امن مورد استفاده در سیستم مخابراتی امن پیشنهادی فرموله می‌گردد. در بخش ۳ طرح مخابراتی امن پیشنهادی ارائه گردیده و در بخش ۴ نتایج شبیه سازی با سیگنال‌های مختلف آمده است. در بخش ۵ آنالیز امنیت با روش جستجوی بروت-فورس و در بخش ۶ نتیجه‌گیری آورده شده است.

## ۲- طرح سنکرون کردن امن مورد استفاده در سیستم مخابراتی امن پیشنهادی

واضح است که اگر یک طرح سنکرون کردن که برای مخابرات امن استفاده می‌شود به راحتی آسیب‌پذیر باشد نامطلوب است. برای فهم این موضوع، مفهوم سنکرون کردن امن را، با توجه به طرح-های کنترل مقاوم و کنترل تطبیقی ارائه می‌دهیم [۲۵]. برای شروع تعریف سنکرون کردن سیستم‌های آشوبی را در تئوری کنترل ارائه می‌نماییم.

سیستم آشوبی غیرخطی را با بردار پارامتر  $\mu$  در نظر بگیرید:

$$\dot{x} = f(x, t, \mu) \quad (1)$$

در حالیکه  $x \in \mathbb{R}^n$  و  $\mu \in \mathbb{R}^m$  است.

تعریف ۱: گوییم سیستم (۱) به سنکرون شدن با حل  $x(t), t \geq t_0$  دست پیدا کرده است، اگر یک خروجی کمکی  $y = y(x) \in \mathbb{R}^p$  و  $p < n$  وجود داشته باشد، به نحوی که با این خروجی، سیستم (۱) دارای مشاهده‌گر مجازی فرم ذیل برای حل  $: x(t), t \geq t_0$

$$\dot{\hat{x}} = f(\hat{x}, t, \mu) + \phi(y(x), y(\hat{x}), \hat{x}, \mu) \quad (2)$$

باشد در حالیکه  $x, \hat{x} \in \mathbb{R}^n$  و  $\mu \in \mathbb{R}^m$  است.

تعریف ۲: گوییم سنکرون کردن به صورت امن ضد تطبیقی<sup>۱</sup> نسبت به پارامتر  $\mu$  است اگر هیچ مشاهده‌گر تطبیقی به شکل (۲) با  $\mu = \hat{\mu}, \hat{\mu} \in \mathbb{R}^m$  وجود نداشته باشد به نحوی که بتواند از الگوریتم تطبیقی ذیل حاصل شود.

$$\dot{\hat{\mu}} = \psi(\hat{\mu}, y(x), y(\hat{x}), \hat{x}, t) \quad (3)$$

تعریف ۳: گوییم سنکرون کردن به صورت امن ضد مقاوم<sup>۲</sup> نسبت به پارامتر  $\mu$  است، هر گاه یک ثابت مثبت  $K$  وجود داشته باشد به نحوی که برای هر  $\bar{\mu}$  و  $\tilde{\mu}$  از یک مجموعه بسته داده شده و برای هر حل سیستم (۱) با  $\bar{\mu} = \mu$  و مشاهده‌گر (۲) با  $\tilde{\mu} = \mu$  داشته باشیم:

استفاده قرار گیرد. سپس، سیگنال پیش رمز کننده،  $E(t)$ ، با سیگنال کلید دوم  $k_2(t)$ ، که متغیر حالت دیگر سیستم آشوبی است، برای رمز کردن بیشتر جمع می شود. این مجموع به سیستم گیرنده از طریق کانال عمومی انتقال داده می شود، در حالیکه دوباره به سیستم آشوبی فرستنده فیدبک می گردد. سیستم گیرنده، مشابه قسمت فرستنده، شامل یک سیستم آشوبی و طرح رمزگشایی است. با استفاده از "کلید" کاملاً مشابه برای پارامترهای سیستم آشوبی، سنکرون کردن بین فرستنده و گیرنده قابل دستیابی است. دو سیگنال کلید،  $k_1(t)$  و  $k_2(t)$ ، دقیقاً مشابه آنچه که توسط سیستم فرستنده استفاده می شود، دوباره توسط طرح سنکرون کردن بازسازی می گردد. طرح رمزگشایی از این کلیدها سیگنال پیام  $P(t)$  را بازیابی می کند.

سیستم آشوبی استفاده شده توسط معادله (۶) با اندکی تغییرات به صورت معادله (۱۰) داده شده است:

$$(10)$$

$$\begin{aligned} \dot{\eta} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta \\ &+ \begin{bmatrix} (\lambda_1 + \lambda_2)y(t) \\ -\lambda_1\lambda_2y(t) - (\lambda_1 - \lambda_2)\eta_3y(t) - 0.5(k+1)(y(t))^3 \\ K(k)(y(t))^2 \end{bmatrix} + LE(t) \\ y &= \eta_1 + E(t) \end{aligned}$$

$E(t) \in \Re$  سیگنال پیش رمز شده است که از طرح رمز نگاری خارج می شود.  $L = [L_1 \ L_2 \ 0]^T$  یک بردار بهره است.  $\eta_1(t)$  را به عنوان سیگنال کلید  $k_2(t)$  در نظر می گیریم، سپس جمع  $k_2(t)$  و  $k_1(t)$  را به نام  $y(t) \in \Re$  می نامیم که به عنوان سیگنال پیش رمز کننده  $E(t)$  را به این شکل داریم. برای درایو کردن گیرنده به کار می رود. برای طرح رمز نگاری، از آنجایی که جزء سوم متغیرهای حالت سیستم آشوبی،  $\eta_3$ ، فقط آشکار پذیر است و مشاهده پذیر نمی باشد، از آن به عنوان سیگنال کلید دیگر  $k_1(t)$  کمک گرفته ایم. این کار سطح امنیت سیستم رمز کننده پیشنهاد شده را افزایش می دهد. سیگنال پیام با استفاده از رمز شیفت دهنده  $n$  تابی<sup>۱</sup> توصیف شده در [۲۲] پیش رمز می گردد. رمز شیفت دهنده  $n$  تابی به صورت رابطه (۱۱) نشان داده می شود:

$$E(t) = \underbrace{f(\dots f(f(p(t), k_1(t)), k_1(t)), \dots, k_1(t))}_n \quad (11)$$

که  $f$  یک تابع غیر خطی داده شده توسط رابطه

$$f(x, k) = \begin{cases} (x+k) + 2h, & -2 \leq (x+k) \leq -h \\ (x+k), & -h \leq (x+k) \leq h \\ (x+k) - 2h, & h \leq (x+k) \leq 2h \end{cases} \quad (12)$$

نشان می دهد امکان طراحی سیستم پاسخ به صورت مشاهده گر برای سنکرون کردن سیستم (۶) وجود دارد. اکنون سیستم ذیل را به عنوان یک پاسخ در نظر بگیرید:

$$\begin{aligned} \dot{\hat{\eta}} &= A\hat{\eta} + F(\hat{\eta}, y) + L(\hat{\eta}_1 - \eta'_1) \\ &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} (\lambda_1 + \lambda_2)\eta'_1 \\ -\lambda_1\lambda_2\eta'_1 - (\lambda_1 - \lambda_2)\eta'_1\hat{\eta}_3 - 0.5(k+1)(\eta'_1)^3 \\ K(k)(\eta'_1)^2 \end{bmatrix} + \begin{bmatrix} I_1 \\ I_2 \\ 0 \end{bmatrix} (\hat{\eta}_1 - \eta'_1) \end{aligned} \quad (7)$$

در حالیکه  $[I_1 \ I_2 \ 0]^T = [\hat{\eta}_1 \ \hat{\eta}_2 \ \hat{\eta}_3]^T$  و  $\eta'_1 = \begin{bmatrix} \hat{\eta}_1 & \hat{\eta}_2 & \hat{\eta}_3 \end{bmatrix}^T$  با  $0$  است. به علاوه،  $\eta'_1$  سیگنال درایو ورودی است، که ممکن است توسط نویز در طول فرایند ارسال با پاسخ شود. با فرض  $\varepsilon < \|\eta_1(t) - \eta'_1(t)\|$  که عیک ثابت مثبت کوچک است، تئوری ذیل به دست می آید:

تئوری ۱ [۲۵]: یک سیستم درایو داده شده توسط (۶) و یک سیستم پاسخ بر مبنای مشاهده گر توسط (۷) را در نظر بگیرید. رابطه زیر به صورت نمایی در زمان برقرار است:

$$\lim_{t \rightarrow \infty} \|\eta(t) - \hat{\eta}(t)\| \leq D\varepsilon \quad (8)$$

در حالیکه  $D$  برخی ثابت های مثبت است. مخصوصاً، اگر  $\eta'_1$  باشد، سیستم پاسخ (۷) به صورت مجانبی سرتاسری سیستم درایو (۶) را سنکرون می سازد، به این معنی که :

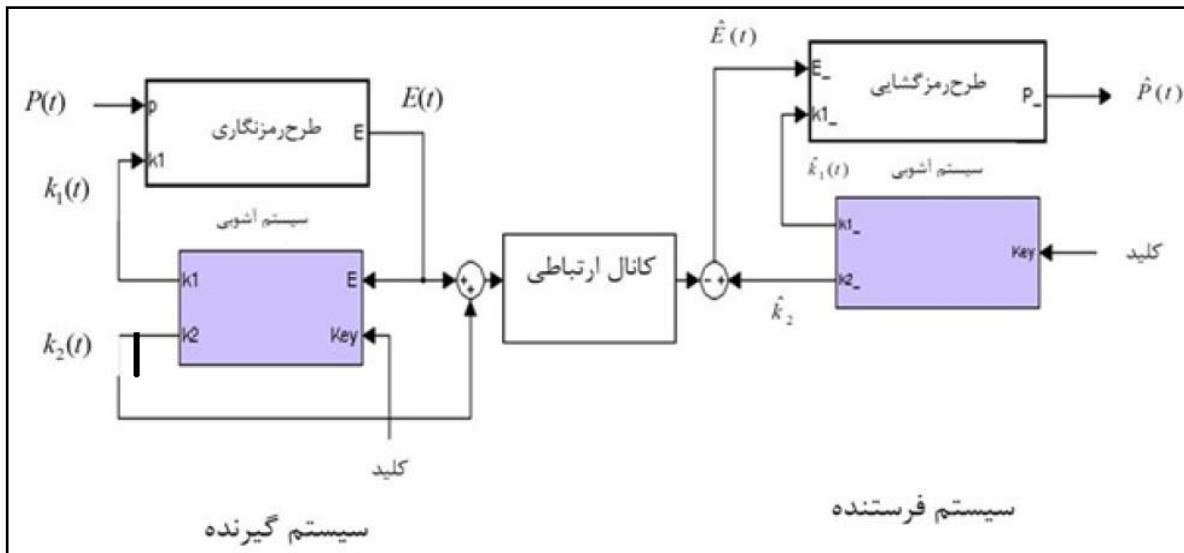
$$\lim_{t \rightarrow \infty} \|\eta(t) - \hat{\eta}(t)\| = 0 \quad (9)$$

به علاوه در [۲۵] اثبات شده که سیستم لورنر تعیین یافته هم خاصیت امن ضد مقاوم و هم امن تطبیقی را برآورده می سازد، لذا برای کاربرد مخابرات امن مناسب به نظر می رسد.

### ۳- طرح مخابراتی امن پیشنهادی

در طرح مخابراتی پیشنهادی از تکنیک رمز نگاری مرسوم همراه با مدولاسیون آشوبی برای رمز نگاری بیشتر استفاده شده است. شکل (۱) بلوك دیاگرام سیستم رمز کننده پیشنهاد شده را نشان می دهد، که شامل یک ماژول رمز کننده (فرستنده)، یک کانال مخابراتی عمومی و یک ماژول رمزگشایی (گیرنده) است. همانطوری که شکل نشان می دهد، فرستنده شامل یک سیستم آشوبی و طرح رمز نگاری است. "کلید" مجرمانه  $Key \equiv \{k, \lambda_1, \lambda_2, \lambda_3\}$ ، که در شکل (۱) نشان داده شده است، برای تنظیم مقادیر پارامترهای سیستم آشوبی استفاده شده است. سیستم آشوبی برای تولید کردن دو سیگنال کلید  $k_1(t)$  و  $k_2(t)$  استفاده شده است. سیگنال کلید اول،  $k_1(t)$ ، یک متغیر حالت سیستم آشوبی است، که بایستی توسط طرح رمز کننده به سیگنال پیام پیش رمز کننده،  $P(t)$ ، مورد

1. n-shift cipher



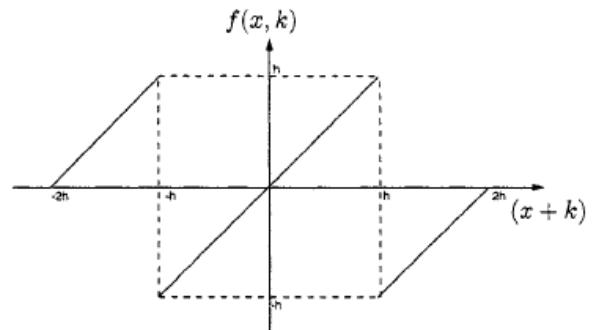
شکل ۱ بلوک دیاگرام سیستم مخابراتی امن جدید

که  $y$  سیگنال دریافت شده و  $L$  بردار بهره مشابه با آن بهره‌ای است که در سیستم فرستنده استفاده شد. بر این عقیده‌ایم که سنکرون شدن فقط زمانی قابل دستیابی است که "کلید" مشابهی در هر دو قسمت فرستنده و گیرنده مورد استفاده قرار گیرد. بنابراین سیگنال‌های کلید که به نام  $k_1(t)$  و  $k_2(t) \rightarrow \hat{k}_1(t)$  و  $\hat{k}_2(t) \rightarrow k_2(t)$  هستند زمانی که  $t$  به سمت بی‌نهایت می‌رود می‌توانند دوباره تولید گردند. سرانجام، طرح رمزگشایی متناظر به صورت رابطه (۱۴) قابل نمایش است:

$$\hat{p}(t) = f(\underbrace{f(\dots f}_{n}(\hat{E}(t), -\hat{k}_1(t)), -\hat{k}_1(t), \dots, -\hat{k}_1(t))) \quad (14)$$

که  $\hat{k}_1(t) = y(t) - \hat{E}(t)$  است. تئوری (۲) را در این مورد بیان می‌کنیم:  
تئوری ۲: فرض کنید که سیگنال پیام،  $P(t)$ ، از طریق سیستم مخابراتی شامل فرستنده با سیستم آشوبی (۱۰) و طرح رمزگاری (۱۱)، و گیرنده با سیستم آشوبی (۱۳) و طرح رمزگاری (۱۴) منتقل شده باشد. با استفاده از "کلید" مشابه هم در سیستم فرستنده و هم در گیرنده یک سنکرون کردن عمومی بین سیستم فرستنده و گیرنده قابل دستیابی است و سیگنال پیام،  $P(t)$ ، به صورت کامل در سمت گیرنده قابل بازسازی است.

اثبات: خطای سنکرون کردن  $\eta(t) = \hat{\eta}(t) - \tilde{\eta}(t)$  را تعریف می‌کنیم در حالیکه  $[\tilde{\eta}_1 \quad \tilde{\eta}_2 \quad \tilde{\eta}_3]^T = \tilde{\eta}$  و داریم:



شکل ۲ تابع مورد استفاده در پیش رمز کننده

است. جاییکه  $h$  پارامتر ثابت انتخاب شده به نحوی است که  $x(t)$  و  $(-h, h)$  بین  $k(t)$  و  $(-h, h)$  قرار بگیرند. این تابع در شکل (۲) نشان داده شده است.

در رمز شیفت‌دهنده  $n$  تایی، سیگنال کلید  $k_i(t)$ ،  $i = 1, 2, \dots, n$  بار برای رمزکردن سیگنال پیام استفاده شده است. از آنجایی که سیگنال پیش‌رمزکننده یک تابعی از  $P(t)$  و  $k_i(t)$  است، و علاوه بر آن سیگنال پیش‌رمزکننده دوباره برای رمزگاری بیشتر توسعه سیگنال کلید دوم که  $k_2(t)$  است مدوله می‌گردد، لذا مشخصات استاتیک و دینامیک  $P(t)$  و  $k_1(t)$  هردو مخفی می‌گردند. به صورت مشابه، سیستم سنکرون آشوبی در قسمت گیرنده به صورت رابطه (۱۳) قابل بازسازی است:

$$\begin{aligned} \dot{\tilde{\eta}} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \tilde{\eta} \\ &+ \begin{bmatrix} (\lambda_1 + \lambda_2)y(t) \\ -\lambda_1\lambda_2y(t) - (\lambda_1 - \lambda_2)\hat{\eta}_3y(t) - 0.5(k+1)(y(t))^3 \\ K(k)(y(t))^2 \end{bmatrix} + L(y(t) - \hat{\eta}_1) \end{aligned} \quad (13)$$

$$\hat{p}(t) = \underbrace{f(\dots f(f(E(t), -K_1(t)), -K_1(t)), \dots, -K_1(t))}_n \quad (20)$$

سیستم (۲۰) روش معکوس طرح رمزنگاری (۱۱) است، این امر نشان می دهد که سیگنال اطلاعات نهایتاً می تواند بازیابی شود.

در هر سیستم مخابراتی واقعی، همیشه یک تاخیر زمانی انتشار در طول فرایند انتقال سیگنال های پیام از فرستنده به گیرنده وجود دارد. از نقطه نظر تئوری کنترل، تاخیر زمانی ممکن است باعث ناپایداری سیستم مخابراتی گردد [۲۶]. همانطور که در کار [۲۷] می بینیم که وجود تاخیر زمانی در سیستم سنکرون شده ممکن است منجر به از بین رفتن فرایند سنکرون شدن شود. حال سنکرون کردن فرستنده و گیرنده برای سیستم مخابراتی با یک زمان تاخیر ثابت نامشخص را تعریف می کنیم:

تعریف ۴ [۲۸]: حالت سیستم گیرنده در زمان  $t$  به صورت مجانبی با سیستم فرستنده در زمان  $t - \tau_d$  سنکرون می گردد، اگر

$$\lim_{t \rightarrow \infty} \|x(t - \tau_d) - \hat{x}(t)\| = 0$$

در حالیکه  $\tau_d$  یک تاخیر زمانی ثابت نامشخص است و  $x(t)$  و  $\hat{x}(t)$  به ترتیب حالت سیستم گیرنده و فرستنده هستند. فرض کنیم که یک زمان تاخیر انتشار ثابت نامشخص،  $\tau_d$ ، برای انتقال سیگنال پیام از فرستنده به گیرنده وجود دارد. این بدان معناست که، در زمان  $t - \tau_d$ ، سیگنال انتقال از فرستنده منتقل شده است. سیگنال انتقال تاخیر دار توسط گیرنده در زمان  $t$  دریافت خواهد شد. سپس سیستم آشوبی (۱۰) در سمت فرستنده به صورت زیر بازنویسی می گردد:

$$\begin{aligned} i\dot{\eta}(t - \tau_d) &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta(t - \tau_d) + LH(t - \tau_d) \\ &\quad + \begin{bmatrix} (\lambda_1 + \lambda_2)y(t - \tau_d) \\ -\lambda_1\lambda_2y(t - \tau_d) - (\lambda_1 - \lambda_2)\eta_3y(t - \tau_d) - 0.5(k+1)(y(t - \tau_d))^3 \\ K(k)(y(t - \tau_d))^2 \end{bmatrix} \\ y(t - \tau_d) &= \eta(t - \tau_d) + E(t - \tau_d) \end{aligned} \quad (21)$$

جاییکه  $L$  بردار بهره مشاهده گر و  $E(t - \tau_d)$  خروجی طرح رمزنگاری است. درینجا نیز از همان طرح رمزنگاری (۱۱) استفاده می شود. سیستم آشوبی در سمت گیرنده، توسط سیگنال تاخیر دار ( $y(t - \tau_d)$ ) برای هدف سنکرون کردن درایو

$$\begin{aligned} \dot{\tilde{\eta}}_1(t) &= \dot{\eta}_1(t) - \dot{\hat{\eta}}_1(t) \\ &= \eta_2(t) + (\lambda_1 + \lambda_2)(\eta_1(t) + E(t)) + L_1 E(t) \\ &\quad - \dot{\hat{\eta}}_2(t) - (\lambda_1 + \lambda_2)(\eta_1(t) + E(t)) - L_1(\eta_1(t) + E(t) - \hat{\eta}_1(t)) \\ &= -L_1(\eta_1(t) - \hat{\eta}_1(t)) + \eta_2(t) - \dot{\hat{\eta}}_2(t) \\ &= -L_1\tilde{\eta}_1(t) + \tilde{\eta}_2(t) \end{aligned} \quad (15)$$

$$\begin{aligned} \dot{\tilde{\eta}}_2(t) &= \dot{\eta}_2(t) - \dot{\hat{\eta}}_2(t) \\ &= (-\lambda_1\lambda_2 - (\lambda_1 - \lambda_2)\eta_3(t))(\eta_1(t) + E(t)) \\ &\quad - 0.5(k+1)(\eta_1(t) + E(t))^3 + L_2 E(t) \\ &\quad - (-\lambda_1\lambda_2 + (\lambda_1 - \lambda_2)\dot{\eta}_3(t))(\eta_1(t) + E(t)) \\ &\quad + 0.5(k+1)(\eta_1(t) + E(t))^3 - L_2(\eta_1(t) + E(t) - \hat{\eta}_1(t)) \\ &= -(\lambda_1 - \lambda_2)(\eta_1(t) + E(t))\tilde{\eta}_3(t) - L_2\tilde{\eta}_1(t) \\ &= -L_2\eta_1(t) + (\lambda_1 - \lambda_2)(\eta_1(t) + E(t))\tilde{\eta}_3(t) \end{aligned} \quad (16)$$

$$\begin{aligned} \dot{\tilde{\eta}}_3(t) &= \dot{\eta}_3(t) - \dot{\hat{\eta}}_3(t) \\ &= \lambda_3\eta_3(t) + K(k)(\eta_1(t) + E(t))^2 - \lambda_3\dot{\eta}_3(t) - K(k)(\eta_1(t) + E(t))^2 \\ &= \lambda_3\tilde{\eta}_3(t) \end{aligned} \quad (17)$$

با توجه به نامساوی [۲۵]  $\lambda_1 > -\lambda_2 > -\lambda_3 > 0$  شرط وجود آشوب در سیستم لورنر تعیین یافته است معادله (۱۸) برآورده می گردد:

$$\lim_{t \rightarrow \infty} \|\tilde{\eta}_3(t)\| = 0 \quad (18)$$

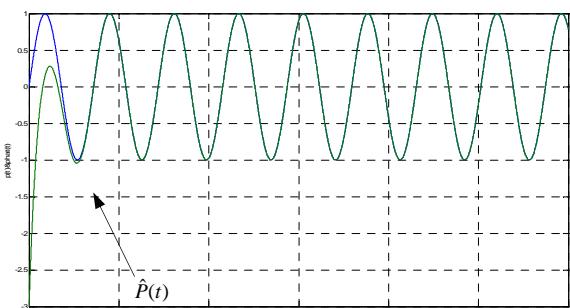
باتوجه به  $\bar{\eta}(t) = [\tilde{\eta}_1(t) \quad \tilde{\eta}_2(t)]^T$ ، داریم:

$$\begin{aligned} \dot{\bar{\eta}}(t) &= \begin{bmatrix} \dot{\tilde{\eta}}_1(t) \\ \dot{\tilde{\eta}}_2(t) \end{bmatrix} \\ &= \begin{bmatrix} -L_1 & 1 \\ -L_2 & 0 \end{bmatrix} \bar{\eta}(t) + \begin{bmatrix} 0 \\ (\lambda_1 - \lambda_2)(\eta_1(t) + E(t)) \end{bmatrix} \tilde{\eta}_3(t) \\ &= S \bar{\eta}(t) + \phi(t) \tilde{\eta}_3(t) \end{aligned} \quad (19)$$

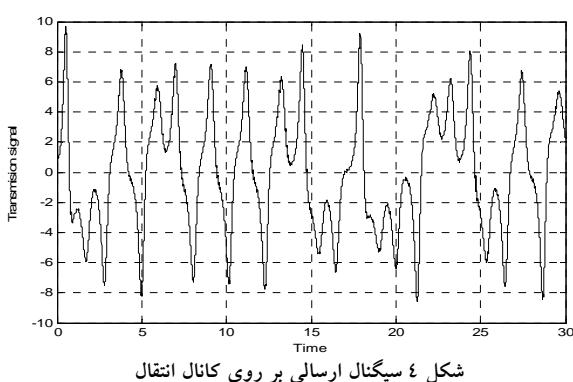
که  $\phi(t) = \begin{bmatrix} 0 \\ (\lambda_1 - \lambda_2)(\eta_1(t) + E(t)) \end{bmatrix}$  و  $S = \begin{bmatrix} -L_1 & 1 \\ -L_2 & 0 \end{bmatrix}$  تابع محدود شده هستند. از آنجایی که  $\phi(t)$  و  $\tilde{\eta}_3(t)$  محدود شده هستند، پس اگر  $L_{1,2}$  را بتوانیم به نحوی انتخاب کنیم که  $S$  یک ماتریس هرویتز باشد، خطای سنکرون کردن به صورت نمایی به سمت صفر میل خواهد کرد. به محض اینکه سنکرون شدن بین فرستنده و گیرنده بدست آید، سیستم آشوبی در سمت گیرنده قادر است سیگنال های کلید را مشابه با سیگنال های استفاده شده در سمت فرستنده تولید کند یعنی اینکه  $\lim_{t \rightarrow \infty} \hat{k}_2(t) \rightarrow k_2(t)$  و  $\lim_{t \rightarrow \infty} \hat{k}_1(t) \rightarrow k_1(t)$ . این بدان معناست که

$\lim_{t \rightarrow \infty} \hat{E}(t) = y(t) - \hat{k}_2(t) = E(t) + k_2(t) - \hat{k}_2(t) \rightarrow E(t)$  و طرح رمزگشایی (۱۴) را می توان به صورت ذیل نوشت:

پیام که یکی سیگنال سینوسی و دیگری سیگنال صوت است برای شبیه سازی انتخاب شده است. پارامترهای سیستم آشوبی به صورت  $\lambda_1 = 8$ ،  $\lambda_2 = -16$ ،  $\lambda_3 = -2$  و  $k = 0$  تنظیم شده‌اند. سیگنال پیام به عنوان یکتابع سینوسی  $L = [5 \quad 8 \quad 0]^T$ ،  $P(t) = \sin(0.5\pi t)$ ، و بردار بهره به صورت  $[5 \quad 8 \quad 0]^T$  انتخاب می‌شود، با بکار بردن این بهره‌ها ماتریس  $S$  در (۱۹) هرویتز است. برای هدف رمزگذاری و رمزگشایی،  $h = 10$  و  $n = 30$  برای رمز شیفت‌دهنده  $n$  تایی (۱۱) و (۱۴) انتخاب شده‌اند. شکل (۳) سیگنال رمزنشده اصلی  $P(t)$  و سیگنال دریافت شده  $\hat{P}(t)$  را با استفاده از کلید مشابه در گیرنده و فرستنده نشان می‌دهد. شکل (۴) سیگنال انتقال داده شده آشوبی را نشان می‌دهد. در مرحله بعد بخشی از یک سیگنال صدا را با پسوند (Wave). به عنوان سیگنال پیام انتخاب کردۀ ایم در این شبیه‌سازی از "کلید" مشابه برای فرستنده و گیرنده استفاده کردۀ ایم. شکل (۵) سیگنال صدای اصلی و صدای بازیابی شده را نشان می‌دهد.



شکل ۳ سیگنال پیام ارسالی و سیگنال پیام بازیابی شده با کلید مشابه



شکل ۴ سیگنال ارسالی بر روی کانال انتقال

در شبیه سازی بعدی تاثیر نویز کانال انتقال بر روی بازسازی سیگنال پیام مورد بررسی قرار گرفته است. در این راستا با استفاده از پیام سینوسی مورد استفاده در شبیه سازی اول و پارامترهای مشابه با آن و نویز کانال به صورت گوسی با

خواهد شد، به نحوی که سیستم (۱۳) به صورت رابطه (۲۲) قابل بازنویسی است:

$$\begin{aligned} \dot{\hat{\eta}}(t) &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta}(t) + L(y(t-\tau_d) - \hat{y}(t)) \\ &\quad + \begin{bmatrix} (\lambda_1 + \lambda_2)y(t-\tau_d) \\ -(\lambda_1\lambda_2 + (\lambda_1 - \lambda_2)\hat{\eta}_3(t))y(t-\tau_d) - 0.5(k+1)(y(t-\tau_d))^3 \\ K(k)(y(t-\tau_d))^2 \end{bmatrix} \\ \hat{y}(t) &= \hat{\eta}_1(t) \end{aligned} \quad (22)$$

جاییکه  $y(t-\tau_d)$  سیگنال دریافت شده و  $L$  بردار بهره مشابه با چیزی است که در سیستم فرستنده استفاده شده بود.

اگر سیستم (۲۱) با سیستم (۲۲) سنکرون گردد،  $\lim_{t \rightarrow \infty} \|x(t-\tau_d) - \hat{x}(t)\| = 0$  و داریم:

$$\begin{aligned} \hat{\eta}_1(t) &\rightarrow \eta_1(t-\tau_d) \quad \text{و} \quad \hat{\eta}_3(t) \rightarrow \eta_3(t-\tau_d) \\ \text{رمزگشایی} &\text{متناظر به صورت زیر قابل بازنویسی است:} \\ \hat{p}(t) &= f(\underbrace{\dots f(f(\hat{E}(t), -\hat{\eta}_3(t)), -\hat{\eta}_3(t)), \dots, -\hat{\eta}_3(t)}_n) \end{aligned} \quad (23)$$

در حالیکه  $\hat{p}(t)$  سیگنال پیام بازیابی شده است، که مشابه با سیگنال پیام اصلی ولی با تاخیر  $\tau_d$  است. حال ثابت می‌کنیم که، با انتخاب مناسب بردار بهره مشاهده  $L$ ، سیستم (۲۲) می‌تواند با (۲۱) همانطوری که در نتیجه ذیل توضیح داده شده است سنکرون گردد.

نتیجه تئوری ۲: فرض کنید که سیگنال پیام،  $p(t)$ ، از طریق یک سیستم مخابراتی امن شامل یک سیستم فرستنده با سیستم آشوبی (۲۱) و طرح رمزگذاری (۱۱)، و سیستم گیرنده با سیستم آشوبی (۲۲) و طرح رمزگشایی (۲۳) باشد. همچنین یک تاخیر زمانی انتشار نامشخص اما ثابت،  $\tau_d$ ، در طول فرایند انتقال درگیر است. با استفاده از "کلید" مشابه در سیستم فرستنده و گیرنده، سنکرون کردن فرستنده و گیرنده قابل دستیابی است، و سیگنال پیام،  $p(t)$ ، در سمت گیرنده، با زمان تاخیر  $\tau_d$  دوباره به صورت کامل بازیابی می‌گردد. اثبات: کافیست خطای سنکرون کردن را به صورت  $\tilde{\eta}(t) = \eta(t-\tau_d) - \hat{\eta}(t)$  تعریف کنیم و بقیه مراحل اثبات مشابه تئوری ۲ قابل انجام است.

#### ۴- نتایج شبیه سازی

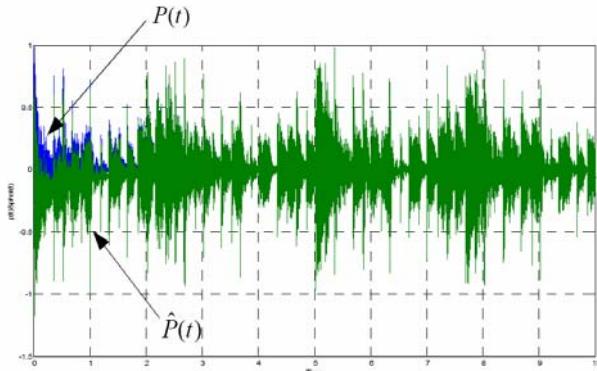
برای بررسی عملکرد سیستم مخابراتی امن پیشنهادی دو نوع

واریانس  $10^{-3}$  شبیه سازی را انجام داده ایم. شکل (۶) سیگنال ارسالی و بازیابی شده با توجه به نویز کanal را نشان می دهد. با توجه به شکل می توانیم ببینیم که مقاومت طرح پیشنهادی در مقابل نویز کanal مناسب است و بازسازی به خوبی انجام می گیرد. برای توصیف عملکرد سیستم مخابراتی امن که با یک تاخیر زمانی نامشخص در طول فرایند انتقال درگیر است، زمان تاخیر به صورت  $\tau_d = 0.5$  (sec) در نظر گرفته شده است. با استفاده از "کلید" مشابه برای هر دو سیستم فرستنده و  $p(t)$  گیرنده شبیه سازی انجام شده است. شکل (۷) سیگنال پیام اصلی و سیگنال بازیابی شده  $\hat{P}(t)$  را نشان می دهد. با توجه به شکل می توان دید که، وقتی یکبار سنکرون شدن بین سیستم های فرستنده و گیرنده حاصل شود، سیگنال پیام اصلی  $p(t)$  با موفقیت ولی با تاخیر  $\tau_d$  قابل بازیابی است.

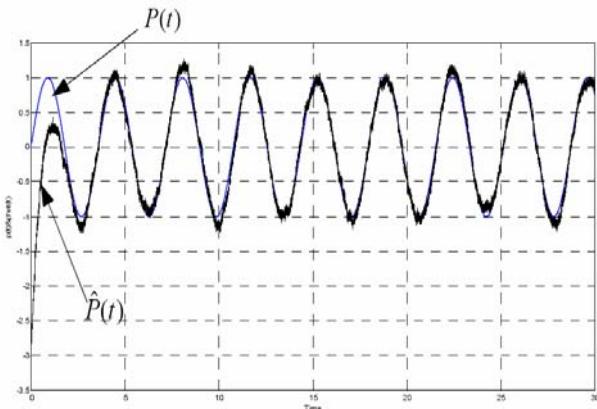
## ۵- آنالیز امنیت سیستم

از نقطه نظر رمزگاری، براساس [۲۰]، امنیت سیستم رمزگاری تابعی از دو چیز است: قدرت الگوریتم و طول کلید. در بخش ۲، مشخصات امنیت در طرح سنکرون کردن آشوب برای سیستم های مخابراتی امن از نقطه نظر تئوری کنترل، مورد بحث قرار گرفت. از آنجایی که سیستم مخابراتی امن پیشنهاد شده در طرح سنکرون کردن، هم دارای مشخصات امن ضد مقاوم و هم امن ضد تطبیقی است، بنابراین می تواند سیستم را از حمله مهاجمان حفظ کند. این بدان معناست که الگوریتم استفاده شده در سیستم مخابراتی امن پیشنهاد شده به اندازه کافی مناسب است. اکنون توجه خود را به آنالیز مشخصه امنیت دیگری از سیستم مخابراتی امن پیشنهاد شده که طول کلید نامیده می شود معطوف می کنیم.

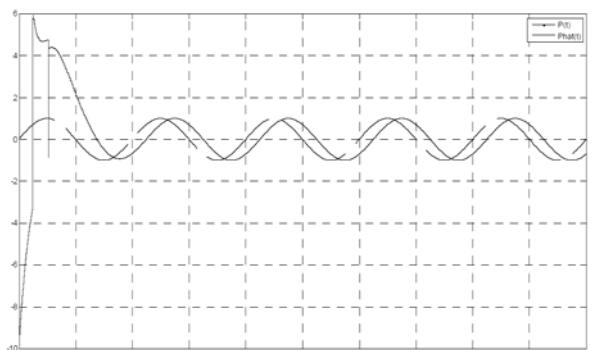
مجموعه "کلید" مورد استفاده در طرح مخابراتی همان پارامترهای سیستم آشوبی به صورت  $\text{Key} \equiv \{k, \lambda_1, \lambda_2, \lambda_3\}$  هستند. طرح مخابراتی امن پیشنهاد شده را با بکارگیری یک "کلید" غلط در سیستم گیرنده با خطاهای مختلف در تخمین تنظیمات پارامتر شبیه سازی کرده ایم. سیگنال پیام به صورت تابع سینوسی  $P(t) = \sin(0.5\pi t)$  انتخاب شده است. با محاسبه مقدار  $RMS$  خطای بازسازی سیگنال پیام و با توجه به اینکه فقط یکی از پارامترها در فرستنده و گیرنده متفاوت انتخاب شده است شبیه سازی انجام شده است. پارامترهای سیستم و بردار بهره  $L$  مانند شبیه سازی اول انتخاب شده است. شکل (۸) اثر خطای تخمین در پارامتر  $\lambda_3$  و نرم  $RMS$  خطای ایجاد شده را



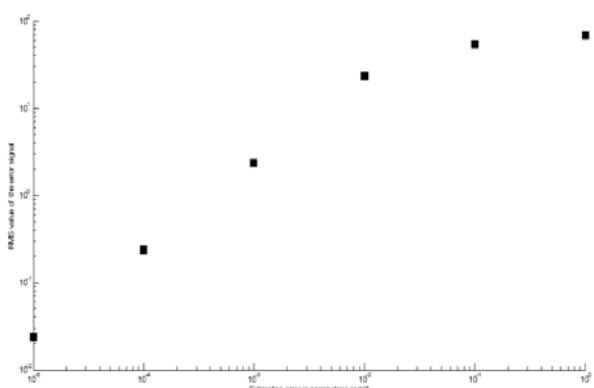
شکل ۵ سیگنال صوت ارسالی و سیگنال بازیابی شده



شکل ۶ سیگنال ارسالی و بازیابی شده در حضور نویز کanal



شکل ۷ سیگنال ارسالی و بازیابی شده در سیستم مخابراتی با تاخیر زمانی

شکل ۸ خطای تخمین در پارامتر  $\lambda_3$

پیشنهادی بر روی پارامتر تاثیرگذار دیگر یعنی طول "کلید" انجام گرفت و طول کلیدی برابر با  $2^{69}$ <sup>69</sup> بدست آمد. با توجه به روش جستجوی بروت-فورس که در جدول(۱) ارائه گردیده است این طول کلید برای یک سیستم رمزنگار بسیار مناسب است.

### مراجع

- [1] Lasota A. and M.C.Mackey, "Chaos,Fractals, and Noise- Stochastic Aspects of Dynamics ." Springer-Verlag, Second Edition, New York, 1997
- [2] Robert C.Hilborn, "Chaos and Nonlinear Dynamics",Second Edition,Department of Physics Amherst Collage,2000
- [3] Kocarev L., G.Jakimoski, T.Stojanovski, and U.Parlitz, "From Chaotic Maps to Encryption Schemes." In Proceedings IEEE International Symposium Circuits and Systems, Vol.4, pp. 514-517, 1998
- [4] K. Elissa, "Title of paper if known," unpublished.
- [5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
- [6] Matthews R.A.J., "On the Derivation of a Chaotic Encryption Algorithm." Cryptologia XIII, Vol .1 , pp. 29-42, 1989
- [7] Habutsu H.,Y.Nishio,I.Sasase and S.Mori, "A Secret Key Cryptosystem by Iterating a Chaotic Map,Advances in Cryptology ",proceedings of EuroCrypt91,Vol .547,pp.127-140,1991
- [8] Masuda N., and K.Aihara, "Cryptosystems with Discretized Chaotic Maps." IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .49 , pp. 28-40, 2002
- [9] Li S., X.Mou, and Y.Cia, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Application in Stream-Ciphers Cryptography. ", Progress in Cryptology-INDOCRYPT 2001,Lecture Notes in Computer Science, Vol .2247 , pp. 316-329, 2001
- [10] Pecora L.M. and T.L.Carroll , " Synchronization in Chaotic Systems", Physical Review Letters , Vol.64,pp.821-824,1990
- [11] Chua L.O., L.J. Kocarev, K.Eckert, and M.Itoh, "Experimental Chaos Synchronization in Chua Circuit.", International Journal of Bifurcation and Chaos, Vol .2 , pp. 705-708, 1992
- [12] Oppenheim A.V., G.W.Wornell, S.H.Isabelle, and K.M.Cuomo, "Signal Processing in the Context of Chaotic Signals.", In Proceedings IEEE ICASSP, Vol .4 , pp. 117-120, 1992
- [13] Halle K.S., C.W.Wu, M.Itoh, and L.O.Chua, "Spread Spectrum Communication Through Modulation of Chaos.", International Journal of Bifurcation and Chaos, Vol .3 , pp. 469-477, 1993
- [14] Wu C.W., and L.O.Chua, "A Unified Framework for Synchronization and Control of Dynamical Systems.", International Journal of Bifurcation and Chaos, Vol .4 , pp.979-998, 1994
- [15] Grassi G. and S.Mascolo , "Non-Linear Observer Design to Synchronize Hyper-chaotic Systems via a Scalar Signal", IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .44(10),pp.1011-1014,1997

بر روی نمودار لگاریتمی نشان می دهد. شکل (۸) نشان می دهد که خطای تخمین می دهد که خطای تخمین پارامتر  $\beta$  به مقدار کم می دهد که خطای تخمین پارامتر  $\beta$  به مقدار کم  $10^5$  باعث خطای رمزگشایی نسبتاً بزرگی می گردد. با شبیه‌سازی‌های مشابه برای پارامترهای دیگر، این مقدار برای  $k$  برابر  $10^6$  و برای پارامترهای  $\beta$  برابر با  $10^5$  می گردد. این بدان معناست که، از نقطه نظر رمزنگاری، اندازه فضای کلید سیستم مخابراتی امن پیشنهاد شده از

$$10^{21} \approx 2^{69} = 10^6 \times 10^5 \times 10^5 = 10^{21}$$

با درنظر گرفتن جستجوی بروت-فورس<sup>1</sup> هر کلید ممکن سیستم مخابراتی امن موثرترین روش در برابر شکسته شدن است. جدول (۱) زمان مورد نیاز برای اینکه سیگنال پیام با فضای کلید داده شده با استفاده از یک ماشین جستجویی که در هر ثانیه 100 میلیون کلید را تولید می کند بازیابی شود خلاصه کرده است. با توجه به جدول فوق طول کلید سیستم مخابراتی امن پیشنهاد شده از نظر رمزنگاری مناسب است. با توجه به این موضوع، سیستم مخابراتی امن پیشنهاد شده می تواند سطح نسبتاً بالایی از امنیت را برای انتقال سیگنالهای پیام به ما بدهد.

### ۶- نتیجه گیری

در این مقاله یک طرح مخابراتی امن جدید ارائه گردید که در مقایسه با مقالات قبلی از نقطه نظر امنیت الگوریتم خواص امن ضد مقاوم و امن ضد تطبیقی را برآورده می سازد. از طریق تئوری (۲) امکان سنکرون شدن فرستنده و گیرنده اثبات گردید. نتایج شبیه‌سازی طرح پیشنهادی بر روی سیگنال سینوسی و سیگنال صوت با موفقیت انجام گرفت. همچنین نتایج تئوری و شبیه‌سازی با توجه به تاخیر انتشار ثابت بین فرستنده و گیرنده انجام گرفته است. پس از آن مقاومت طرح مخابراتی پیشنهادی در برابر نویز گوسی با واریانس<sup>3</sup> ۱۰ با استفاده از شبیه‌سازی بررسی گردید و نتایج بسیار خوبی در بازیابی سیگنال پیام حاصل شد. در انتها آنالیز امنیت سیستم

جدول ازمان‌های جستجوی کلید بروت-فورس  
برای اندازه‌های مختلف کلید

اندازه کلید	زمان مورد نیاز	ساعت	روز	سال	۵۸۴۹/۴	۳۴/۵	۳/۱	۲ <sup>69</sup>
۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰

1. Brute-force

- [23] Grassi G. and S.Mascolo ,“A System Theory Approach for Designing Cryptosystems Based on Hyperchaos.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .46(9),pp.1135-1138,1999
- [24] Suykens J.A.K., P.F. Curran, and L.O. Chua, “Robust Synthesis for Master-Slave Synchronization of Lure Systems.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .46 , pp. 841-850, 1999
- [25] Celikovsky S. and G.Chen,“Secure Synchronization of a Class of Chaotic Systems From a Nonlinear Observer Approach”, IEEE Transactions on Automatic Control, Vol .50,pp.76-82,2005
- [26] Kamen E.W., “Linear Systems with Commensurate Time Delays:Stability and Stabilization Independent of Delay”, IEEE Transactions on Automatic Control.,Vol. 27, pp.367-375,1982
- [27] Chen H. and J.Liu, “Open-Loop Chaotic Synchronization of Injection-Locked Semiconductor Lasers with Gigahertz Range Modulation.”, IEEE Journal of Quantum Electronics,Vol. 36, pp.27-34, 2000
- [28] Jiang G.P., W.X.Zheng and G.Chen, “Global Chaos Synchronization with Channel Time-Delay.”, Chaos Solution and Fractals,Vol. 20, pp.267-275, 2004
- [29] Schneier B. “Applied Cryptography : Protocols , Algorithms ,and Source Code in C”, John Wiley and Sons ,Inc.,New York ,second edition,1996.
- [16] Liao T.L. and N.S.Huang ,“An Observer-Based Approach for Chaotic Synchronization with Application to Secure Communication”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .46,pp.1144-1150,1999
- [17] Pecora L.M. and T.L.Carroll , “ Synchronization in Chaotic Systems”, Physical Review Letters , Vol.64,pp.821-824,1990
- [18] Lian K.Y., P.Liu, T.S.Chiang, “Adaptive Synchronization Design for Chaotic Systems via a Scalar Driving Signal.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .49, pp.17-27,2002
- [19] Kolumban G., M.P.Kennedy, and L.O.Chua, “The Role of Synchronization in Digital CommunicationUsing Chaos—Part I:Fundamentals of Digital Communications.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .44, pp.927-936, 1997
- [20] Murali K., H. Yu, V.Varadan, H.Leung ,“Secure Communication Using a Chaos Based Signal Encryption Scheme.”, IEEE Transactions on Consumer Electronics, Vol .47, pp.709-714, 2001
- [21] Short k., “Unmasking a modulated Chaotic Communication Scheme.” International Journal of Bifurcation and Chaos, Vol .6 , pp. 367-375, 1996
- [22] Yang T., C.W. Wu, and L.O. Chua,“Cryptography Based on Chaotic Systems”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .44,pp.469-472,1997