УДК 621.373

КРИПТОСИСТЕМА ЗВ'ЯЗКУ НА СХЕМІ ЧУА

І. Булюк, Я. Матвійчук

Національний університет "Львівська політехніка"
вул. Бандери, 12, 79013 Львів, Україна
matv@ua.fm

Описано зразок системи зв'язку з маскуванням інформаційного сигналу псевдовипадковим сигналом схеми Чуа. Запропоновано синхронізацію схем Чуа в передавачі та приймачі.

Ключові слова: криптосистема зв'язку, схема Чуа, синхронізація.

У 1963 р. Г. Лоренц запропонував просту модель гідродинаміки у вигляді системи звичайних нелінійних диференціальних рівнянь зі сталими коефіцієнтами, яка була першим прикладом дивного атрактора [4].

Системи називають атракторами, якщо перехідні відхилення загасають і система "притягується" до одного з трьох положень рівноваги: точка, періодичний рух (граничний цикл), квазіперіодичний рух.

Дивні атрактори – це така коливна система, у якій нема положення рівноваги, а траєкторії в просторі станів "намотуються" на область притягання без замикання. Рухи дивного атрактора є випадковими. Ознаки його такі: нема положення рівноваги; спектр коливань вихідного сигналу наближається до спектра випадкового процесу; автокореляційна функція вихідного сигналу швидко спадає. Найменші зміни початкових умов спричиняють суттєві зміни форми генерованого сигналу дивного атрактора [4].

Схема на рис. 1 запропонована професором Каліфорнійського університету Л. Чуа (L. Chua) 1971 р. Схема Чуа – це проста детермінована система, здатна реалізувати хаотичні рухи [2].

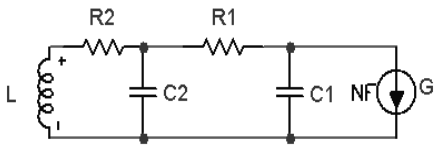

Рис. 1. Схема Чуа.

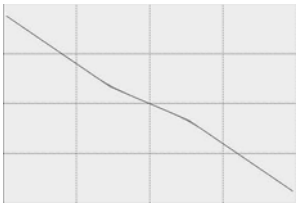

Рис. 2. ВАХ опору NF(G).

У схемі Чуа, крім звичайних лінійних елементів, є нелінійний негативний опір NF(G), що має вольт-амперну характеристику (ВАХ), якісно зображену на рис. 2. Цей опір називають діодом Чуа. За певних співвідношень параметрів у схемі можуть виникати дивні атрактори, інакше схема є звичайним автогенератором [3].

Сучасні криптосистеми використовують генератори хаосу, що є детермінованими системами з шумоподібними, хаотичними сигналами. Генератори хаосу формують несучі та модульовані коливання криптосистеми. Часто генератори хаосу є цифровими. Як низькочастотний аналоговий генератор хаосу в системах захисту інформації з успіхом використовують схему Чуа [1].

Криптосистема зі схемою Чуа. Розглянемо найпростіший алгоритм передавання інформації із застосуванням генераторів хаосу [1]. Інформаційний сигнал $s_1(t)$ підсумовують з вихідним сигналом $y_1(t)$ генератора хаосу в передавачі (рис. 3). Сумарний сигнал $s_1(t)+y_1(t)$ передають у канал зв'язку.

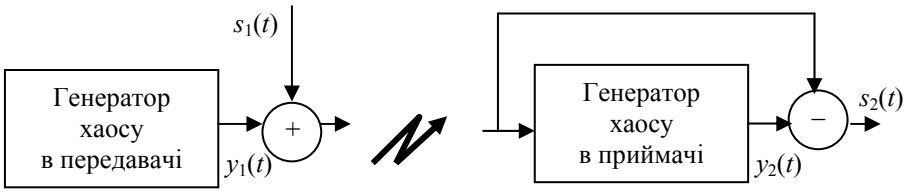

Рис. 3. Схема маскування хаотичним сигналом.

У приймачі генератор хаосу узгоджений (синхронізований) з генератором передавача. Тому сигнали хаосу $y_1(t)$ та $y_2(t)$ збігаються. Тоді вихідний сигнал приймача $s_2(t)=(s_1(t)+y_1(t))-y_2(t)=s_1(t)$ збігається з вхідним сигналом передавача. Якщо енергія інформаційного сигналу значно менша від енергії сигналу генератора хаосу, то на фоні псевдовипадкового сигналу корисний сигнал непомітний. Отже, така система зв'язку приховує інформаційний сигнал, тобто є системою криптозв'язку.

Передавач і приймач криптосистеми містять схеми Чуа. Схема передавача і приймача на вхідній мові MicroCap-6 показана на рис. 4.

Вихідні сигнали схем Чуа – це напруги на діодах Чуа NF(G1) та NF(G2). У передавачі напруга $V2$ підсумовується з напругою $V1$ синусоїдного джерела частотою 5 кГц, яка імітує інформаційне повідомлення.

Номінали елементів схем Чуа в приймачі та передавачі збігаються. Але навіть за цієї умови вихідні сигнали двох схем з часом помітно відрізняються внаслідок накопичення похибок числового інтегрування. Це є проявом особливості дивного атрактора. Тому для правильного відтворення інформаційного сигналу в приймачі необхідно час від часу вирівнювати значення змінних стану, тобто значення напруг на конденсаторах і струмів у індуктивностях [5].

Схема Чуа в приймачі відрізняється від схеми у передавачі елементами синхронізації NF(G3), NF(E2), NF(E3), NF(E4), NF(E5), $R6$, $R7$, $R8$. Синхронізація генераторів хаосу забезпечена періодичним передаванням вектора стану схеми Чуа від передавача до приймача.

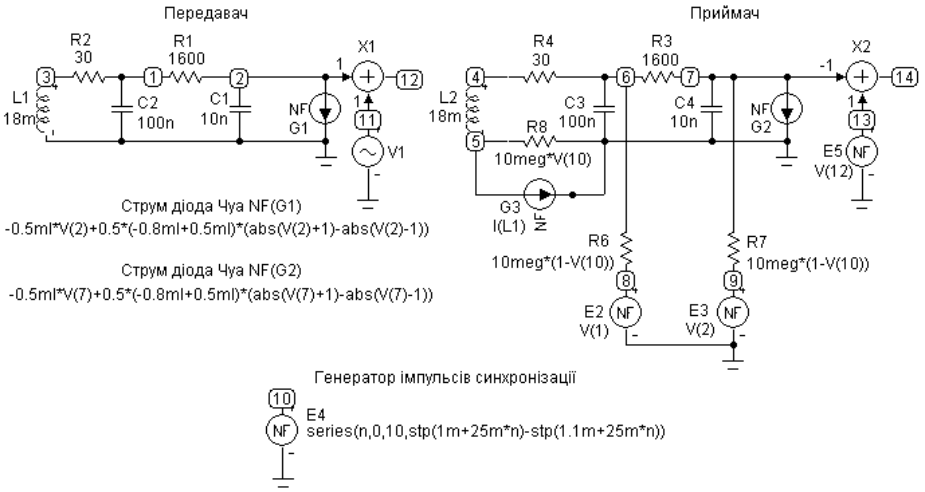

Рис. 4. Схема криптосистеми з генераторами хаосу на схемах Чуа.

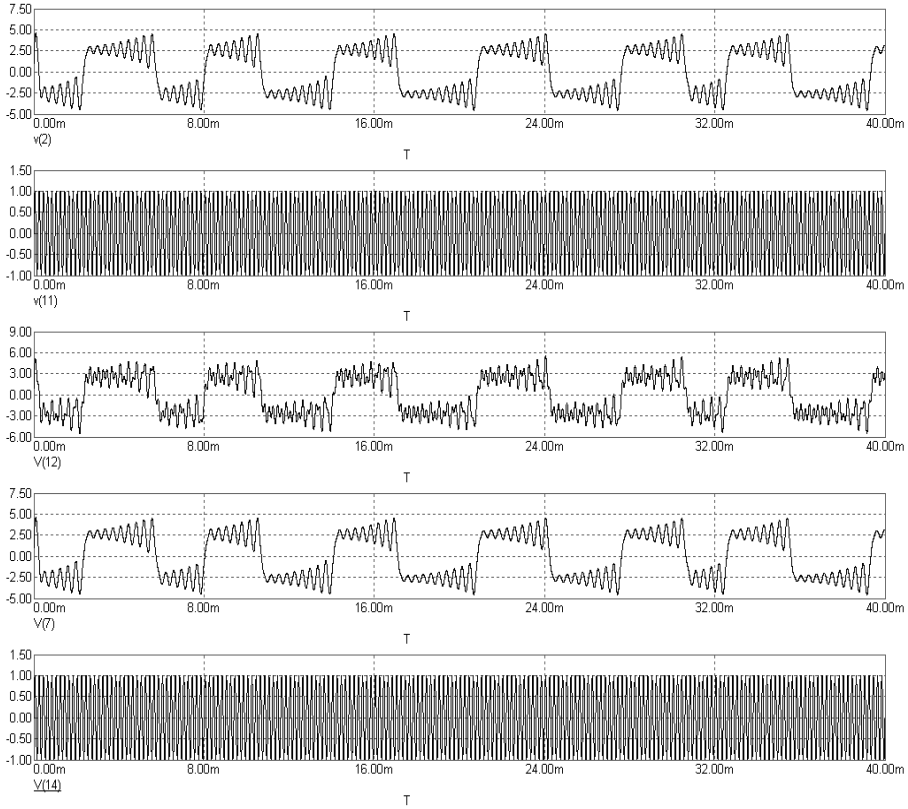

Рис. 5. Часові діаграми сигналів криптосистеми.

Джерело імпульсів синхронізації NF(E4) задає інтервали синхронізації. Майже постійно $V(10)=0$, лише впродовж 0,1 мс на початку кожних 25 мс $V(10)=1$.

Керовані джерела NF(G3), NF(E2) та NF(E3) повторюють змінні стану схеми передавача. Опори $R6$, $R7$ та $R8$ змінюють значення від 10 Мом до нуля залежно від значення напруги $V(10)$. Завдяки цьому впродовж 0,1 мс кожні 25 мс у схемі приймача примусово задаються струм індуктивності та напруги ємностей, які збігаються з відповідними у схемі передавача.

На суматорі $X2$ віднімається сигнал $V(7)$ від сигналу $V(13)=V(12)$.

Часові діаграми сигналів криптосистеми, розраховані MicroCap-6, зображені на рис. 5: вихід схеми Чуа передавача $V(2)$; інформаційний сигнал $V(11)$; вихідний сигнал передавача $V(12)$; вихід схеми Чуа приймача $V(7)$; інформаційний сигнал відтворений у приймачі $V(14)$.

Як бачимо, на виході приймача повністю відтворений інформаційний сигнал.

Отже, описаний зразок системи зв'язку з маскуванням інформаційного сигналу псевдовипадковим сигналом схеми Чуа є лише ілюстрацією принципової можливості такої системи з перевіркою схеми сихронізації. У реальних системах вектор стану повинен передаватись каналом зв'язку після відповідного імпульсу синхронізації.

---

1. *Губанов Д., Дмитриев А., Панас А., Старков С., Стешенко В.* Генераторы хаоса в интегральном исполнении / www.chipinfo.ru.
2. *Матвійчук Я. М.* Математичне моделювання хаотичних рухів у детермінованих системах // Вісн. Львів. ун-ту. Сер. фіз. 1993. Вип. 26. С. 61–66.
3. *Матвійчук Я. М., Хараба М. В*. Електрична та математичні реалізації схеми Чуа // Теор. електротехніка. 1994. Вип. 52. С. 169–179.
4. *Мун Ф*. Хаотические колебания / Пер. с англ. М., 1990.
5. *Чуа Л. О., Пен-Мин Ли* Машинный анализ электронных схем / Пер. с англ. М., 1980.

CRYPTOSYSTEM OF CONNECTION ON THE SCHEME CHUA.

I. Buliuk, Y. Matvijchuk

Lviv Polytechnic National University
Bandera Str., 12, Lviv 79013, Ukraine
matv@ua.fm

The sample of a communications system with disguise of an information signal by a pseudo-random signal of the scheme Chua is circumscribed. It is offered synchronization of the schemes Chua in the repeater and in the receiver.

Key words: cryptosystem of connection, scheme Chua, synchronization method.

Стаття надійшла до редколегії 20.05.2007
Прийнята до друку 01.07.2007