Схема, приведённая на рис. 2, изображает этапы модифицированного квантового вычисления (слева направо):

1) инициализация, вычисление, измерение с сохранением результата – то же, что и в обычном варианте квантовых вычислений;

2) обработка и анализ сохранённого результата, ветвление по некоторым условиям;

3) повторение действий, аналогичных этапу 1;

4) завершение вычисления измерением результирующего состояния системы.

Следует отметить, что методика, приведённая на схеме, не может быть использована в случае организации непрерывного квантового вычисления. Причина именно в том, что измерение состояний квантовых систем приводит к проецированию смешанных состояний на оси сферы Блоха. В результате будут потеряны все преимущества, связанные с запутанностью и квантовым параллелизмом вычислений.

Реализовать предложенную методику модификации квантовых вычислений можно посредством дополнения программы управляющего компьютера возможностями анализа и изменения сохраняемых значений квантового регистра и перехода на заданные участки управляющей программы вычислений в зависимости от анализируемых значений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления. – Москва: МЦНМО, ЧеРо 1999. – 192с.
2. *Кокин А. А.* Твердотельные ядерные магнитно-резонансные (ЯМР) ансамблевые квантовые компьютеры (Исследование физических основ и проблем реализации). – Москва: Физико-технологический институт Российской Академии Наук, 2003. – 187с.
3. *Кокин А.А.* Физические реализации квантового компьютера. – Москва: ФТИАН / http://elanina.narod.ru/lanina/index.files/student/tehnology /text/ kvant .htm#J18.

УДК 681.51

А.О. Кожанов

МЕТОД СКРЫТИЯ ПЕРЕДАЧИ ИНФОРМАЦИИ ПРИ ПОМОЩИ СТРАННОГО АТТРАКТОРА АНИЩЕНКО–АСТАХОВА

В последние годы был предложен ряд способов скрытой передачи информации, базировавшихся на применении в качестве несущего сигнала широкополосных колебаний генератора хаоса. Авторы работ по данной тематике с целью выделения информационного сигнала из хаотического обычно использовали явление хаотической синхронизации. Методы, основанные на явлении синхронизации, имеют ряд недостатков, наиболее существенным из которых является требование идентичности генераторов хаотических колебаний в приемнике и передатчике [1].

В статье представлен метод обработки и защиты информации, основанный на теории глобальной реконструкции динамической хаотической системы Анищенко–Астахова с использованием синергетического наблюдателя.

Моделирование системы

Для построения модели использовался подход параметрически модулированных хаотических генераторов. Исходная динамическая система Анищенко–Астахова описывается нелинейными дифференциальными уравнениями:

$$\frac{dx}{dt} = m_0 x + y - xz\,,\ \frac{dy}{dt} = -x\,,\ \frac{dz}{dt} = -g_0 + 0.5 g_0 (x + |x|) x\,. \qquad (1)$$

Путем замены переменных эта система была преобразована к следующему виду:

$$\frac{dY}{dt} = Z, \frac{dZ}{dt} = X, \frac{dX}{dt} = f(X,Y,Z,\mu), \mu = (m_0, g_0)\,. \qquad (2)$$

Будем модулировать параметр m_0 информационным сигналом таким образом, чтобы значения параметра оставались в пределах хаотического режима динамической системы. Обозначим его

$$r = m_0 + m(t)\,. \qquad (3)$$

Примем *m(t)* кусочно-постоянным, таким образом:

$$f(X,Y,Z,\mu) = \frac{X(X+Y)}{Z} + (rg_0 - 1)Z - g_0(X+Y) + 0.5 g_0 (|Z| - Z) Z^2\,. \quad (4)$$

Далее будем передавать в канал одномерную реализацию X(t). Для построения синергетического наблюдателя за параметром *r* на принимающей стороне необходимо заменить неизвестный параметр его динамической моделью *dw/dt* = 0, решением этого уравнения является *w(t) = const,* что и отражает скачкообразное изменение во времени *r(t)*.

$$\dot{Y}(t) = Z; \dot{Z}(t) = X; \dot{X}(t) = wg_0 Z + G_1\,, \qquad (5)$$

где $G_1 = \frac{X(X+Y)}{Z} - Z - g_0(X+Y) + 0.5 g_0 (|Z| - Z) Z$.

Пусть $\hat{w}$ – искомая оценка параметра, введем макропеременную

$$\psi = w - \hat{w}\,, \qquad (6)$$

и запишем уравнение редукции

$$\hat{w} = Q(X,Y,Z) + v_1\,, \qquad (7)$$

где *Q(X,Y,Z)* – неизвестная функция от наблюдаемых переменных состояния системы (5), v_1 – переменная состояния динамического наблюдателя. Макропеременная (6) должна удовлетворять функциональному уравнению

$$\dot{\psi}(t) + L(X,Y,Z)\psi = 0\,, \qquad (8)$$

где *L(X,Y,Z)* – неизвестная функция, обеспечивающая устойчивость уравнения (8). Выразив производную макропеременной из уравнения (6) и производную $\hat{w}$ из уравнения (7) , подставим в уравнение (8):

$$-\frac{\partial Q}{\partial X}(wg_0 Z + G_1) - \frac{\partial Q}{\partial Y} Z - \frac{\partial Q}{\partial Z} X - \frac{dv}{dt} + L(X,Y,Z)(w - \hat{w}) = 0\,. \qquad (9)$$

Разделим уравнение на 2 части, первая из которых содержит ненаблюдаемую переменную *w*:

$$w\left(-\frac{\partial Q}{\partial X} g_0 Z + L(X,Y,Z)\right) = 0\,. \qquad (10)$$

Положим, что L не зависит от X и проинтегрируем выражение в скобках

$$Q(X,Y,Z) = \frac{L(X,Y,Z)X}{g_0 Z}\,. \qquad (11)$$

С учетом полученного примем

$$L(X,Y,Z) = \alpha Z^2\,. \qquad (12)$$

Подставив L и Q во вторую часть уравнения (9), получим

$$\frac{d\nu}{dt} = -(\frac{\alpha}{g_0}Z)G_1 - (\frac{\alpha}{g_0}X)X - \alpha Z^2(\frac{\alpha}{g_0}ZX + \nu)\,. \tag{13}$$

Кроме того, подставив Q в уравнение (7) имеем

$$\hat{w} = \frac{\alpha}{g_0}ZX + \nu\,. \tag{14}$$

Таким образом, был синтезирован наблюдатель за модулируемым параметром хаотического генератора Анищенко–Астахова. Параметр α определяет скорость оценивания параметра. Для моделирования системы мы выбрали его значение $\alpha = 0{,}0025$. Результаты численного моделирования приведены на рис. 1 и 2. Мы продемонстрировали метод построения самоорганизующейся системы скрытой передачи информации

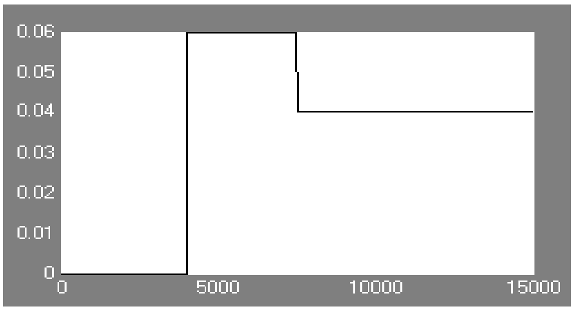

Рис.1. Информационный сигнал на передатчике

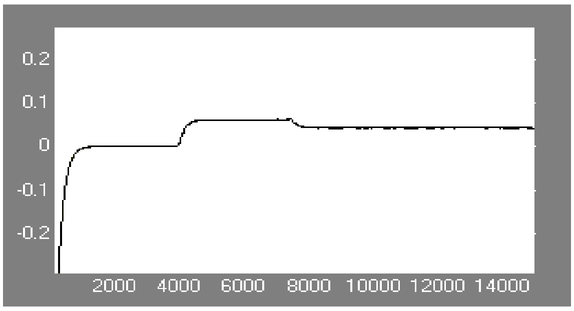

Рис.2. Восстановленный информационный сигнал на приемнике

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Анищенко В.С., Астахов В.В., Вадивасова Т.Е., Нейман А.Б.* Нелинейные эффекты в хаотических и стохастических системах. – Москва-Ижевск: Институт компьютерных исследований, 2003.
2. *Анищенко В.С., Вадивасова Т.Е., Астахов В.В.* Нелинейная динамика хаотических и стахостических систем . – Саратов: Изд-во Саратовского университета, 1999.
3. *Колесников А.А. и др.* Современная прикладная теория управления. Ч. II: Синергетический подход в теории управления. – Москва-Таганрог: Изд-во ТРТУ, 2000.