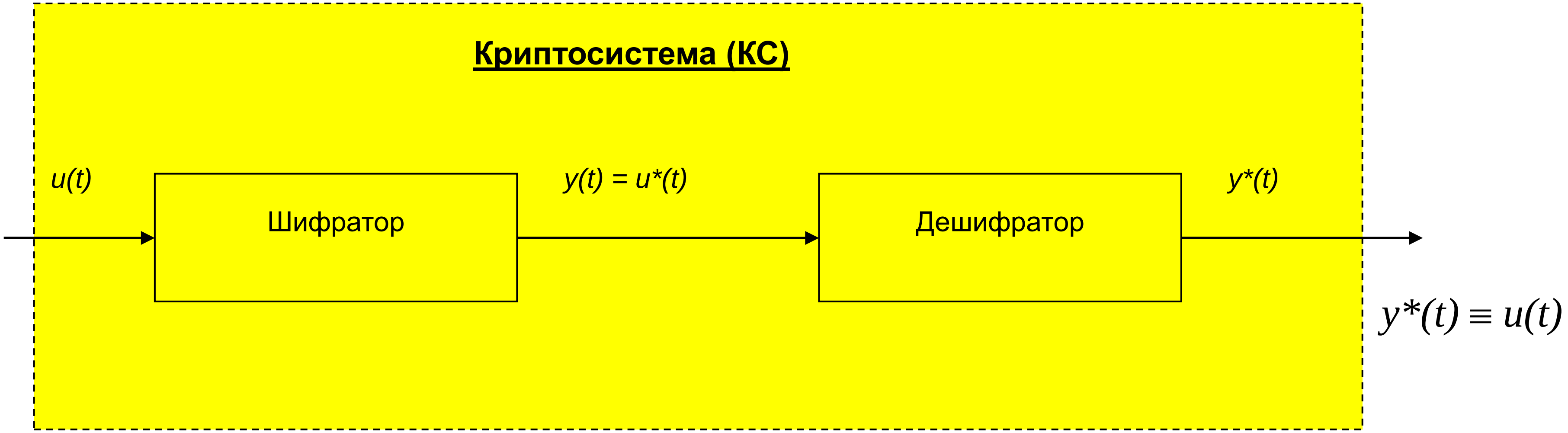
Параметрическая идентификация для линейных математических моделей криптосистем

Общая схема криптосистемы (КС)



Математическая Модель (ММ) типа «черный Ящик» Источника данных в форме синхронного автомата Хаффмана – Глушкова

$$\begin{cases} \boldsymbol{y}(t) = \lambda\left(\boldsymbol{x}(t), \boldsymbol{u}(t); \boldsymbol{p}\right) \\ \boldsymbol{x}(t+1) = \gamma\left(\boldsymbol{x}(t), \boldsymbol{u}(t); \boldsymbol{p}\right) \\ \boldsymbol{x}(0) = \boldsymbol{x}_н \end{cases}$$

Здесь

- $t \in [0,1,\ldots,M\text{-}1]$ – дискретное время
- $\boldsymbol{u}(t) \equiv \left[u(t)\right]_{k\times M} = \left[u_0\right]_{k\times 1}, \left[u_1\right]_{k\times 1}, \ldots, \left[u_{M-1}\right]_{k\times 1}$ – входной векторный *k*-мерный сигнал автомата
- $\boldsymbol{y}(t) \equiv \left[y(t)\right]_{r\times M} = \left[y_0\right]_{r\times 1}, \left[y_1\right]_{r\times 1}, \ldots, \left[y_{M-1}\right]_{r\times 1}$ – выходной векторный *r*-мерный сигнал автомата
- $\boldsymbol{x}(t) \equiv \left[x(t)\right]_{n\times M} = \left[x_0\right]_{n\times 1}, \left[x_1\right]_{n\times 1}, \ldots, \left[x_{M-1}\right]_{n\times 1}$ – внутреннее *n*-мерное состояние автомата
- $\boldsymbol{x}_н$ – начальное *n*-мерное состояние автомата
- $\boldsymbol{p}$ – вектор рабочих (свободных) параметров

Набор *базовых параметров* (БП) ММ Источника экспериментальных данных

Открытый текст КС, шифротекст и их объединенный вектор можно рассматривать как сигналы, порождаемые соответствующими гипотетическими Источниками экспериментальных данных. К набору ***базовых параметров*** (**БП**) ММ источника i-го участка стационарности длиной $m^{(i)}$ изначально квантованного по времени с интервалом $\Delta t=1$ текста относятся пары:

$$\text{БП} = \{\, q \,,\, n \,\}$$

где q – число уровней квантования, n – т.н. «сложность» упомянутых гипотетических Источников стационарных участков данных. Значения оптимальных по минимуму энтропии БП q и n гипотетических Источников текста могут определяться экспериментально по его реализации.

При определении значений базовых параметров модели по известным наборам отсчетов экспериментальных данных решается задача ***структурной идентификации*** ММ Источника экспериментальных данных.

Набор *свободных параметров* ММ Источника экспериментальных данных

К набору рабочих (свободных) параметров ***p*** относятся все остальные параметры, используемые при описании ММ Источника экспериментальных данных. Сюда могут относиться весовые коэффициенты моделей авторегрессии (АР) и скользящего среднего (СС), коэффициенты матриц, вектора начального состояния и пр.

При определении значений рабочих (свободных) параметров модели по известным наборам отсчетов экспериментальных данных решается задача ***параметрической идентификации*** ММ Источника экспериментальных данных.

Идентифицируемая линейная *ABCD*-модель

Линейным случаем модели типа «чёрный Ящик» Источника данных является система уравнений, описывающая ММ линейного цифрового автомата (ЛЦА) на языке *ABCD*-формализма:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \\ x(0) = x_0 \end{cases}$$

Описание математической модели (ММ) криптосистемы на языке *ABCD*-формализма

Шифратор

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \\ x(0) = x_0 \end{cases}, \quad y(t) = u^*(t),$$

Дешифратор

(*восстанавливающий автомат* (*))

$$\begin{cases} x^*(t+1) = A^* x^*(t) + B^* u^*(t) \\ y^*(t) = C^* x^*(t) + D^* u^*(t) \\ x^*(0) = x_0^* \end{cases}$$

где:

$\exists\ D^{-1}$,

$A^* = [A - BD^{-1}C]$, $B^* = [BD^{-1}]$,

$C^* = [-D^{-1}C]$, $D^* = [D^{-1}]$, $x_0^* = x_0$

В ряде технических приложений, иногда более удобной является схема описания ММ криптосистем, опирающаяся на *Z*-преобразование

$$Z[s(t)] \text{€} S(z) = \sum_{t=0}^{\infty} s(t)\, z^{-t} \bmod q$$

Z-преобразование для шифратора:

$$u(t) \Rightarrow U(z), \quad y(t) \Rightarrow Y(z), \quad x(t) \Rightarrow X(z),$$

$$x(t+1) \Rightarrow z \cdot (X(z) - x_0)$$

$$zX(z) - zx_0 = AX(z) + BU(z),$$

$$Y(z) = CX(z) + DU(z)$$

$$Y(z) = [C(zE - A)^{-1}B + D] \cdot U(z) +$$

$$+ [zC(zE - A)^{-1}] \cdot x_0 \equiv$$

$$\equiv K_1(z) \cdot U(z) + K_2(z) \cdot x_0$$

Z-преобразование для дешифратора:

$$u^*(t) \Rightarrow U^*(z), \quad y^*(t) \Rightarrow Y^*(z), \quad x^*(t) \Rightarrow X^*(z),$$

$$x^*(t+1) \Rightarrow z \cdot (X^*(z) - x_0^*)$$

$$zX^*(z) - zx_0^* = A^*X^*(z) + B^*U^*(z),$$

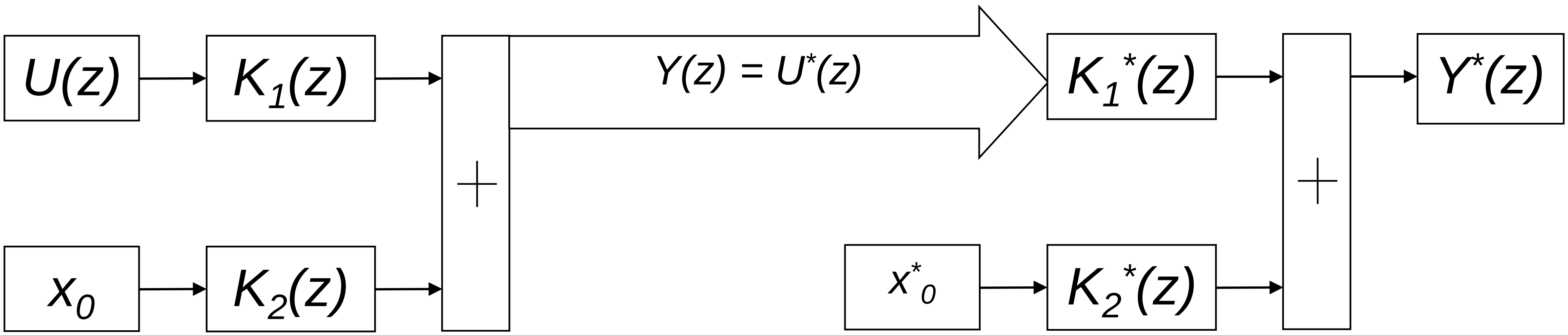
$$Y^*(z) = C^*X^*(z) + D^*U^*(z)$$

$$Y^*(z) = [C^*(zE - A^*)^{-1}B^* + D^*] \cdot U^*(z) +$$

$$+ [zC^*(zE - A^*)^{-1}] \cdot x_0^* \equiv$$

$$\equiv K_1^*(z) \cdot U^*(z) + K_2^*(z) \cdot x_0^*$$

Схема КС с коэффициентами передачи *K*(*z*)



$$K_1(z) \equiv C(zE - A)^{-1}B + D \qquad K_1^*(z) \equiv C^*(zE - A^*)^{-1}B^* + D^*$$

$$K_2(z) \equiv zC(zE - A)^{-1} \qquad K_2^*(z) \equiv zC^*(zE - A^*)^{-1}$$

Условия восстановления в «частотной» области

Учтем что:

- $Y(z) = U^*(z)$ – канал без искажений
- $U(z) = Y^*(z)$ – точное восстановление исходного сигнала

$$\Rightarrow \begin{cases} K_1^*(z) = (K_1(z))^{-1} \\ K_2^*(z) = -(K_1(z))^{-1} \cdot K_2(z) \\ x_0^* = x_0 \end{cases}$$

или:

$$\begin{cases} C^* \cdot (zE - A^*) \cdot B^* + D^* = (C \cdot (zE - A)^{-1} \cdot B + D)^{-1} \\ zC^* \cdot (zE - A^*)^{-1} = -(C \cdot (zE - A)^{-1} \cdot B + D)^{-1} \cdot zC \cdot (zE - A)^{-1} \end{cases}$$

Идентифицируемая линейная АРСС-модель

В линейном случае прогнозирующего оператора приходим к соответствующей линейной АРСС-модели дискретной динамической системы (ДДС):

$$y(t) = \alpha_1 y(t-1) + \alpha_2 y(t-2) + \ldots + \alpha_n y(t-n) +$$
$$+ \beta_0 u(t) + \beta_1 u(t-1) + \beta_2 u(t-2) + \ldots + \beta_n u(t-n)$$

Описание математической модели (ММ) криптосистемы на языке АРСС-формализма

Шифратор

$$y(t) = \alpha_1 y(t-1) + \alpha_2 y(t-2) + \ldots + \alpha_n y(t-n) + \beta_0 u(t) + \beta_1 u(t-1) + \beta_2 u(t-2) + \ldots + \beta_n u(t-n) \quad , \quad y(t) = u^*(t),$$

Дешифратор

(*восстанавливающий автомат* (*))

$$y*(t) = \alpha_1 * y*(t-1) + \alpha_2 * y*(t-2) + \ldots + \alpha_n * y*(t-n) + \beta_0 * u*(t) + \beta_1 * u*(t-1) + \beta_2 * u*(t-2) + \ldots + \beta_n * u*(t-n)$$

где:

$$\exists \beta_0^{-1} : \quad \alpha_1 * = -\beta_0^{-1}\beta_1 \quad , \quad \alpha_2 * = -\beta_0^{-1}\beta_2 \quad , \quad \ldots \quad , \quad \alpha_n * = -\beta_0^{-1}\beta_n \quad ,$$

$$\beta_0 * = \beta_0^{-1} \quad , \quad \beta_1 * = -\beta_0^{-1}\alpha_1 \quad , \quad \beta_2 * = -\beta_0^{-1}\alpha_2 \quad , \quad \ldots \quad , \quad \beta_n * = -\beta_0^{-1}\alpha_n$$

Идентификация линейной АРСС-модели

Идентификацию АРСС-модели

$$y(t) = \alpha_1 y(t-1) + \alpha_2 y(t-2) + \ldots + \alpha_n y(t-n) +$$
$$+ \beta_0 u(t) + \beta_1 u(t-1) + \beta_2 u(t-2) + \ldots + \beta_n u(t-n)$$

можно провести при помощи системы $2n+1$ линейных уравнений, для составления которых потребуется измерить как минимум $3n+1$ первых входных и выходных отсчетов ЛЦА

$$\begin{cases} y(n) = \alpha_1 y(n-1) + \alpha_2 y(n-2) + \ldots + \alpha_n y(0) + \beta_0 u(n) + \beta_1 u(n-1) + \beta_2 u(n-2) + \ldots + \beta_n u(0) \\ y(n+1) = \alpha_1 y(n) + \alpha_2 y(n-1) + \ldots + \alpha_n y(1) + \beta_0 u(n+1) + \beta_1 u(n) + \beta_2 u(n-1) + \ldots + \beta_n u(1) \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ y(3n) = \alpha_1 y(3n-1) + \alpha_2 y(3n-2) + \ldots + \alpha_n y(2n) + \beta_0 u(3n) + \beta_1 u(3n-1) + \beta_2 u(3n-2) + \ldots + \beta_n u(2n) \end{cases}$$

Идентификация линейной *ABCD*-модели

После идентификации АРСС-модели можно сразу же определить матрицы A и D :

$$a_1 := \alpha_1\ ;\ a_2 := \alpha_2\ ;\ \ldots\ ;\ a_n := \alpha_n\ ;$$

$$D = \beta_0$$

$$A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Тогда, задав произвольно коэффициенты одной из матриц – B или C , для другой можно решать систему уравнений

$$\beta_1 := CB - a_1 \cdot D$$

$$\beta_2 := CAB - a_1 \cdot CB - a_2 \cdot D$$

$$\beta_3 := CA^2B - a_1 \cdot CAB - a_2 \cdot CB - a_3 \cdot D$$

$$\ldots$$

$$\beta_{n-2} := CA^{n-3}B - a_1 \cdot CA^{n-4}B - a_2 \cdot CA^{n-5}B - \ \ldots\ - a_{n-4} \cdot CAB - a_{n-3} \cdot CB - a_{n-2} \cdot D$$

$$\beta_{n-1} := CA^{n-2}B - a_1 \cdot CA^{n-3}B - a_2 \cdot CA^{n-4}B - \ \ldots\ - a_{n-3} \cdot CAB - a_{n-2} \cdot CB - a_{n-1} \cdot D$$

$$\beta_n := CA^{n-1}B - a_1 \cdot CA^{n-2}B - a_2 \cdot CA^{n-3}B - \ \ldots\ - a_{n-2} \cdot CAB - a_{n-1} \cdot CB - a_n \cdot D$$

Найти вектор начального состояния x_0 можно, например, исходя из формулы полной реакции ЛЦА, когда уже известны все матрицы – A, B, C, D .

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике. Пер. с англ. под ред. Р.Л. Добрушина и О.Б. Лупанова. М.: ИЛ, 1963. С. 333-402.
2. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002.
3. Гилл А. Линейные последовательностные машины: Перев. с англ. М.: Наука, Гл. редакция физ.-мат. литературы, 1974.
4. Кирьянов К.Г. Выбор оптимальных базовых параметров источников экспериментальных данных при их идентификации // Труды III Международной конференции «Идентификация систем и задачи управления» SICPRO’04. Москва, 28-30 января 2004 г. Институт проблем управления им. В.А.Трапезникова РАН. М.: Институт проблем управления им. В.А.Трапезникова РАН, 2004. С.187-208.
5. Кирьянов К.Г. Соотношение неопределенности для базовых параметров генетических карт и применение его для идентификации нестационарных источников экспериментальных данных // Труды V Международной конференции «Идентификация систем и задачи управления» SICPRO’06. Москва, 26-28 января 2006 г. Институт проблем управления им. В.А.Трапезникова РАН. М.: Институт проблем управления им. В.А.Трапезникова РАН, 2006. С.155-182.
6. Горбунов А.А., Кирьянов К.Г. Динамические модели криптосистем с закрытым ключом. Синтез дешифраторов // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Радиофизика. Выпуск 1 (2). Н. Новгород: ННГУ, 2004. С. 24–36.