СПИСОК ЛИТЕРАТУРЫ

1. Дистанционно управляемые роботы и манипуляторы / Под ред. В.С. Кулешова и Н.А. Лакоты. М.: Машиностроение, 1986.

2. **Зенкевич С.Л., Ющенко А.С.** Управление роботами. Основы управления манипуляционными роботами: Учеб. для вузов. М.: Изд-во МГТУ, 2000.

3. **Игнатова Е.И., Кочкарев Д.А.** Особенности математического моделирования робототехнических систем// Экстремальная робототехника, нано-, микро- и макророботы. Матер. XX Междунар. науч.-техн. конф. Дивноморское, Россия, 2009.

4. **Игнатова Е.И., Ростов Н.В.** Методика компьютерного исследования динамики существенно гибких многомерных электромеханических систем // Робототехника для экстремальных условий. Матер. VI науч.-техн. конф. СПб.: СПбГТУ, 1996.

5. **Игнатова Е.И., Ростов Н.В.** Компьютерное моделирование исполнительных систем роботов: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2009.

6. **Игнатова Е.И., Ростов Н.В.** Компьютерное моделирование систем управления роботами: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2009.

7. **Кондратьев А.С., Лопота В.А., Юревич Е.И.** Робототехника и техническая кибернетика. Тенденции и перспективы развития // Научно-технические ведомости СПбГПУ. 2003. № 2.

8. **Лесков А.Г., Ющенко А.С.** Моделирование и анализ робототехнических систем. М.: Машиностроение, 1992.

9. **Лопота В.А., Юревич Е.И.** Экстремальная робототехника и проблемы безопасности, актуальные проблемы защиты и безопасности. // Экстремальная робототехника. Матер. VII Всерос. науч.-практ. конф. СПб.: Изд-во НПО спецматериалов, 2004.

10. Моделирование робототехнических систем и гибких автоматизированных производств / Под ред. И.М. Макарова // Робототехника и гибкие автоматизированные производства. Кн. 5. М.: Высш. шк., 1986.

11. **Морозов Б.И., Семенов И.М., Юревич Е.И.** Электромеханические исполнительные системы робототехники: Учеб. пособие / Под ред. Е.И. Юревича. СПб: СПбГТУ, 1994.

12. **Морозов Б.И., Станкевич Л.А., Юревич Е.И.** Системы управления роботами: Учеб. пособие. Л.: ЛПИ, 1987.

13. **Советов Б.Я., Яковлев С.А.** Моделирование систем: Учеб. пособие. М.: Высш. шк., 2001.

14. **Фу К., Гонсалес Р., Ли К.** Робототехника: Пер. с англ. / Под ред. В.Г. Градецкого. М.: Мир, 1989.

15. **Шахинпур М.** Курс робототехники: Пер. с англ. / Под ред. С.Л. Зенкевича. М.: Мир, 1990.

16. **Юревич Е.И.** Основы робототехники: Учеб. для вузов. СПб.: БХВ-Петербург, 2005.

УДК 681.3 (075.8)

Е.И. Игнатова, Н.В. Ростов

КИНЕМАТИЧЕСКИЕ ЗАДАЧИ В МАТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ РОБОТОВ

В робототехнике для анализа кинематики исполнительных механизмов (ИМ) широкое применение находят алгебраические векторно-матричные модели в представлении Денавита–Хартенберга, использующие однородные координаты. Методы аналитического решения прямых и обратных задач кинематики (ПЗК и ОЗК) с использованием таких моделей описаны в [2, 5–7]. Однако при компьютерном моделировании манипуляционных роботов более эффективными часто оказываются решения, получаемые итерационными методами.

Обсудим вначале общие формулировки прямых и обратных задач кинематики (ПЗК и ОЗК).

Прямые задачи кинематики

ПЗК о положении и ориентации схвата. По заданному $N\times1$ вектору обобщенных координат звеньев:

$$q = (q_1, q_2,..., q_N)^{\mathrm{T}}$$

и известной 6×1 вектор-функции $\Phi(\cdot)$, соответствующей кинематической схеме ИМ робота, определяется 6×1 вектор состояния схвата:

$$S_C = \Phi(q), \qquad (1)$$

где $S_C = (x_C, y_C, z_C, \varphi_C, \theta_C, \psi_C)^{\mathrm{T}}$ – вектор линейных координат положения и угловых координат ориентации схвата.

ПЗК о скоростях схвата. По заданному вектору обобщенных скоростей $\dot{q} = (\dot{q}_1, \dot{q}_2, ..., \dot{q}_N)^T$ определяется вектор проекций линейной и угловой скорости схвата:

$$\begin{pmatrix} V_C \\ \Omega_C \end{pmatrix} = J(q) \cdot \dot{q}, \qquad (2)$$

где $V_C = (v_x, v_y, v_z)^T$; $\Omega_C = (\omega_\varphi, \omega_\theta, \omega_\psi)^T$.В зависимости от числа звеньев N робота матрица Якоби в (2) может быть квадратной или иметь прямоугольный вид.

ПЗК о силе и моменте в схвате. По заданному $N\times1$ вектору обобщенных сил в шарнирах звеньев $Q = (Q_1, Q_1, ..., Q_N)^T$ определяются составляющие силы и момента в схвате:

$$\begin{pmatrix} F_C \\ M_C \end{pmatrix} = (J^T(q))^{-1} \cdot Q, \qquad (3)$$

где $F_C = (F_x, F_y, F_z)^T$; $M_C = (M_\varphi, M_\theta, M_\psi)^T$.

Однако выражение (3) справедливо только для случая идеального ИМ, не имеющего потерь энергии в шарнирах звеньев.

Обратные задачи кинематики

ОЗК о положениях звеньев. По 6×1 вектору состояния схвата S_C вычисляется $N\times1$ вектор значений обобщенных координат звеньев:

$$q = \Phi^{-1}(S_C), \qquad (4)$$

где $\Phi^{-1}(\cdot)$ – $N\times1$ вектор-функция, обратная $\Phi(\cdot)$.

ОЗК о скоростях звеньев. По вектору линейных и угловых скоростей схвата вычисляется вектор обобщенных скоростей звеньев:

$$\dot{q} = J^{-1}(q) \cdot \begin{pmatrix} V_C \\ \Omega_C \end{pmatrix}, \qquad (5)$$

где $J^{-1}(\cdot)$ – матрица, обратная матрице Якоби.

ОЗК о силах и моментах в шарнирах звеньев. По вектору проекций силы и момента в схвате определяется вектор обобщенных сил в шарнирах:

$$Q = J^T(q) \cdot \begin{pmatrix} F_C \\ M_C \end{pmatrix}. \qquad (6)$$

Выражение (6) предполагает отсутствие потери энергии в шарнирах звеньев.

Итерационные методы решения ОЗК

Задача (6) требует вычисления и транспонирования матрицы Якоби, а выражение (5) представляет собой решение системы линейных алгебраических уравнений вида:

$$J(q) \cdot \dot{q} = \begin{pmatrix} V_C \\ \Omega_C \end{pmatrix}.$$

Если число звеньев робота $N \neq 6$, то матрица Якоби такой системы:

$$J(q) = \frac{\partial F(q)}{\partial q} = \left\{ \frac{\partial F_i(q)}{\partial q_j},\ i = \overline{1,6},\ j = \overline{1,N} \right\}$$

имеет прямоугольный вид.

Наиболее сложной с вычислительной точки зрения является задача (4), представляющая собой задачу решения системы нелинейных алгебраических уравнений вида:

$$\Phi(q) - S_C = F(q) = 0 \qquad (7)$$

где 0 – нулевой 6×1 вектор. В случае, когда $N = 6$, для решения (7) можно воспользоваться итерационным методом Ньютона со следующим алгоритмом [1]:

$$q^{k+1} = q^k - h_k \cdot J^{-1}(q^k) \cdot F(q^k), \qquad (8)$$

где $J^{-1}(\cdot)$ – 6×6 матрица, обратная матрице Якоби; h_k – величина шага (скаляр). В классическом методе Ньютона $h_k = 1$, а при регулировке шага $h_k = \text{var}$, $h_k < 1$. Но при плохой обусловленности матрицы Якоби или её вырождаемости в особых конфигурациях ИМ (при некоторых положениях звеньев) итерационное решение ОЗК затрудняется.

При избыточном числе звеньев, когда $N > 6$, в алгоритме (8) вместо обратной матрицы следует использовать квадратную 6×6 псевдообратную матрицу:

$$J^{-1} = (J^T J)^{-1} J^T,$$

то есть:

$$q^{k+1} = q^k - h_k \cdot J^{+1}(q^k) \cdot F(q^k). \qquad (9)$$

Если значения вектора ограничены допустимой областью D^N, то точные решения системы (7) в принципе могут отсутствовать. В таком случае ОЗК формулируется как задача минимизации квадрата нормы вектора невязки:

$$\left\| F(q) \right\|^2 \to \min_{q \in D^N}, \qquad (10)$$

и решается итерационными численными методами условной минимизации в ограниченном пространстве значений вектора q.

Решение ПЗК о положении схвата

Положение центра и ориентацию осей N-й системы координат схвата в базовой СК робота определяет матрица:

$$T_N(q) = A_1(q_1)A_2(q_2)\cdots A_N(q_N) = \\ = \begin{pmatrix} n_{N,0} & o_{N,0} & a_{N,0} & p_{N,0} \\ 0 & 0 & 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} n_{x,0} & o_{x,0} & a_{x,0} & x_{N,0} \\ n_{y,0} & o_{y,0} & a_{y,0} & y_{N,0} \\ n_{z,0} & o_{z,0} & a_{z,0} & z_{N,0} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (11)$$

где $p_{N,0} = (x_{N,0}, y_{N,0}, z_{N,0})^{\mathrm{T}}$ – вектор положения центра; $a_{N,0}$, $o_{N,0}$, $n_{N,0}$ – векторы подхода, ориентации и нормали, характеризующие пространственное положение осей.

По заданному в СК схвата положению точки С:

$$r_{C,N} = (x_{C,N}, y_{C,N}, z_{C,N}, 1)^{\mathrm{T}},$$

можно определить её положение в базовой СК следующим образом:

$$r_{C,0}, = T_N(q) r_{C,N} = (x_C, y_C, z_C, 1)^{\mathrm{T}}. \quad (12)$$

Если же точка С является центром системы координат схвата $r_{C,N} = (0, 0, 0, 1)^{\mathrm{T}}$, то её координатами в базовой СК являются элементы 4-го столбца матрицы (11):

$$x_C = x_{N,0} = T_N(1,4);$$
$$y_C = y_{N,0} = T_N(2,4);$$
$$x_C = z_{N,0} = T_N(3,4).$$

Из (12) следует, что по вектору положения точки С схвата $p_{C,N} = (x_{C,N}, y_{C,N}, z_{C,N}, 1)^{\mathrm{T}}$, заданному в его собственной СК, и матрице $T_N(q)$ можно определить 4×4 матрицу:

$$T_{C,0}(q) = T_N(q) \begin{pmatrix} E_{3\times3} & p_{C,N} \\ 0\ 0\ 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} n_{N,0} & o_{N,0} & a_{N,0} & p_{C,0} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (13)$$

элементами 4-го столбца которой являются координаты рассматриваемой точки в базовой СК робота:

$$x_{C,0} = T_{1,4}(q);$$
$$y_{C,0} = T_{2,4}(q); \quad (14)$$
$$x_{C,0} = T_{3,4}(q).$$

Решение ОЗК о положениях звеньев

Рассмотрим возможные постановки и решения ОЗК на основе использования выражений (13) и (14).

1. Решение ОЗК по алгоритму (9) предполагает вычисление на каждом шаге итерационного процесса матрицы Якоби и её псевдообратной матрицы. В общем случае она представляет собой 6x6 матрицу следующего вида [5]:

$$J(q) = \\ = \begin{pmatrix} n_x & n_y & n_z & (p\times n)_x & (p\times n)_y & (p\times n)_z \\ o_x & o_y & o_z & (p\times o)_x & (p\times o)_y & (p\times o)_z \\ a_x & a_y & a_z & (p\times a)_x & (p\times a)_y & (p\times a)_z \\ 0 & 0 & 0 & n_x & n_y & n_z \\ 0 & 0 & 0 & o_x & o_y & o_z \\ 0 & 0 & 0 & a_x & a_y & a_z \end{pmatrix}, \quad (15)$$

требующую вычисления векторов нормали, ориентации и подхода – столбцов матрицы поворота $R_{C,0}(q)$, и вектора положения $p_{C,0}$ схвата.

2. В общем случае N-вектор обобщенных координат q определяется по вектору положения схвата $p_{C,0} = (x_{C,0}, y_{C,0}, z_{C,0})^{\mathrm{T}}$ и проекциям векторов ориентации его осей $n_{N,0}$, $o_{N,0}$, $a_{N,0}$) , заданным в базовой системе координат матрицей:

$$T_{C,0}(q) = \begin{pmatrix} n_{x,0} & o_{x,0} & a_{x,0} & x_{C,0} \\ n_{y,0} & o_{y,0} & a_{y,0} & y_{C,0} \\ n_{z,0} & o_{z,0} & a_{z,0} & z_{C,0} \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

путём решения соответствующей нелинейной системы двенадцати алгебраических уравнений с N неизвестными:

$$\left.\begin{array}{c} T_{1,1}(q) = n_{x,0} \\ T_{2,1}(q) = n_{y,0} \\ \cdots \\ T_{2,4}(q) = y_{C,0} \\ T_{3,4}(q) = z_{C,0} \end{array}\right\}. \quad (16)$$

При числе звеньев $N < 12$ система (16) является избыточной, и для её решения достаточно использовать только N уравнений, однако их выбор неоднозначен.

3. В случае, когда ориентация осей СК схвата задаётся вектором направляющих косинусов $(c_{x,0}, c_{y,0}, c_{z,0})^{\mathrm{T}}$, ОЗК можно решать как задачу ми-

нимизации квадрата нормы 6×1 вектора невязки:

$$\left\| \begin{matrix} (T_{1,4}(q) - x_{C,0}) \\ (T_{2,4}(q) - y_{C,0}) \\ (T_{3,4}(q) - z_{C,0}) \\ (c_x(q) - c_{x,0}) \\ (c_y(q) - c_{y,0}) \\ (c_z(q) - c_{z,0}) \end{matrix} \right\|^2 \to \min_{q \in D^N}. \qquad (17)$$

Направляющие косинусы $c_x(q)$, $c_y(q)$ и $c_z(q)$ можно вычислять по следующим формулам [2]:

$$c_x = \frac{o_z - a_y}{2\sin\delta};\ c_y = \frac{a_x - n_z}{2\sin\delta};\ c_z = \frac{n_y - o_x}{2\sin\delta}, \qquad (18)$$

где угол δ определяется по следу матрицы $T_{C,0}(q)$ или матрицы поворота:

$$R_{C,0} = \begin{pmatrix} n_x & o_x & a_x \\ n_y & o_y & a_y \\ n_z & o_z & a_z \end{pmatrix} = \begin{pmatrix} T_{1,1}(q) & T_{1,2}(q) & T_{1,3}(q) \\ T_{2,1}(q) & T_{2,2}(q) & T_{2,3}(q) \\ T_{3,1}(q) & T_{3,2}(q) & T_{3,3}(q) \end{pmatrix};$$

$$\delta = \arccos\left(\frac{1}{2}(trT_{C,0} - 2)\right) = \arccos\left(\frac{1}{2}(trR_{C,0} - 1)\right) = \arccos\left(\frac{1}{2}(n_x + o_y + a_z - 1)\right).$$

Направляющие косинусы $(c_{x,0}, c_{y,0}, c_{z,0})$ являются проекциями единичных векторов-ортов СК схвата в неподвижной системе координат, задаваемых в соответствии с используемыми углами Эйлера.

4. В частном случае трёхзвенного робота вектор q вычисляется только по вектору положения схвата $p_{C,0} = (x_{C,0}, y_{C,0}, z_{C,0})^{\mathrm{T}}$, а ориентация осей СК схвата не задаётся. При этом ОЗК может решаться методом Гаусса–Ньютона как задача минимизации квадрата нормы 3×1 вектора невязки:

$$\left\| \begin{matrix} (T_{1,4}(q) - x_{C,0}) \\ (T_{2,4}(q) - y_{C,0}) \\ (T_{3,4}(q) - z_{C,0}) \end{matrix} \right\|^2 \to \min_{q \in D^N} \qquad (19)$$

в неограниченном или ограниченном пространстве значений вектора q.

При плохой обусловленности матрицы Якоби или её вырождаемости в особых конфигурациях ИМ решение ОЗК в любых их постановках затрудняется. Кроме того, результаты, получаемые итерационными методами, могут быть неоднозначными и зависеть от начальных значений вектора q. Поскольку в реальных роботах значения координат звеньев всегда ограничены допустимой областью D^N, то точные решения ОКЗ на некоторых участках задаваемой траектории схвата могут в принципе отсутствовать.

Пример решения ОЗК

Рассмотрим шестизвенный робот, три первых вращательных звена которого работают в вертикально-ангулярной системе координат, а звенья 4, 5 и 6 (также вращательного типа) обеспечивают ориентацию схвата.

На рис. 1 точками изображена заданная программная траектория схвата, а его ориентация на траектории задана постоянным вектором направляющих косинусов:

$$(c_{x,0}, c_{y,0}, c_{z,0})^{\mathrm{T}} = (\cos(\pi/4), (\cos(\pi/4), 0)^{\mathrm{T}}.$$

На рис. 2 представлены траектории звеньев, вычисленные путём итерационного решения ОЗК методом Гаусса–Ньютона, а на рис. 3 – соответствующие им направляющие косинусы, практически равные заданным.

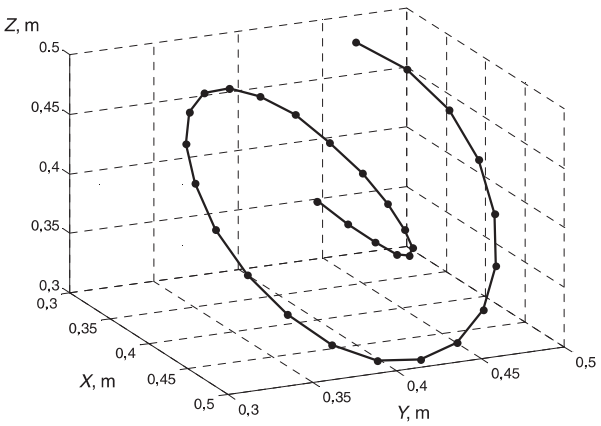


Рис. 1. Траектория схвата робота
(•) S_g; (———) S_c

Однако в других случаях (при задании иных начальных значений координат звеньев и ориентации схвата) итерационное решение ОЗК для данного робота оказывается неоднозначным или несходящимся.

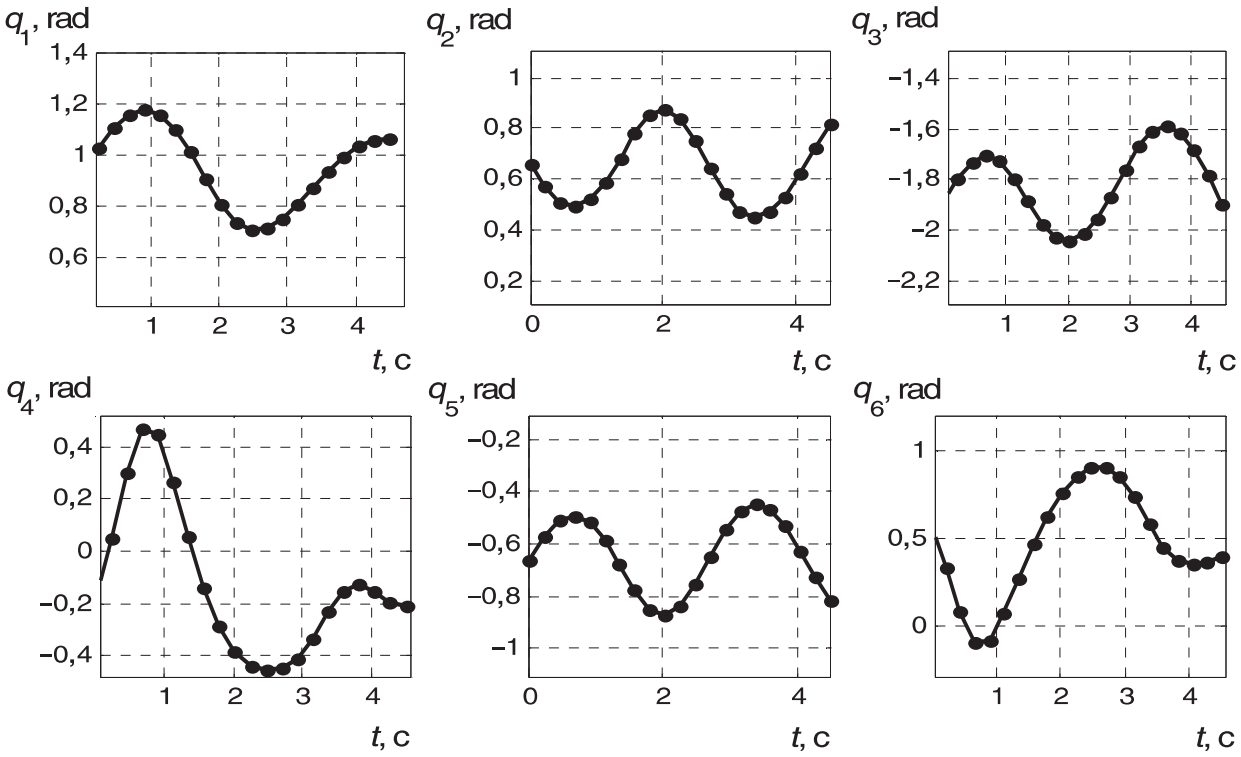


Рис. 2. Траектории звеньев

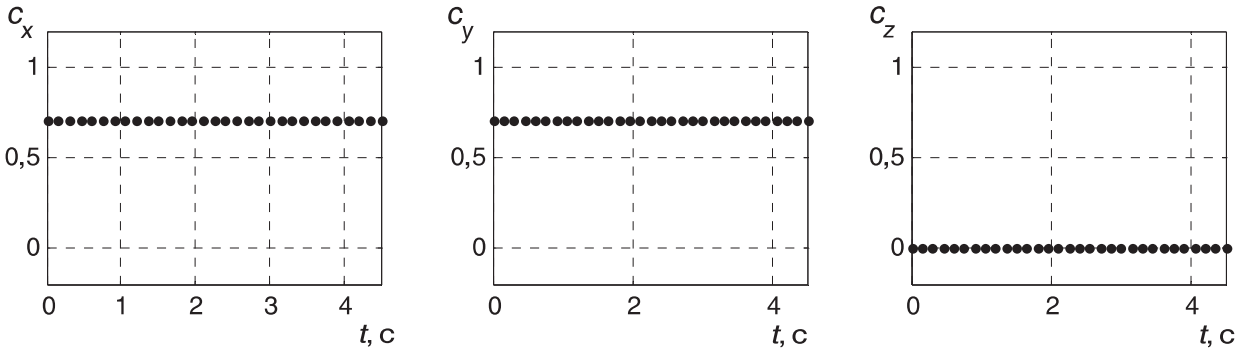


Рис. 3. Направляющие косинусы ориентации схвата

Для роботов со сложной кинематикой целесообразно применять итерационные методы решения ОЗК.

Использование моделей в однородных координатах позволяет получать наиболее точное решение ОЗК с вычислением элементов матрицы Якоби без численного дифференцирования.

Методики решения задач кинематики средствами пакета MATLAB для роботов конкретных типов при моделировании их исполнительных систем и СУ изложены в [3, 4].

СПИСОК ЛИТЕРАТУРЫ

1. **Деннис Д., Шнабель Р.** Численные методы безусловной оптимизации и решения нелинейных уравнений. М.: Мир, 1988.

2. **Зенкевич С.Л., Ющенко А.С.** Управление роботами. Основы управления манипуляционными роботами: Учеб. для вузов. М.: Изд-во МГТУ, 2000.

3. **Игнатова Е.И., Ростов Н.В.** Компьютерное моделирование исполнительных систем роботов: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2009.

4. **Игнатова Е.И., Ростов Н.В.** Компьютерное моделирование систем управления роботами: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2009.

5. **Шахинпур М.** Курс робототехники: Пер. с англ. / Под ред. С.Л. Зенкевича. М.: Мир, 1990.

6. **Фу К., Гонсалес Р., Ли К.** Робототехника: Пер. с англ. / Под ред. В.Г. Градецкого. М.: Мир, 1989.

7. **Юревич Е.И.** Основы робототехники: Учеб. для вузов. СПб.: БХВ-Петербург, 2005.

УДК 681.3.055

Н.И. Червяков, М.Г. Бабенко

ЛИНЕЙНЫЕ РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Псевдослучайные последовательности используются для генерации секретных ключей шифрования, для вычисления цифровой подписи и для работы многих алгоритмов аутентификации. Для построения псевдослучайных последовательностей используются линейные рекуррентные последовательности на эллиптической кривой.

Поставим задачу проанализировать существующие генераторы на эллиптической кривой и построить генератор на эллиптической кривой, в котором арифметические операции будут выполняться в системе остаточных классов. Генератор псевдослучайных последовательностей должен удовлетворять следующим двум требованиям, предложенным в работе [9]:

1. Статистической безопасности: последовательность, созданная генератором псевдослучайных чисел, должна статистически ничем не отличаться от абсолютно случайной последовательности.

2. Криптографической безопасности: возможность, зная k-битов последовательности, предсказать следующий или $k + 1$ бит.

Эллиптическая кривая широко используется для построения криптосистем [4]. Одним из инструментов построения генераторов псевдослучайных последовательностей является эллиптическая кривая над конечным полем.

Эллиптическая кривая E над простым полем F_q, где $q > 3$, задаётся уравнением в форме Вейерштрасса $E(F_q): y^2 = x^3 + Ax + B$, где $4A^3 + 27B^2 \neq 0$.

Халлгрен в 1994 г. в работе [2] рассмотрел датчик псевдослучайной последовательности, который называется арифметической прогрессией на E с начальным членом $P_0 \in E$ и разностью $G \in E$ и задаётся следующим рекуррентным соотношением:

$$P_n = P_{n-1} \oplus G = nG \oplus P_0,\ n = 1, 2, 3, ..., \qquad (1)$$

где $\oplus$ – групповая операция в $E(F_p)$.

Выходными значениями датчика (1) могут быть либо точки P_n, либо только их абсциссы x_n, либо только их ординаты y_n.

Следует отметить также статистическую безопасность генератора псевдослучайных чисел, построенного на базе арифметической прогрессии на эллиптической кривой. Она обладает хорошими статистическими свойствами, что показано в [5]: равномерностью распределения элементов арифметической прогрессии для большого t; также указан порядок величины отклонения от равномерности $O\left(\frac{\sqrt{p}\log^2 p}{t}\right)$.

Для случая, при котором известна разность G, старшие биты P_n и P_{n-1}, в работе [3] Гутиэррехом и Ибиасом предложен эффективный алгоритм нахождения P_0 для генераторов, построенных на базе арифметической прогрессии на эллиптической кривой. Он не обладает криптографической безопасностью. Секретным ключом в генераторе псевдослучайных чисел (1) должны являться P_0 и G. В этом случае неизвестны эффективные алгоритмы предсказания бит, и генератор (1) является криптографически безопасным.

В работе [1] в более общем виде рассмотрены генераторы псевдослучайных последовательностей типа арифметическая прогрессия на эллиптической кривой. Пусть порядок $|E(F_p)|$ группы $E(F_p)$ равен r.

Последовательность $P_0, P_1, P_2, ...$ точек E, удовлетворяющих рекуррентному соотношению:

$$P_{n+k} = \sum_{i=0}^{m-1} c_i P_{i+k} \oplus Q,\ k = 0, 1, 2, ..., \qquad (2)$$