к средствам высоконадежной биометрической аутентификации.
5. Надеев Д.Н. Моделирование биномиального зависимого закона распределения значений вероятностей ошибок нейросетевых преобразователей для высоконадежной биометрической защиты // Вопросы защиты информации. №3, 2008. – С. 31-35.
6. Надеев Д.Н., Иванов А.И. Модуль-нормальная связь коэффициентов парной корреляции со стойкостью нейросетевой защиты // Вопросы защиты информации. №3, 2008. – С. 35-38.
7. Шалыгин А.С., Палагин Ю.И. Прикладные методы статистического моделирования. Л.: Машиностроение, 1986. – 320 с.

CODE CHAINS MODELLING WITH ENTROPY NETURAL AND SYNTETIC LANGUAGE

Ivanov A.I., Mayorov A.V., Nadeev D.N., Funtikov V.A.

It is shown, that changing entropy of natural and synthetic languages function is unambiguously concerned with parameters of hi-dimension correlation matrix of random code chains. For any natural or synthetic languages can be constructed the generator of random sequences reproducing sorting pair-correlation matrix of language and its exponent of lowering entropy, when spectator dimension is growth.

Keywords: *modeling, biometric codes, entropy, hi-dimension correlation matrix.*

Иванов Александр Иванович, д.т.н., доцент, начальник Лаборатории нейросетевых и биометрических технологий ФГУП «ПНИЭИ» (г. Пенза). Тел. (8-841) 259-33-10.
Майоров Александр Викторович, инженер ФГУП «ПНИЭИ». Тел. 8-906-397-24-27. E-mail: sasha.maiorov@mail.ru
Надеев Дамир Наилевич, к.т.н., м.н.с. ФГУП «ПНИЭИ». Тел. (8-841) 259-33-10.
Фунтиков Вячеслав Александрович, к.т.н., генеральный директор ФГУП «ПНИЭИ». Тел. (8412) 59-33-10.

УДК 681.3

АЛГОРИТМ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Бабенко М.Г., Стрекалов Ю.А., Червяков Н.И.

В статье проанализированы существующие алгоритмы цифровой подписи на эллиптической кривой. Выработаны требования для построения алгоритма цифровой подписи на эллиптической кривой над кольцом Z_q, все вычисления в которой производятся с использованием системы остаточных классов.

Ключевые слова: эллиптическая кривая, цифровая подпись, криптосистемы, поля Галуа, система остаточных классов, дискретный логарифм, сингулярные и несингулярные кривые.

Введение. Постановка задачи

Эллиптические кривые над конечными полями – один из самых перспективных инструментов для построения криптографических алгоритмов [1]. Это обусловлено тем, что эллиптическая кривая обеспечивает максимально возможную для криптосистемы с открытым ключом стойкость на один бит размера задачи [2]. Эллиптическая кривая E над простым полем F_p, где $p > 3$, задана уравнением в форме Вейерштрассе

$$E(F_p): y^2 = x^3 + ax + b, \text{ где } 4a^3 + 27b^2 \neq 0. \quad (1)$$

Решение уравнения (1) совместно с бесконечно удаленной точкой задает множество точек эллиптической кривой.

Алгоритм формирования цифровой подписи на эллиптической кривой состоит из двух этапов:

1. Сжатие текста M до размера поля с помощью однонаправленной хеш-функции $h(M)$.

2. Шифрование $h(M)$ с помощью секретного ключа отправителя на эллиптической кривой.

Первый этап формирования цифровой подписи – алгоритмы вычисления хеш-функций по SHA, ГОСТ Р34.11-94 и др. – в данной статье мы рассматривать не будем.

Проанализируем второй этап формирования цифровой подписи – шифрование $h(M)$ с ис-

пользованием секретного ключа по ГОСТ Р34.10-2001, согласно которому эллиптическая кривая задается уравнением (1), где простое число $p > 2^{255}$. Для этой эллиптической кривой находим порядок группы точек эллиптической кривой. Из известных в настоящее время алгоритмов самым быстрым для произвольной эллиптической кривой является SEA, требующий $\log_2^6 p$ операций, так как $p > 2^{255}$, то $\log_2^6 p > 274\,941\,996\,890\,625$. При условии, что процессор выполняет $2{,}4 \times 10^9$ операций в секунду, получим, что порядок одной кривой будет вычисляться приблизительно 32,5 часа. Этот алгоритм является непрактичным из-за большой сложности.

Сложность генерации может быть уменьшена при использовании эллиптической кривой над кольцом Z_q, где $q = \prod_{i=1}^{n} p_i$, p_i – попарно различные простые числа и для каждого $i \in \{1; 2 \ldots n\}$, $p_i > 3$.

Пусть эллиптическая кривая над кольцом задана уравнением

$$E(Z_q): y^2 = x^3 + ax + b \text{ над } Z_q, \qquad (2)$$

где $q = \prod_{j=1}^{n} p_j$ и p_j – попарно простые числа и $p_i > 3$.

Основной задачей исследования является разработка требования к алгоритму цифровой подписи на эллиптической кривой над кольцом Z_q.

Решение поставленной задачи включает в себя рассмотрение следующих пунктов.

1. Анализ существующих методов построения криптосистем на эллиптической кривой.

2. Разработка метода нахождения порядка группы точек эллиптической кривой, заданной уравнением (2).

3. Оценка значений, которые может принимать порядок группы точек эллиптической кривой.

4. Выработка критерия, при котором кривая $E(Z_q)$ была бы несингулярной.

5. Анализ методов решения задачи дискретного логарифмирования на эллиптической кривой.

Анализ существующих методов построения криптосистем на эллиптической кривой

Методы построения криптосистем на эллиптической кривой можно разделить на две группы в зависимости от того, над каким полем они строятся.

1. Над расширенным полем Галуа F_{p^n}, где p – простое число, $p > 3$ и $m > 0$.

2. Над расширенным полем Галуа F_{2^n}, где $m > 1$.

В зависимости от того, над каким полем строится криптосистема, к ней предъявляют соответствующие требования. Проанализируем критерии, которым должна удовлетворять эллиптическая кривая по международному стандарту ISO/IEC CD 15946-2.

Рассмотрим первый тип.

Используются кривые, заданные уравнением $E(F_{p^m}): y^2 = x^3 + ax + b$, где $a, b \in F_{p^m}$ и $m > 0$, порядка $\#E(F_{p^m}) = hn$ с генератором $G = (x_G, y_G)$. Причем a, b генерируются случайным образом из двоичной случайной последовательности и $4a^3 + 27b^2 \neq 0$ в F_{p^m}.

1. Числа $x_G, y_G \in F_{p^m}$ удовлетворяют $y_G^2 = x_G^3 + ax_G + b$ в F_{p^m}.

2. На n накладываются ограничения: n – простое число, $n > 4\sqrt{p^m}$, $nG \neq O$.

3. Проверяется, чтобы $h \neq \left[\frac{(\sqrt{p^m} + 1)^2}{n} \right]$.

4. Проверяется выполнение MOV-условия с целью исключения криптографически слабых кривых $p^{mk} \neq 1 \bmod n$, $k = 1; 2; 3 \ldots B$, $B \geq 20$.

Проверка того, чтобы кривая не являлась аномальной $\#E(F_{p^m}) \neq p^m$.

Рассмотрим второй тип.

Используются кривые, заданные уравнением $E(F_{2^m}): y^2 + xy = x^3 + ax^2 + b$, где $a, b \in F_{2^m}$ и $m > 1$, порядка $\#E(F_{2^m}) = hn$ с генератором $G = (x_G, y_G)$. Причем a, b-генерируются случайным образом из двоичной случайной последовательности.

1. Числа a, b, x_G, y_G являются двоичными векторами длины m и $a, b \notin F_2$ удовлетворяют $y_G^2 + x_G y_G = x_G^3 + ax_G^2 + b$ в F_{2^m}.

2. На n накладываются ограничения: n – простое число, $n > 2^{160}$ и $n > 4\sqrt{2^m}$, $nG \neq O$.

3. Проверяется, чтобы $h \neq \left[\frac{(\sqrt{2^m} + 1)^2}{n} \right]$.

4. Проверяется выполнение MOV-условия, исключающего суперсингулярные кривые и слабые несуперсингулярные кривые $2^{mk} \neq 1 \bmod n$, $k = 1; 2; 3 \ldots B$, $B \geq 20$.

Данная криптосистема обладает существенным недостатком, так как допускается к использованию составное число m. Это может привести к взлому криптосистемы методом спуска Вейля [3].

В первом и втором случаи проверяют на MOV-условия, так как если эти условия не выполняются, то можно вычислить дискретный логарифм методом [4].

Метод нахождения порядка группы точек, заданной уравнением (2)

Для этого рассмотрим уравнение

$$y^2 = x^3 + ax + b \pmod{p_i}. \quad (3)$$

1. Найдем количество решений n_i сравнения (3), используя формулу $n_i = p_i + \sum_{x \in F_{p_i}} \left(\frac{x^3 + ax + b}{p_i} \right)$, где $\left(\frac{x^3 + ax + b}{p_i} \right)$ – символ Лежандра.

2. Вычислим порядок по формуле

$$\#E(Z_q) = \prod_{i=1}^{n} n_i + 1. \quad (4)$$

Предложенный метод применим при небольших значения числа p_i, так как сложность возрастает по экспоненциальному закону с увеличением числа p_i. Из того, что между числом и его удвоением существует хотя бы одно простое число, следует, что при соответствующем выборе простых чисел сложность нахождения $\#E(Z_q)$ не превысит $O(\log^2(q))$.

Оценим, какие значения может принимать порядок группы точек эллиптической кривой. Для чего воспользуемся границами Хассе [2]:

$$p_i + 1 - 2\sqrt{p_i} \le \#E(F_{p_i}) \le p_i + 1 + 2\sqrt{p_i}. \quad (5)$$

Из неравенства (5) следует, что n_i ограничено неравенством

$$p_i - 2\sqrt{p_i} \le \#E(F_{p_i}) \le p_i + 2\sqrt{p_i}. \quad (6)$$

Воспользовавшись формулой (4) и неравенством (6), получим, что

$$q\prod_{i=1}^{n}\left(1 - \frac{2}{\sqrt{p_i}}\right) + 1 \le \#E(Z_q) \le q\prod_{i=1}^{n}\left(1 + \frac{2}{\sqrt{p_i}}\right) + 1. \quad (7)$$

Оценим, какие значения может принимать левая часть неравенства (7) – $q\prod_{i=1}^{n}\left(1 - \frac{2}{\sqrt{p_i}}\right) + 1$.

Так как $1 - \frac{2}{\sqrt{p_i}} < 1$, то $\prod_{i=1}^{n}\left(1 - \frac{2}{\sqrt{p_i}}\right) < 1$, и значит левая часть неравенства $q\prod_{i=1}^{n}\left(1 - \frac{2}{\sqrt{p_i}}\right) + 1 < q + 1$.

Используя неравенство о среднем геометрическом $\min(x_1, x_2, ..., x_n) \le \sqrt[n]{\prod_{i=1}^{n} x_i}$, получим, что $\frac{1}{10^m} < \left(1 - \frac{2}{\sqrt{5}}\right)^n \le \prod_{i=1}^{n}\left(1 - \frac{2}{\sqrt{p_i}}\right)$ и следовательно $\frac{q}{10^n} + 1 < q\prod_{i=1}^{n}\left(1 - \frac{2}{\sqrt{p_i}}\right) + 1 < q + 1$.

Оценим, какие значения может принимать правая часть неравенства (7) – $q\prod_{i=1}^{n}\left(1 + \frac{2}{\sqrt{p_i}}\right) + 1$, используя неравенство о среднем геометрическом $\sqrt[n]{\prod_{i=1}^{n} x_i} \le \max(x_1, x_2, ..., x_n)$. Получим $\prod_{i=1}^{n}\left(1 + \frac{2}{\sqrt{p_i}}\right) \le \left(1 + \sqrt{2}\right)^n$.

Определение. Кривая E называется сингулярной, если существует хотя бы одна точка (x, y), в которой частные производные функции $F(x, y) = y^2 - x^3 - ax - b$ одновременно обращаются в 0. В противном случае кривая E называется несингулярной.

Определим, каким условиям должна удовлетворять эллиптическая кривая, заданная уравнением (2), чтобы быть несингулярной.

Известно, что эллиптическая кривая, заданная над полем F_{p_i}, несингулярна, если $4a^3 + 27b^2 \ne 0 \pmod{p_i}$.

Утверждение 1. Эллиптическая кривая $E(Z_q)$, заданная уравнением (2), несингулярна тогда и только тогда, когда существует p_i такое, что $4a^3 + 27b^2 \ne 0 \pmod{p_i}$.

Следствие. Эллиптическая кривая $E(Z_q)$, заданная уравнением (2), несингулярна тогда и только тогда, когда $4a^3 + 27b^2 \ne 0 \pmod{q}$.

Из следствия получим метод определения, является ли эллиптическая кривая сингулярной.

Метод определения сингулярности или несингулярности кривой $E(Z_q)$

1. Вычисляем значение $D = 4a^3 + 27b^2$.

2. Проверка: если $D \equiv 0 \bmod q$, то эллиптическая кривая сингулярна, иначе – несингулярна.

Утверждение 2. Пусть точки $P(x_P, y_P), Q(x_Q, y_Q) \in E(Z_q)$, где $E(Z_q)$ – эллиптическая кривая, заданная уравнением (1) и $P = lQ$, $l \in Z$. Тогда точки $P_i(x_P \bmod p_i, y_P \bmod p_i)$, $Q_i(x_Q \bmod p_i, y_Q \bmod p_i)$ принадлежат $E(F_{p_i})$ и $l = k_i \pmod{ord(Q_i)}$, где $E(F_{p_i})$: $y^2 = x^3 + a^{(i)}x + b^{(i)}$ и $a^{(i)} \equiv a \pmod{p_i}$ и

$b^{(i)} \equiv b(\mathrm{mod}\, p_i)$, справедлива система $P_i = k_i Q_i$ для всех $i = 1 \ldots n$.

Из утверждения 2 следует метод нахождения дискретного логарифма над Z_q.

Метод нахождения дискретного логарифма над Z_q

1. Вычислим порядок точки $ord(Q)$ на кривой $E(Z_q)$.

2. Вычислим $P_i(x_P \bmod p_i, y_P \bmod p_i)$, $Q_i(x_Q \bmod p_i, y_Q \bmod p_i)$ принадлежит $E(F_{p_i})$.

3. Вычислим порядок точки $ord(Q_i)$ на эллиптической кривой $E(F_i)$.

4. Решим задачу дискретного логарифмирования при каждом из p_i. При этом найдем k_i.

5. По китайской теореме об остатках найдем l по модулю $HOK(ord(Q_i))$.

6. Найдем истинное значение l, используя формулу $l = l_1 + s \cdot HOK(ord(Q_i))$, где s может принимать значения

$$0 \le s \le \frac{\#E(Z_q)}{HOK(ord(Q_i))} \le \frac{q\prod_{i=1}^{n}\left(1+\frac{2}{\sqrt{p_i}}\right)+1}{HOK(ord(Q_i))}.$$

Из предложенного метода следует, что стойкость криптосистемы зависит от диапазона значений, которые может принимать s.

Оценим, каким должно быть число n, чтобы криптосистема, построенная над Z_q, обладала такой же криптостойкостью, как ГОСТ 34.10.2001.

Пусть $ord(Q_i) = ck_i$ для всех $i = 1 \ldots n$, где $c = const$ и k_i – попарно простые числа, тогда $HOK(ord(Q_i)) = c\prod_{i=1}^{n} k_i$. Так как $k_i < \frac{p_i + 2\sqrt{p_i}}{c}$, то $HOK(ord(Q_i)) < \frac{\prod_{i=1}^{n}\left(p_i + 2\sqrt{p_i}\right)}{c^{n-1}}$ и значит $s < c^{n-1}$.

Из неравенства следует, что n должно удовлетворять неравенству $n \ge 128 \times \log_c 2$.

На основании анализа изложенных фактов получим требования, которым должна удовлетворять криптосистема эллиптической кривой над Z_q.

Требования к кривой для алгоритма цифровой подписи над Z_q

Эллиптическая кривая задается уравнением (2) порядка $\#E(Z_q) = hm$ с генератором $G = (x_G, y_G)$, a, b генерируются случайным образом из двоичной случайной последовательности.

1. Вычисляем $c \ge 1$.

2. Количество различных простых чисел p_i для построения модуля $q = \prod_{i=1}^{n} p_i$ должно быть больше $n \ge 128 \times \log_c 2$.

3. Используя метод проверки на сингулярность эллиптической кривой, проверяем несингулярность кривой.

4. Проверяем, чтобы $m > 4\sqrt{q}$.

5. Вычисляем $\frac{\#E(Z_q)}{HOK(ord(Q_i))}$ и проверяем, чтобы $\frac{ord(Q)}{HOK(ord(Q_i))} \ge 2^{128}$.

6. Проверяем, чтобы $h \ne \left\lfloor \frac{(\sqrt{q}+1)^2}{m} \right\rfloor$.

7. Проверяем выполнение MOV-условия с целью исключения криптографически слабых кривых $(q^k - 1) \ne 0 \bmod m$, $k = 1; 2; 3 \ldots B$, $B \ge 20$.

Приведем пример эллиптической кривой для Z_q, удовлетворяющий данным условиям.

Эллиптическая кривая задается уравнением: $E(Z_q): y^2 = x^3 + 3x + 49$, где $n = 16$, $q = \prod_{i=1}^{n} p_i$, $p_1 = 1307$, $p_2 = 1523$, $p_3 = 3301$, $p_4 = 3851$, $p_5 = 5023$, $p_6 = 5519$, $p_7 = 6037$, $p_8 = 6067$, $p_9 = 6673$, $p_{10} = 7517$, $p_{11} = 8243$, $p_{12} = 8521$, $p_{13} = 9157$, $p_{14} = 9311$, $p_{15} = 9623$, $p_{16} = 9859$.

Промежуточные вычисления для нахождения порядка группы точек эллиптической кривой $E(Z_q)$ оформим в идее таблицы 1.

Таблица 1. Вычисление n_i, $\#E(F_{p_i})$, k_i

i	n_i	$\#E(F_{p_i})$	k_i
1	1279	1280	5
2	1535	1536	6
3	3327	3328	13
4	3839	3840	15
5	5119	5120	20
6	5375	5376	21
7	6143	6144	24
8	6143	6144	24
9	6655	6656	26
10	7679	7680	30
11	8191	8192	32
12	8447	8448	33
13	9215	9216	36
14	9215	9216	36
15	9727	9728	38
16	9983	9984	39

1. Из таблицы 1 видно, что $c = 256$.

2. Проверяем, что $n \geq 128 \times \log_{256} 2 = 16$.

3. $\Delta = 4 \times 3^3 + 27 \times 49^2 = 64935$, $\Delta \bmod p_1 = 892$, следовательно, эллиптическая кривая не является сингулярной.

4. Вычислим m, для этого найдем порядок группы точек эллиптической кривой $\#E(Z_a)$.

$$\#E(Z_q) = \prod_{i=1}^{n} n_i = 2 \times 13 \times 631 \times 2719 \times 5602747 \times$$

$$\times 10237351 \times m,$$

где

$m = 296685799117865607917473 47 \backslash$

7163894836097,

$m > 4\sqrt{\mathrm{q}} = 348504693348947141907940601 5120$.

5. Для того, чтобы вычислить $\frac{\#E(Z_q)}{HOK(ord(Q_i))}$, найдем

$$HOK(k_1, k_2, k_2, ..., k_{16}) = 2^5 \times 3^2 \times 5 \times 7 \times 11 \times 13 \times$$

$$\times 19 = 27387360.$$

Значит, на s накладывается следующее ограничение:

$$0 \leq s \leq \frac{\#E(Z_q)}{256 \times HOK(k_1, k_2, ..., k_{16})} \approx 10^{51},$$ что больше 2^{128}, так как $2^{128} \approx 3 \times 10^{39}$.

6. Для проверки $h \neq \left\lfloor \frac{(\sqrt{q}+1)^2}{m} \right\rfloor$ найдем разность h и $\left\lfloor \frac{(\sqrt{q}+1)^2}{m} \right\rfloor$.

$$h = 2 \times 13 \times 631 \times 2719 \times 5602747 \times$$

$$\times 10237351 = 2558588952676677901058$$

$$h - \left\lfloor \frac{\left(\sqrt{q}+1\right)^2}{m} \right\rfloor = 90556016565396294140.$$

Так как $h - \left\lfloor \frac{\left(\sqrt{q}+1\right)^2}{m} \right\rfloor \neq 0$, то

$$h \neq \left\lfloor \frac{\left(\sqrt{q}+1\right)^2}{m} \right\rfloor.$$

7. Проверка MOV-условия:

$(q-1) \bmod m = 267323210302817714937740 \backslash$

886539267449194;

$(q^2-1) \bmod m = 972007144864701615742665 \backslash$

6178903092680;

$(q^3-1) \bmod m = 235519303793933492771330 \backslash$

38368360948215;

$(q^4-1) \bmod m = 467859575511914031767984 \backslash$

37442996274278;

$(q^5-1) \bmod m = 210614378960071804894573 \backslash$

930358891128258;

$(q^6-1) \bmod m = 260418606776683823972406 \backslash$

282798753101389;

$(q^7-1) \bmod m = 655353591809606861187457 \backslash$

12211829732557;

$(q^8-1) \bmod m = 208262806612173146148393 \backslash$

926223189470760;

$(q^9-1) \bmod m = 738811342024954176386014 \backslash$

50076588198160;

$(q^{10}-1) \bmod m = 242124613933090416680968 \backslash$

1628186020996;

$(q^{11}-1) \bmod m = 253288485034591403345628 \backslash$

500477125565267;

$(q^{12}-1) \bmod m = 281479075443583511656418 \backslash$

414819410001441;

$(q^{13}-1) \bmod m = 236785606338307899921581 \backslash$

80332638568613;

$(q^{14}-1) \bmod m = 203659533140525513619215 \backslash$

228727546026051;

$(q^{15}-1) \bmod m = 121565525058526780634507 \backslash$

778132694543593;

$(q^{16}-1) \bmod m = 487853009766654043567840 \backslash$

174626359090;

$(q^{17}-1) \bmod m = 999464153558158931191584 \backslash$

01593143678816;

$(q^{18}-1) \bmod m = 748173768404199522817378 \backslash$

59581396501641;

$(q^{19}-1) \bmod m = 500757187164170909705585 \backslash$

38645954097754;

$(q^{20}-1) \bmod m = 190976903375553814332991 \backslash$

734977266399815;

$(q^{21}-1) \bmod m = 121024018883379912562610 \backslash$

170063031719450.

Следовательно, данная кривая удовлетворяет всем требованиям для алгоритма цифровой подписи над Z_q.

Выводы

В работе проанализированы существующие методы построения криптосистем и предложен

алгоритм построения цифровой подписи на эллиптической кривой над кольцом Z_q с выбором параметров криптосистемы. Это обусловлено тем, что все вычисления в этой криптосистеме можно производить в проективной системе координат с использованием системы остаточных классов, что позволяет существенно ускорить вычисления и повысить скорость работы криптосистемы.

Литература

1. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. CRC press, 2. 1997. – 816 p.
2. Ростовцев А. Г. Маховенко Е. Б. Два подхода к логарифмированию на эллиптической кривой. http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf
3. Gordon M. D. A Survey of Fast Exponentiation Methods // Journal of Algorithms, 27. 1998. – P. 129-146.
5. Menezes A., Okamoto T., Vanstone S., Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Transactions on Information Theory, 39, 1993. – P. 1639-1660.

ALGORITHM OF THE DIGITAL SIGNATURE ON AN ELLIOTIC CURVE

Babenko M.G., Strekalov Y.A., Chervaykov N.I.

The existing algorithms of the digital signature on an elliptic curve are analyzed in article. Requirements for construction of algorithm of the digital signature on an elliptic curve over a ring Z_q are worked out, all calculations in it are made with use of system of residual classes.

Keywords: *elliptic curve, digital signature, cryptosystem, fields Galois, system of residual classes, discrete logarithm, singular and not singular curves.*

Бабенко Михаил Григорьевич, аспирант Кафедры «Высшая алгебра и геометрия» Ставропольского государственного университета (СГУ). Тел (8-8652) 38-80-84. E-mail: whbear@yandex.ru

Стрекалов Юрий Анатольевич, к.т.н., доцент Ставропольского филиала Поволжского государственного университета телекоммуникаций и информатики. (8-8652) 35-19-76. E-mail: sfpgati@yandex.ru

Червяков Николай Иванович, д.т.н., профессор, заведующий кафедрой «Прикладная математика и информатика» СГУ. Тел. (8-8652) 35-68-32, доб. 1154; 8 (8652) 35-48-61.

УДК 654.9

АЛГОРИТМ ОБРАБОТКИ ИЗОБРАЖЕНИЙ ПРИ ФОТОГРАММЕТРИЧЕСКИХ ИЗМЕРЕНИЯХ

Первунинских Д.В.

В статье рассмотрены специфика и варианты обработки изображений фотограмметрических измерений при съемке неметрической фотокамерой.

Ключевые слова: измерения; метрологические параметры; калибровка; фотограмметрия; неметрическая фотокамера; концевые меры; обработка изображений; программное обеспечение; стереомодель.

Введение

Наиболее часто при проведении фотограмметрических измерений используют стереоскопические фотоаппараты (неметрические фотокамеры). При этом делается два снимка одинаковыми объективами, выставленными в определенных направлениях.

Для вычисления результатов измерения в трехмерных координатах полагают следующие допущения [1]:

- точки размещения фотокамеры по горизонтальной оси симметричны ($x_1 = 0{,}5\ b$; $y = 0$; $z = 0$ и $x_2 = -0{,}5b$; $y = 0$; $z = 0$; b – расстояние между центрами осей фотоаппаратов при съемке);
- оптическая ось фотоаппарата параллельна вертикальной оси z измерительной системы координат;
- оси x и y систем координат снимка и измерительной системы совпадают;
- отсутствуют искажения геометрии изображения (дисторсия).

Координаты точки объекта x, y, z определяются из подобия треугольников [1] путем нахождения координат отображений u и v на первом и втором снимках.

$$u_1 = -f\frac{x - b/2}{z},\ v_1 = -f\frac{y}{z};$$
$$u_2 = -f\frac{x + b/2}{z},\ v_2 = -f\frac{y}{z}. \quad (1)$$