УДК 004.052.2

РЕАЛИЗАЦИЯ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ С ДОКАЗАТЕЛЬСТВОМ НУЛЕВОГО РАЗГЛАШЕНИЯ ЗНАНИЙ С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНЫХ КОДОВ

[1]Калмыков М.И., [2]Бабенко Л.К., [1]Калмыков И.А., [1]Ефременков И.Д.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;
[2]ФГАОУ ВО «Южный федеральный университет», Ростов-на-Дону

Применение низкоорбитальных систем спутниковой связи (ССС) в автоматизированных системах дистанционного контроля и управления, которые располагаются за Полярным кругом, позволяет осуществлять с высокой достоверностью передачу данных от объектов нефтедобычи в центр управления. Для обеспечения эффективной работы ССС содержит от 48 до 60 космических аппаратов. Увеличение числа таких орбитальных группировок может привести к ситуации, когда спутник-нарушитель попытается навязать ретрансляционную помеху приемному устройству, расположенному на необслуживаемом объекте управления. В результате этого такая имитированная команда управления приведет к выходу из строя объекта нефтедобычи, что может нанести ущерб природе Арктики. Для устранения такой ситуации предлагается использовать запросно-ответные системы опознавания статуса спутника. Очевидно, что имитостойкость такой системы во многом зависит от протокола аутентификации. С целью сокращения временных затрат на выполнение процедур аутентификации в статье предлагается использовать модулярные коды. В данных кодах вычисления осуществляются параллельно по модулям кода и независимо от друг от друга. Целью исследований является повышение скорости выполнения протокола аутентификации типа «запрос – ответ» за счет использования модулярных кодов.

Ключевые слова: запросно-ответная система распознавания спутника, протоколы аутентификации типа «запрос – ответ», протоколы доказательства с нулевым разглашением знаний, модулярный код

THE IMPLEMENTATION OF AUTHENTICATION PROTOCOLS WITH ZERO-KNOWLEDGE PROOF OF KNOWLEDGE USING MODULAR CODES

[1]Kalmykov M.I., [2]Babenko L.K., [1]Kalmykov I.A., [1]Efremenkov I.D.

[1]Federal State Autonomous Educational Institution Higher Professional Education «North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru;
[2]Federal State Autonomous Educational Institution of Higher Education «Southern Federal University», Rostov-on-Don

The use of low-orbit satellite communication systems (SCS) in automated systems for remote monitoring and control, which are located in the Arctic Circle, allows for high reliability of data transfer from oil drilling sites to the control center. To ensure effective work of the SCS contains from 48 to 60 spacecraft. The increase in the number of orbital groups can lead to the situation when the satellite-the offender tries to impose on relay interference receptor, located on the automatic control object. As a result, such simulated management team will lead to the failure of oil production facilities that may cause damage to the environment of the Arctic. To resolve this situation, we propose to use a request-response system of the recognition of the status of the satellite. It is obvious that infotouriste of such a system depends on the authentication Protocol. With the aim of reducing the time spent on the implementation of authentication procedures, the article proposes the use of modular codes. In these codes, calculations are performed in parallel according to the code modules and independently from each other. The aim of the research is to increase the speed of execution of the authentication Protocol of the type «request-response» through the use of modular codes.

Keywords: request-response detection system of the satellite, the authentication protocols of the type «request-response», protocols of the proof with zero disclosure of knowledge, modular code

Для снижения стоимости добычи и транспортировки углеводородов из Арктики широко применяются автоматизированные системы дистанционного контроля и управления объектами нефтедобычи. Для организации связи между необслуживаемыми объектами и центром управления используются низкоорбитальные системы спутниковой связи (ССС). С целью противодействия навязывания ретрансляционной помехи спутником-нарушителем, которая имитирует команду управления, в работах [1] предлагается использовать запросно-ответную систему распознавания спутника (ЗОСРС). Очевидно, что имитостойкость такой системы во многом зависит от протокола аутентификации. Как правило, такие протоколы типа «запрос – ответ», базирующиеся на доказательстве с нулевым разглашением знаний (ДНРЗ), реализуются по большому модулю, что негативно сказывается на скорости аутентификации. Снизить временные затраты на проверку статуса спутника можно за счет применения модулярных кодов (МК). Поэтому реализация протоколов аутентификации с доказательством нулевого разглашения знаний с использованием модулярных кодов является актуальной задачей.

Цель исследования

Для повышения имитостойкости запросно-ответной системы распознавания спутника применяются протоколы, базирующиеся на доказательстве с нулевым разглашением знаний. С целью повышения криптостойкости в таких протоколах используются большие числа. Однако увеличение разрядности обрабатываемых данных приводит к снижению скорости выполнения мультипликативных операций. Применение непозиционных МК позволяет не только повысить точность, но и скорость вычислений. Это обусловлено тем, что в этих кодах операнды – это остатки, полученные по модулям МК. А операции сложения, вычитания и умножения выполняются параллельно без обмена данными между разными модулями [2–4]. Поэтому целью работы является повышение скорости выполнения протокола аутентификации за счет использования модулярных кодов.

Материалы и методы исследования

К модулярным кодам относятся непозиционные коды, в которых число А представляется в виде остатков $A = (\alpha_1, \alpha_2, ..., \alpha_k)$, где $\alpha_i \equiv A \bmod m_i$, m_i – основания МК, в качестве которых используют взаимно простые целые числа, $i = 1, 2, \ldots, k$ [2–4]. Тогда для МК справедливы следующие выражения

$$A + Y = ((\alpha_1 + y_1) \bmod m_1, (\alpha_2 + y_2) \bmod m_2, ..., (\alpha_k + y_k) \bmod m_k), \quad (1)$$

$$A - Y = ((\alpha_1 - y_1) \bmod m_1, (\alpha_2 - y_2) \bmod m_2, ..., (\alpha_k - y_k) \bmod m_k), \quad (2)$$

$$A \cdot Y = ((\alpha_1 \cdot y_1) \bmod m_1, (\alpha_2 \cdot y_2) \bmod m_2, ..., (\alpha_k \cdot y_k) \bmod m_k), \quad (3)$$

где $Y \equiv y_i \bmod m_i$; $i = 1,2,\ldots, k$.

Для получения правильного ответа в МК необходимо, чтобы результаты операций не выходили за пределы рабочего диапазона, определяемого

$$P_{\text{раб}} = \prod_{i=1}^{k} m_i. \quad (4)$$

Анализ выражений (1)–(3) показывает, что операции сложения, вычитания и умножения можно свести к соответствующим операциям по модулю m_i, что позволяет повысить скорость вычислений.

Для построения имитостойкой ЗОСРС целесообразно использовать протоколы аутентификации, которые базируются на доказательстве с нулевым разглашением знаний и обладают высокой криптостойкостью. В работе [5] показан протокол аутентификации Фиата – Шамира, для реализации которого требуется t раундов проверки. При этом в каждом раунде выполняется трехшаговый алгоритм интерактивного обмена информацией для проверки претендента несколько раундов. Причем при увеличении числа раундов растет криптостойкость протокола. Аналогичным недостатком обладает протокол аутентификации Гиллоу – Куискуотера [6], также базирующийся на ДНРЗ. Данный протокол использует меньшее количество раундов информационного обмена, чем протокол Фиата – Шамира. Однако для достижения заданной вероятности доказательств корректности представленного идентификатора требуется использование многораундовой процедуры аутентификации.

Устранить данный может протокол аутентификации Шнорра, алгоритм работы которого приведен в [7]. Рассмотрим реализацию данного протокола в модулярном коде. Выбираем в качестве оснований простые числа m_1, m_2, …, m_k, для которых ищем простое число q_i, – делитель m_i. Затем определяется число g_i, которое удовлетворяет условию

$$g_i^{q_i} \equiv 1 \bmod m_i. \quad (5)$$

Секретным ключом выбирают число $X = (x_1, x_2, \ldots, x_k)$, которое удовлетворяет условию

$$X < Q = \prod_{i=1}^{k} q_i. \quad (6)$$

Открытым ключом является число $Y = (y_1, y_2, \ldots, y_k)$, где справедливо

$$y_i = g_i^{-x_i} \bmod m_i. \quad (7)$$

Протокол аутентификации выполняется следующим образом.

1. Претендент A выбирает случайное число $S = (s_1, s_2, \ldots, s_k)$, которое удовлетворяет условию $S < Q$. Затем осуществляется вычисление числа $R = (r_1, r_2, \ldots, r_k)$, согласно

$$r_i = g_i^{s_i} \bmod m_i. \quad (8)$$

Вычисленное значение передается проверяющему абоненту B.

2. Абонент B выбирает случайное число $E = (e_1, e_2, ..., e_k) \in \{1, 2, ..., 2^t - 1\}$, где t – некоторый параметр. Данное число посылается абоненту А.

3. Абонент A, получив число E, вычисляет число $D = (d_1, d_2,\ldots, d_k)$, согласно равенству

$$d_i = (s_i + e_i x_i) \bmod q_i . \quad (9)$$

Вычисленное значение $D = (d_1, d_2,\ldots, d_k)$, посылается абоненту B.

4. Абонент B, получив ответ $D = (d_1, d_2,\ldots, d_k)$, проверяет правильность ответа

$$W_i = g_i^{d_i} y_i^{e_i} \bmod m_i . \quad (10)$$

Если вычисленное значение $W = (w_1, w_2,\ldots, w_k)$ совпадает с числом $R = (r_1, r_2,\ldots, r_k)$, то претендент A – «свой». В противном случае абонент A является «чужим».

Для проведения сравнительного анализа воспользуемся разработанным протоколом аутентификации. В основу данного протокола был положен одномодульный протокол, позволяющий определить статус претендента [8]. Осуществим его реализацию с помощью модулярного кода.

В данном протоколе применяют представленные в МК: секретный ключ $U = (u_1, u_2, ..., u_k)$, сеансовый ключ $S(j) = (S_1(j), S_2(j), ..., S_k(j))$, параметр $T(j) = (T_1(j), T_2(j), ..., T_k(j))$, используемый для уравнения «повторного применения сеансового ключа», где $U \equiv u_i \bmod m_i$; $S(j) \equiv S_i(j) \bmod m_i$; $T(j) \equiv T_i(j) \bmod m_i$; $i = 1,2,\ldots, k$.

На предварительном этапе аутентификации выполняются следующие вычисления:

1. Претендент A вычисляет истинный статус спутника, представленный в МК

$$C_i = \left| g^{u_i} g^{S_i(j)} g^{T_i(j)} \right|_{m_i}^{+}, \quad (11)$$

где g – порождающий мультипликативную группу по модулю m_i; $i = 1,2,\ldots, k$.

2. Претендент A проводит операцию зашумления секретных параметров протокола

$$u_i^* = \left| u_i + \Delta u_i \right|_{m_i}^{+};$$

$$S_i^*(j) = \left| S_i(j) + \Delta S_i(j) \right|_{m_i}^{+};$$

$$T_i^*(j) = \left| T_i(j) + \Delta T_i(j) \right|_{m_i}^{+}, \quad (12)$$

где $\Delta U, \Delta S(j), \Delta T(j)$ – случайные значения; $\Delta U \equiv \Delta u_i \bmod m_i$; $\Delta S(j) \equiv \Delta S_i(j) \bmod m_i$; $\Delta T(j) \equiv \Delta T_i(j) \bmod m_i$; $i = 1,2,\ldots, k$.

3. Претендент A вычисляет зашумленный статус спутника, используя МК

$$C_i^* = \left| g^{u_i^*} g^{S_i^*(j)} g^{T_i^*(j)} \right|_{m_i}^{+}. \quad (13)$$

Алгоритм аутентификации состоит из следующих этапов.

1. Запросчик B передает претенденту A случайное число $d = (d_1, d_2,\ldots, d_k)$.

2. Претендент A, получив $d = (d_1, d_2,\ldots, d_k)$, вычисляет ответы, согласно

$$r_i(1) = \left| u_i^* - d_i u_i \right|_{\varphi(m_i)}^{+};$$

$$r_i(2) = \left| S_i^*(j) - d_i S_i(j) \right|_{\varphi(m_i)}^{+};$$

$$r_i(3) = \left| T_i^*(j) - d_i T_i(j) \right|_{\varphi(m_i)}^{+}. \quad (14)$$

Претендент A передает запросчику B следующие данные

$$\left\{ (C_1, ..., C_k), (C_1^*, ..., C_k^*), (r_1(1), ..., r_k(1)), (r_1(2), ..., r_k(2)), (r_1(3), ..., r_k(3)) \right\}.$$

3. Запросчик B осуществляет проверку полученных ответов на вопрос $d = (d_1, d_2,\ldots, d_k)$

$$Y_i = \left| C_i^{d_i} g^{r_i(1)} g^{r_i(2)} g^{r_i(3)} \right|_{m_i}^{+}. \quad (15)$$

Претендент А имеет статус «свой», если выполняется равенство

$$\left\{ Y_1 = C_1^*, Y_2 = C_2^*, ..., Y_k = C_k^* \right\}. \quad (16)$$

Результаты исследования и их обсуждение

Рассмотрим выполнение протокола аутентификации Шнорра в модулярном коде. Выбираем основания модулярного кода МК $m_1 = 11$, $m_2 = 23$, $m_3 = 29$. Рабочий диапазон системы равен $P_{\text{раб}} = 7337$. Определим делители оснований МК $q_1 = 5$, $q_2 = 11$, $m_3 = 7$, которые имеют $Q = 385$. Воспользуемся условием (5) и выберем $g_1 = 3$, $g_1 = 2$, $g_3 = 7$. Пусть секретный ключ абонента A равен $X = (3, 5, 5)$. Тогда первая часть открытого ключа, представленного в модулярном коде, будет равна

$$y_1 = g_1^{-x_1} \bmod m_1 = 3^{-3} \bmod 11 = 3^7 \bmod 11 = 9;$$

$$y_2 = g_2^{-x_2} \bmod m_2 = 2^{-5} \bmod 23 = 2^6 \bmod 23 = 18;$$

$$y_3 = g_3^{-x_3} \bmod m_3 = 7^{-5} \bmod 29 = 2^{23} \bmod 29 = 20.$$

В этом случае открытый ключ имеет вид $(y_i, p_i, g_i) = ((9, 18, 20)(11, 23, 29)(3, 2, 7))$.

1. Претендент A выбирает числа S = (2, 7, 3) и вычисляет число $R = (r_1, r_2, r_3)$, согласно

$$r_1 = g_1^{s_1} \bmod m_1 = 3^2 \bmod 11 = 9;$$

$$r_2 = g^{s_2} \bmod m_2 = 2^7 \bmod 23 = 13;$$

$$r_3 = g_3^{s_3} \bmod m_3 = 7^3 \bmod 29 = 24.$$

Вычисленное значение $R = (9, 13, 24)$ передается запросчику B.

2. Запросчик B выбирает число E = (4, 8, 4), которое передается претенденту A.

3. Претендент A вычисляет ответ на поставленный вопрос e, используя равенство (9)

$$d_1 = (s_1 + e_1 x_1) \bmod q_1 = (2 + 4 \cdot 3) \bmod 5 = 4;$$

$$d_2 = (s_2 + e_2 x_2) \bmod q_2 = (7 + 8 \cdot 5) \bmod 11 = 3;$$

$$d_3 = (s_3 + e_3 x_3) \bmod q_3 = (3 + 4 \cdot 5) \bmod 7 = 2.$$

Вычисленное значение $D = (4, 3, 2)$ посылается абоненту B.

4. Абонент B проверяет правильность ответа согласно (10)

$$w_1 = g_1^{s_1} y_1^{e_1} \bmod m_1 = (3^4 \cdot 9^4) \bmod 11 = 3^2 \bmod 11 = 9;$$

$$w_2 = g_2^{s_2} y_2^{e_2} \bmod m_2 = (2^3 \cdot 18^8) \bmod 23 = 13;$$

$$w_3 = g_3^{s_3} y_3^{e_3} \bmod m_3 = (7^2 \cdot 20^4) \bmod 29 = 24.$$

Так как справедливо, что $W = (9, 13, 24) = R$, то статус претендента A – «свой».

Рассмотрим выполнение разработанного протокола аутентификации в модулярном коде. Пусть заданы основания $m_1 = 13$, $m_2 = 19$, $m_3 = 29$, для которых имеется $g = 2$. Рабочий диапазон будет равен $P_{раб} = 7136$. В качестве секретного ключа выбираем $U = 24 = (11, 5, 24)$, в качестве сеансового ключа $S(j) = 16 = (3, 16, 16)$, а параметр $T(j) = 25 = (12, 6, 25)$. Воспользуемся выражением (11) и получим истинный статус космического аппарата

$$C_1 = g^{U_1} g^{S_1} g^{T_1} \bmod m_1 = \left|2^{11} \cdot 2^3 \cdot 2^{12}\right|_{13}^{+} = \left|2^2\right|_{13}^{+} = 4;$$

$$C_2 = g^{U_2} g^{S_2} g^{T_2} \bmod m_2 = \left|2^5 \cdot 2^{16} \cdot 2^6\right|_{19}^{+} = \left|2^9\right|_{19}^{+} = 18;$$

$$C_3 = g^{U_3} g^{S_3} g^{T_3} \bmod m_3 = \left|2^{24} \cdot 2^{16} \cdot 2^{25}\right|_{29}^{+} = \left|2^9\right|_{29}^{+} = 19.$$

Истинный статус в коде $C = (4, 18, 19)$ записывается в память спутника.

Выбираем величину «зашумление» равное $\Delta U = 4, \Delta S = 7, \Delta T = 8$. Тогда получаем следующие зашумленные значения $U^* = (15, 7, 16)$, $S^*(j) = (12, 4, 13)$ и $T^*(j) = (3, 24, 4)$. Воспользуемся выражение (12) и получим значение зашумленного статуса спутника

$$C_1^* = g^{K_1^*} g^{S_1^*} g^{T_1^*} \bmod m_1 = \left(2^{15} \cdot 2^7 \cdot 2^{16}\right) \bmod 13 = 2^2 \bmod 13 = 4;$$

$$C_2^* = g^{K_2^*} g^{S_2^*} g^{T_2^*} \bmod m_2 = \left(2^{12} \cdot 2^4 \cdot 2^{13}\right) \bmod 19 = 2^{11} \bmod 19 = 15;$$

$$C_3^* = g^{K_3^*} g^{S_3^*} g^{T_3^*} \bmod m_3 = \left(2^3 \cdot 2^{24} \cdot 2^4\right) \bmod 29 = 2^3 \bmod 29 = 8.$$

Вычисленное значение зашумленного статуса $C^* = (4, 15, 8)$ записывается в память.

Рассмотрим процесс аутентификации спутника. Запросчик, увидев космический аппарат, передает случайное число $d = (8, 5, 4)$. Найдем ответы на вопрос $d_1 = 8$. Получаем

$$r_1(1) = \left(U_1^* - d_1 U_1\right) \bmod \varphi(13) = \left(15 - 8 \cdot 11\right) \bmod 12 = (-1) \bmod 12 = 11;$$

$$r_1(2) = \left(S_1^*(j) - d_1 S_1(j)\right) \bmod \varphi(13) = \left(12 - 8 \cdot 3\right) \bmod 12 = 0;$$

$$r_1(3) = \left(T_1^*(j) - d_1 T_1(j)\right) \bmod \varphi(13) = \left(3 - 8 \cdot 12\right) \bmod 12 = 3.$$

Найдем ответы на вопрос $d_2 = 5$. Получаем следующие ответы:

$$r_2(1) = \left(U_1^* - d_2 U_1\right) \bmod \varphi(19) = \left(7 - 5 \cdot 5\right) \bmod 18 = 0;$$
$$r_2(2) = \left(S_2^*(j) - d_2 S_2(j)\right) \bmod \varphi(19) = \left(4 - 5 \cdot 16\right) \bmod 18 = 14;$$
$$r_2(3) = \left(T_2^*(j) - d_2 T_2(j)\right) \bmod \varphi(19) = \left(24 - 5 \cdot 6\right) \bmod 18 = 12.$$

Найдем ответы на вопрос $d_3 = 4$. Получаем следующие ответы:

$$r_3(1) = \left(U_3^* - d_3 U_3\right) \bmod \varphi(29) = \left(16 - 4 \cdot 24\right) \bmod 28 = 4;$$
$$r_3(2) = \left(S_3^*(j) - d_3 S_3(j)\right) \bmod \varphi(29) = \left(13 - 4 \cdot 16\right) \bmod 28 = 5;$$
$$r_3(3) = \left(T_3^*(j) - d_3 T_3(j)\right) \bmod \varphi(29) = \left(4 - 4 \cdot 25\right) \bmod 28 = 6.$$

Истинный и зашумленный статусы, а также ответы на случайное число d пересылаются в запросчик. Запросчик проводит проверку статуса космического аппарата

$$A_1 = C_1^{d_1} g^{r_1(1)} g^{r_1(2)} g^{r_1(3)} \bmod m_1 = 2^2 \bmod 13 = 4;$$
$$A_2 = C_2^{d_2} g^{r_2(1)} g^{r_2(2)} g^{r_2(3)} \bmod m_2 = 2^{11} \bmod 19 = 15;$$
$$A_3 = C_3^{d_3} g^{r_3(1)} g^{r_3(2)} g^{r_3(3)} \bmod m_3 = 2^3 \bmod 29 = 8.$$

Так как значения $A_1 = C_1^* \bmod m_1 = 4$, $A_2 = C_2^* \bmod m_2 = 15$, $A_3 = C_3^* \bmod m_3 = 8$, то запросчик определяет, что космический аппарат «свой», и между спутником и объектом управления начинается обмен данными.

Проведенные исследования показали, что доказывают эффективность использования модулярного кода в рассмотренных протоколах аутентификации, базирующихся на доказательстве с нулевым разглашением данных. Известно, что скорость выполнения мультипликативных операций по модулю пропорциональна разрядности операндов. В рассмотренных примерах использование изоморфизма, порожденного китайской теоремой об остатках, позволило перейти от вычислений с 17 разрядными числами к вычислениям с 5 разрядными операндами. Таким образом, использование модулярного кода позволило повысить скорость проводимых вычислений более чем в 3 раза по сравнению с одномодульной реализацией протокола. Кроме того, полученные результаты наглядно свидетельствуют о том, что разработанный протокол определения статуса спутника, реализованный в модулярном коде, требует в 1,33 раза меньше временных затрат на аутентификацию по сравнению с протоколом Шнорра. Это связано с тем, что разработанный протокол аутентификации содержит меньшее число этапов, необходимых на выявление статуса спутника. Таким образом, разработанный протокол аутентификации, реализованный в модулярном коде, является наиболее перспективным для использования в системах опознавания «свой – чужой».

Заключение

В статье представлен разработанный протокол аутентификации, базирующийся на доказательстве с нулевым разглашением знаний, который реализуется с помощью модулярных кодов. Проведен сравнительный анализ разработанного протокола аутентификации с протоколом Шнорра, при использовании многомодульной реализации. Полученные результаты показали, что разработанный протокол определения статуса спутника, реализованный в модулярном коде, требует в 1,33 раза меньше временных затрат на аутентификации по сравнению с протоколом Шнорра. Полученные результаты свидетельствуют о целесообразности использования разработанного протокола аутентификации, реализованного в модулярном коде, в запросно-ответной системе распознавания спутника.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-37-50017.

Список литературы

1. Пашинцев В.П., Калмыков М.И., Ляхов А.В. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи // Инфокоммуникационные технологии. – 2015. – № 2. – С. 183–190.

2. Ananda Mohan Residue Number Systems. Theory and Applications // Springer International Publishing Switzerland. – 2016. – 351 p.

3. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. – М.: ФИЗМАТЛИТ, 2017. – 400 с.

4. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation // Imperial College Press. UK 2007. – 296 p.

5. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2007. – 320 с.

6. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009. – 272 с.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.

8. Калмыков М.И., Саркисов А.Б., Петрова Е.В. Способ построения системы опознавания «свой – чужой» на основе протокола с нулевым разглашением // Патент 2570700. 2015. Бюл. № 34.