УДК 004.94

Я. А. Калиновский, Ю. Е. Бояринова, А. С. Сукало
Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина

Построение алгоритма цифровой подписи с использованием функций от обобщенных кватернионов

Предложено использование гиперкомплексной числовой системы четвертой размерности — обобщеных кватернионов для построения алгоритма цифровой подписи.

Ключевые слова: *обощенные кватернионы, экспоненциальная функция, логарифмическая функция, цифровая подпись.*

Введение

Применение электронного документооборота все больше и больше входит в повседневную жизнь современного человека. Это существенно сокращает объемы бумажной документации, экономит время на оформление платежных документов, а также их пересылку. Документы могут быть подписаны электронной цифровой подписью (ЭЦП) и переданы по назначению в течение нескольких секунд. Конфиденциальность информации (невозможность доступа к ней лицам, у которых нет секретного ключа) обеспечивается благодаря надежным криптографическим преобразованиям [1].

При этом необходимо, чтобы применение ЭЦП без знания закрытого ключа было *вычислительно сложным процессом.* Обеспечение этого во всех асимметричных алгоритмах цифровой подписи опирается на следующие вычислительные задачи: 1) задачу дискретного логарифмирования (EGSA); 2) задачу факторизации, то есть разложения числа на простые множители (RSA) [2].

Алгоритм RSA относится к так называемым асимметричным алгоритмам, у которых ключ шифрования не совпадает с ключом дешифровки. Один из ключей доступен всем (так делается специально) и называется открытым ключом, другой хранится только у его хозяина и неизвестен никому другому. С помощью одного ключа можно производить операции только в одну сторону. Если сообщение зашифровано с помощью одного ключа, то расшифровать его можно только с помощью другого. Имея один из ключей, очень сложно найти другой ключ, если разрядность ключа высока.

Для повышения стойкости ЭЦП можно использовать либо увеличение длины ключа, либо иной способ представления данных. Одним из таких способов можно считать представление данных с помощью гиперкомплексных числовых систем (ГЧС). Применение гиперкомплексных числовых систем второй размерности в алгоритме RSA обеспечило большую устойчивость по сравнению с алгоритмом, основанным на действительных числах [3].

Целью работы является построение алгоритма цифровой подписи с использованием системы гиперкомплексных чисел четвертой размерности — обобщенных кватернионов.

Обычная схема алгоритма RSA

1. Шифрование — некоторый текст M шифруется с помощью открытого ключа (e, n) по формуле

$$C = E(M) = M^e \bmod n. \tag{1}$$

2. Расшифровки — с использованием закрытого ключа (d, n) по формуле

$$M = D(C) = C^d \bmod n. \tag{2}$$

Число *d* может быть вычислено с помощью расширенного алгоритма Евклида [4, 5]. Алгоритм Евклида также используется в поиске числа *e*.

Гиперкомплексная версия алгоритма RSA

Для использования гиперкомплексного представления данных в алгоритме RSA необходимо рассмотреть представление функций гиперкомплексной переменной [6]. То есть построить выражения (1) и (2) с использованием следующего свойства экспоненциальной функции:

$$a^x = \exp(x \cdot \ln a). \tag{3}$$

Таким образом, чтобы рассчитать алгоритм RSA следует построить представление функций от обобщенных кватернионов, в соответствии с (3). Это будут экспоненциальная и логарифмическая функции.

Построение некоммутативных гиперкомплексных числовых систем четвертой размерности

Рекуррентные процедуры удвоения ГЧС позволяют строить ряды ГЧС повышенной размерности. Существуют два типа процедур удвоения: процедура Кели-Диксона (КД-процедура) и процедура Грассмана Клиффорда (ГК-процедура).

КД-процедура позволяет строить вполне нормированные ГЧС размерности 2^n, где $n \in N$ — порядок удвоение [7–12]. При $n \geq 4$ получаются только неассоциативные ГЧС.

ГК-процедура позволяет получать ГЧС с более широкими возможностями как по размерности, так и по свойствам [7, 9, 13].

Введем следующие обозначения. В самом общем случае ГЧС будем обозначать так: $\Gamma(e,n)$, где $e = \{e_1,...,e_n\}$ — базис ГЧС, а n — ее размерность. В том случае, когда речь идет о ГЧС конкретного типа, она будет обозначаться именем своего типа как, например, система комплексных чисел $C(e)$. Здесь размерность можно не указывать, так как она известна из имени ГЧС. Но идентификатор базиса приводить надо, поскольку при удвоении могут рассматриваться два экземпляра ГЧС одного типа, но их базисы надо различать между собой.

Будем обозначать процесс удвоения системы $\Gamma_1(e,m)$ системой $\Gamma_2(f,2)$ с помощью некоммутативной КД-процедуры так:

$$Д(\Gamma_1(e,m),\Gamma_2(f,2)) = \Gamma_3(g,2m),$$

где $Д$ — оператор удвоения, а $2m$ — размерность полученной в результате удвоения ГЧС Γ_3 с базисом:

$$g = \{e_1f_1, e_1f_2, e_2f_1,..., e_mf_2\}.$$

Таблица Кели состоит из произведений элементов базиса, значения которых отражают свойства конкретной ГЧС.

Рассмотрим класс некоммутативных ГЧС четвертой размерности, состоящий из некоммутативных удвоений ГЧС второй размерности C, W и D с помощью КД-процедуры. Базис таких ГЧС состоит из четырех элементов:

$$g = \{g_1, g_2, g_3, g_4\} = \{e_1f_1, e_1f_2, e_2f_1, e_2f_2\}.$$

Первые два операнда в операторе удвоения не коммутируют. С учетом этого исследуемый класс ГЧС состоит из девяти ГЧС:

1. $Д(C, C, 4) = H$ — система кватернионов;
2. $Д(C, W, 4) = AH$ — система антикватернионов;
3. $Д(C, D, 4)$;
4. $Д(D, C, 4)$;
5. $Д(W, W, 4)$;
6. $Д(D, D, 4)$;
7. $Д(W, D, 4)$;
8. $Д(D, W, 4)$;
9. $Д(W, C, 4)$.

Таблицы Кели этих ГЧС приведены в табл. 1.

Таблица 1. Таблицы Кели гиперкомплексных числовых систем 4-й размерности

№	Обозначение	Таблица Кели
1.	$H = Д(C,C)$	H | e_1 | e_2 | e_3 | e_4 e_1 | e_1 | e_2 | e_3 | e_4 e_2 | e_2 | $-e_1$ | e_4 | $-e_3$ e_3 | e_3 | $-e_4$ | $-e_1$ | e_2 e_4 | e_4 | e_3 | $-e_2$ | $-e_1$
2.	$AH = Д(C,W)$	AH | e_1 | e_2 | e_3 | e_4 e_1 | e_1 | e_2 | e_3 | e_4 e_2 | e_2 | $-e_1$ | e_4 | $-e_3$ e_3 | e_3 | $-e_4$ | e_1 | $-e_2$ e_4 | e_4 | e_3 | e_2 | e_1
3.	$Д(C,D)$	$Д(C,D)$ | e_1 | e_2 | e_3 | e_4 e_1 | e_1 | e_2 | e_3 | e_4 e_2 | e_2 | $-e_1$ | e_4 | $-e_3$ e_3 | e_3 | $-e_4$ | 0 | 0 e_4 | e_4 | e_3 | 0 | 0
4.	$Д(W,C)$	$Д(W,C)$ | e_1 | e_2 | e_3 | e_4 e_1 | e_1 | e_2 | e_3 | e_4 e_2 | e_2 | e_1 | e_4 | e_3 e_3 | e_3 | $-e_4$ | $-e_1$ | e_2 e_4 | e_4 | $-e_3$ | $-e_2$ | e_1
5.	$Д(W,W)$	$Д(W,W)$ | e_1 | e_2 | e_3 | e_4 e_1 | e_1 | e_2 | e_3 | e_4 e_2 | e_2 | e_1 | e_4 | e_3 e_3 | e_3 | $-e_4$ | e_1 | $-e_2$ e_4 | e_4 | $-e_3$ | e_2 | $-e_1$

Продолжение табл. 1

6. $Д(W,D)$

$Д(W,D)$	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	e_1	e_4	e_3
e_3	e_3	$-e_4$	0	0
e_4	e_4	$-e_3$	0	0

7. $Д(D,C)$

$Д(D,C)$	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	0	e_4	0
e_3	e_3	$-e_4$	$-e_1$	e_2
e_4	e_4	0	$-e_2$	0

8. $Д(D,W)$

$Д(D,W)$	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	0	e_4	0
e_3	e_3	$-e_4$	e_1	$-e_2$
e_4	e_4	0	e_2	0

9. $Д(D,D)$

$Д(D,D)$	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	0	e_4	0
e_3	e_3	$-e_4$	0	0
e_4	e_4	0	0	0

Выполнение операций в некоммутативных гиперкомплексных числовых системах четвертой размерности

Будем обозначать числа в каждой из этих ГЧС в виде

$$w = a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4,$$

где $a_i \in R$. С этими числами можно производить все алгебраические действия, необходимые для построения математических моделей [14]: сложение, умножение, деление, нормирование и сопряжение. Формулы для выполнения этих операций определяются в зависимости от таблицы Кели рассматриваемой ГЧС. В табл. 2

приведены взятые из [15] формулы для определения псевдонорм, с помощью которых можно определять сопряжения и делители нуля.

Таблица 2. Псевдонорма

№	ГЧС	Псевдонорма
1.	H	$N(w)=a_1^2+a_2^2+a_3^2+a_4^2$
2.	AH	$N(w)=a_1^2+a_2^2-a_3^2-a_4^2$
3.	$Д(C,D)$	$N(w)=a_1^2+a_2^2$
4.	$Д(W,C)$	$N(w)=a_1^2-a_2^2+a_3^2-a_4^2$
5.	$Д(W,W)$	$N(w)=a_1^2-a_2^2-a_3^2+a_4^2$
6.	$Д(W,D)$	$N(w)=a_1^2-a_2^2$
7.	$Д(D,C)$	$N(w)=a_1^2+a_3^2$
8.	$Д(D,W)$	$N(w)=a_1^2-a_3^2$
9.	$Д(D,D)$	$N(w)=a_1^2$

Введенные таким образом алгебраические процедуры позволяют строить представления экспоненциальной функции [14].

Представление экспоненты $Exp(M)$ от гиперкомплексного числа M в ГЧС $Г(e,n)$ есть частное решение гиперкомплексного линейного уравнения с правой частью

$$\frac{dX}{dt}=MX$$

с начальным условием

$$Exp(0)=e_1.$$

Представления экспоненты для всех вышерассмотренных ГЧС приведены в табл. 3.

Таблица 3. Представления экспоненты

№	ГЧС	Представления
1.	H	$Exp(M)=e^{m_1}\left(\cos\overline{m}\cdot e_1+\frac{(m_2e_2+m_3e_3+m_4e_4)}{\overline{m}}sh\overline{m}\right),\ \overline{m}=\sqrt{m_2^2+m_3^2+m_4^2}$
2.	AH	$Exp(M)=e^{m_1}\left(ch\overline{m}\cdot e_1+\frac{(m_2e_2+m_3e_3+m_4e_4)}{\overline{m}\cdot}sh\overline{m}\right),\ \overline{m}=\sqrt{\left\|-m_2^2+m_3^2+m_4^2\right\|}$
3.	$Д(C,D)$	$Exp(M)=e^{m_1}\left(\cos\lvert m_2\rvert e_1+\frac{\sin\lvert m_2\rvert}{\lvert m_2\rvert}(m_2e_2+m_3e_3+m_4e_4)\right)$

Продолжение табл. 3

4.	$Д(W,C)$	$Exp(M)=e^{m_1}\left(ch\overline{m}\cdot e_1+\frac{(m_2e_2+m_3e_3+m_4e_4)}{\overline{m}\cdot}sh\overline{m}\right),\ \overline{m}=\sqrt{\lvert m_2^{\,2}-m_3^{\,2}+m_4^{\,2}\rvert}$
5.	$Д(W,W)$	$Exp(M)=e^{m_1}\left(ch\overline{m}\cdot e_1+\frac{(m_2e_2+m_3e_3+m_4e_4)}{\overline{m}\cdot}sh\overline{m}\right),\ \overline{m}=\sqrt{\lvert m_2^{\,2}+m_3^{\,2}-m_4^{\,2}\rvert}$
6.	$Д(W,D)$	$Exp(M)=e^{m_1}\left(ch\lvert m_2\rvert e_1+\frac{sh\lvert m_2\rvert}{\lvert m_2\rvert}(m_2e_2+m_3e_3+m_4e_4)\right)$
7.	$Д(D,C)$	$Exp(M)=e^{m_1}\left(\cos\lvert m_3\rvert e_1+\frac{\sin\lvert m_3\rvert}{\lvert m_3\rvert}(m_2e_2+m_3e_3+m_4e_4)\right)$
8.	$Д(D,W)$	$Exp(M)=e^{m_1}\left(\cos\lvert m_3\rvert e_1+\frac{\sin\lvert m_3\rvert}{\lvert m_3\rvert}(m_2e_2+m_3e_3+m_4e_4)\right)$
9.	$Д(D,D)$	$Exp(M)=e^{m_1}(e_1+m_2e_2+m_3e_3+m_4e_4)$

Представления логарифмической функции могут быть построены, как показано в работах [16, 17], обращением экспоненциальных функций. Так, например, в работе [16] показано, что главное значение логарифмической функции $Ln_{\Gamma}(X)$ от кватерниона $X=x_1e_1+x_2e_2+x_3e_3+x_4e_4$ имеет представление:

$$Ln_{\Gamma}(X)=\ln\lvert X\rvert+\frac{1}{x}\arccos\frac{q_1}{\lvert X\rvert}(x_2e_2+x_3e_3+x_4e_4)$$

Выводы

В работе на основе исследования современного состояния теории гиперкомплексных числовых систем показана возможность построения алгоритма цифровой подписи с использованием экспоненциальной и логарифмической функций от обобщенных кватернионов.

1. *Stinson D.R.* Cryptography: Theory and Practice / D. R. Stinson. — Chapman and Hall, 2006.

2. *Bakhtiari M.* Serious Security Weakness in RSA Cryptosystem / M. Bakhtiari, M.A. Maarof // IJCSI International Journal of Computer Science. — January 2012. — Vol. 9, N 3. — Issue 1.

3. *Kalinovsky Y.O.* Applying of hypercomplex number systems to RSA-algorithms / Y.O. Kalinovsky, Y.E. Boyarinova, I.V. Khitsko / Proc. of the 6-th International Conf. «Advanced Computer Systems and Networks: Design and Application» ACSN-2013. — Львів: НВФ «Українські технології». — 2013. — P. 114–115.

4. *Ноден П.* Алгебраическая алгоритмика с упражнениями и решениями / П. Ноден, К. Китте. — М.: Мир, 1999. — 720 с

5. *Бояринова Ю.Е.* Восстановление информации в задаче разделения секрета для гиперкомплексных числовых систем 2-го порядка с помощью алгоритма Евклида / Ю.Е. Бояринова, Я.В. Одарич // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 1. — С. 103–114.

6. *Гіперкомплексні* числові системи: основи теорії, практичні використання, бібліографія / Синьков М.В., Боярінова Ю.Є., Каліновський Я.О. [та ін.]. — К.: ІПРІ НАН України, 2009. — 44 с. — (Препринт / НАН України, Ін-т пробл. реєстрації інформації).

7. *Кантор И.Л.* Гиперкомплексные числа / И.Л. Кантор, А.С. Солодовников. — М.: Наука, 1973. — 144 с.

8. *Chaitin-Chatelin F.* Computation with Hypercomplex Numbers / F. Chaitin-Chatelin, T. Meskauskas, A. Zaoui // GERFACS Technical Report TR/PA/00/69. — On line: http://www.gerfacs.fr (2000).

9. *Сильвестров В.В.* Системы чисел / В.В. Сильвестров // Соросовский образовательный журнал. — 1998. — № 8. — С. 121–127.

10. *Baez J.C.* The Octonions / J.C. Baez. — On line: http://math/ucr.edu/home/baez/Octonions/octonions.html (2001).

11. *Chaitin-Chatelen F.* Geometry and Algebra. CERFACS Technical Report TR/PA/00/74 / F. Chaitin-Chatelen, T. Meskauskas, A. Zaoui. — On line: http://www.cerfacs.fr/algor/reports/2000/TR-PA-00-74.ps.gz (2000).

12. *Chaitin-Chatelen F.* The computing power of Geometry. CERFACS Technical Report TR/PA/99/74 / F. Chaitin-Chatelen. — On line: http://www.cerfacs.fr/algor/reports/ 2000/ TR-PA-99-74.ps.gz (1999).

13. *Калиновский Я.А.* Высокоразмерные изоморфные гиперкомплексные числовые системы и их использование для повышения эффективности вычислений / Я.А. Калиновский, Ю.Е. Бояринова. — К.: Инфодрук, 2012. — 183 с.

14. *Синьков М.В.* Конечномерные гиперкомплексные числовые системы. Основы теории. Применения / М.В. Синьков, Ю.Е. Бояринова, Я.А. Калиновский. — К.: Инфодрук, 2010. — 388 с.

15. *Computing* Characteristics of One Class of Non-commutative Hypercomplex Number Systems of 4-dimension. [Электронный ресурс] / Y.O. Kalinovsky, D.V. Lande, Y.E. Boyarinova, A.S. Turenko. — Режим доступа: http://arxiv.org/ftp/arxiv/papers/1409/1409.3193.pdf

16. *Каліновський Я.О.* Розробка та дослідження алгоритмів побудови зображення обернених функцій від гіперкомплексного змінного / Я.О. Каліновський, М.В. Синьков, Ю.Є. Боярінова // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 1. — С. 32–42.

17. *Синьков М.В.* Логарифмическая функция от кватерниона / М.В. Синьков, Я.А. Калиновский, Т.Г. Постникова, Т.В. Синькова // Реєстрація, зберігання і оброб. даних. — 2002. — Т. 4, № 1. — С. 35–37.

18. *Калиновский Я.А.* Исследование свойств изоморфизма квадриплексных и бикомплексных числовых систем / Я.А. Калиновский // Реєстрація, зберігання і оброб. даних. — 2003. — Т. 5, № 1. — С. 69–73.

Поступила в редакцию 03.09.2015