СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУММАТОРОВ ДВОИЧНО-ДЕСЯТИЧНЫХ ЧИСЕЛ ПРИ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Сахыбай Тынымбаев[1], Евгения Айтхожаева[1], Гульнур Жангисина[1], Владимир Щербина[2]

[1]Казахский национальный технический университет им. К.И. Сатпаева, Казахстан
[2]Национальный авиационный университет, Украина

ТЫНЫМБАЕВ Сахыбай, к.т.н., профессор

Год и место рождения: 1939 год, г. Туркестан, Казахстан.
Образование: КазПТИ 1964 год.
Должность: профессор кафедры «Вычислительная техника».
Научные интересы: проектирование цифровых систем, новые аппаратные архитектуры, аппаратные средства защиты информации, информационные технологии в обучении.
Публикации: более 100 публикаций, среди них 8 учебников и учебных пособий.
E-mail: ait_evg@mail.ru

АЙТХОЖАЕВА Евгения Жамалхановна, к.т.н., профессор

Год и место рождения: 1947 год, Южно-Казахстанская область, Казахстан.
Образование: КазПТИ 1969 год.
Должность: профессор кафедры «Вычислительная техника».
Научные интересы: защита и безопасность информации, методы и средства проектирования и защиты цифровых устройств и баз данных, новые аппаратные архитектуры, информационные технологии в обучении.
Публикации: более 130 публикаций, среди них 1 изобретение, 3 учебника, 14 учебных пособий.
E-mail: ait_evg@mail.ru

ЖАНГИСИНА Гульнур Давлетжановна, д.п.н., профессор

Год и место рождения: 1958 год, г. Алматы, Казахстан.
Образование: КазНУ имени Аль-Фараби, 1980 год.
Должность: заведующая кафедрой «Информационная безопасность».
Научные интересы: информационная безопасность, компьютерная безопасность, параллельные вычисления, информационные системы и дистанционное образование.
Публикации: более 300 публикаций, среди них 4 монографии, более 20 учебных пособий, 200 научных статей.
E-mail: gul_zhd@mail.ru

ЩЕРБИНА Владимир Порфирьевич, доцент

Год и место рождения: 1950 год, г. Магдебург, Германия.
Образование: Киевский государственный университет им. Т.Г. Шевченко
Должность: доцент кафедры безопасности информационных технологий.
Научные интересы: информационная безопасность, криптографические методы защиты информации.
Публикации: 42 научные статьи, научно-методические работы.
E-mail: smya@nau.edu.ua

Аннотация. *Эксплуатация информационных систем сейчас невозможна без применения современных средств и методов защиты информации, среди которых основная роль в обеспечении безопасности традиционно отводится криптографии. Большинство систем шифрования данных, а также систем цифровой подписи используют целочисленную арифметику по модулю большого положительного числа. Поэтому для обеспечения лучшей производительности систем защиты информации необходимы*

эффективные методы реализации операций перемножения и возведения в степень для чисел большой разрядности. Высокую производительность, простоту, защищенность, надежность можно обеспечить при аппаратной реализации криптографических алгоритмов с использованием сумматоров двоично-десятичных чисел. В статье проводится сравнительный анализ существующих сумматоров двоично-десятичных чисел. Выявляются различные варианты построения и проводится оценка сумматоров двоично-десятичных чисел по быстродействию и сложности реализации.

Ключевые слова: *криптографические алгоритмы, двоично-десятичные сумматоры, сложность, общая задержка, эффективный способ, криптография.*

Вступление

Эксплуатация информационных систем сейчас невозможна без применения современных средств и методов защиты информации, среди которых основная роль в обеспечении безопасности традиционно отводится криптографии. Постоянный рост объемов информации, которую следует защищать, предъявляет жесткие требования к криптографическим методам защиты. Главными, из которых, являются обеспечение стойкости ко всем известных методов криптоанализа и высокой скорости обработки данных.

Большинство систем шифрования данных, а также систем цифровой подписи используют целочисленную арифметику по модулю m, где m — очень большое положительное натуральное чисто (например, в RSA, Rabin или Эль Гамале используются числа имеющие порядки 10^{309}). Поэтому необходимы эффективные методы реализации операций перемножения и возведения в степень для чисел большой разрядности для обеспечения лучшей производительности систем защиты информации. Высокую производительность, простоту, защищенность, надежность можно обеспечить при аппаратной реализации криптографических алгоритмов с использованием сумматоров двоично-десятичных чисел (ДДС). Существует большое количество таких сумматоров, поэтому актуальной является задача сравнительного анализа их эффективности, для последующего использования при аппаратной реализации криптографических алгоритмов.

Целью работы есть сравнительный анализ сумматоров двоично-десятичных чисел для реализации криптографических алгоритмов.

В статье проводится анализ существующих сумматоров ДДС. Выявляются различные варианты построения, и проводится их оценка. Для этого вводится понятие сложности и быстродействия сумматоров. При этом под сложностью (N) понимается суммарное число входов логических схем, на базе которых строятся ДДС. Под быстродействием понимается суммарная задержка (T) входных сигналов на логических элементах И-НЕ, ИЛИ-НЕ, НЕ. Для интегральной оценки ДДС используется произведение N*T и вводится понятие коэффициента эффективности, который позволяет сравнивать различные варианты ДДС и определить эффективный вариант построения ДДС.

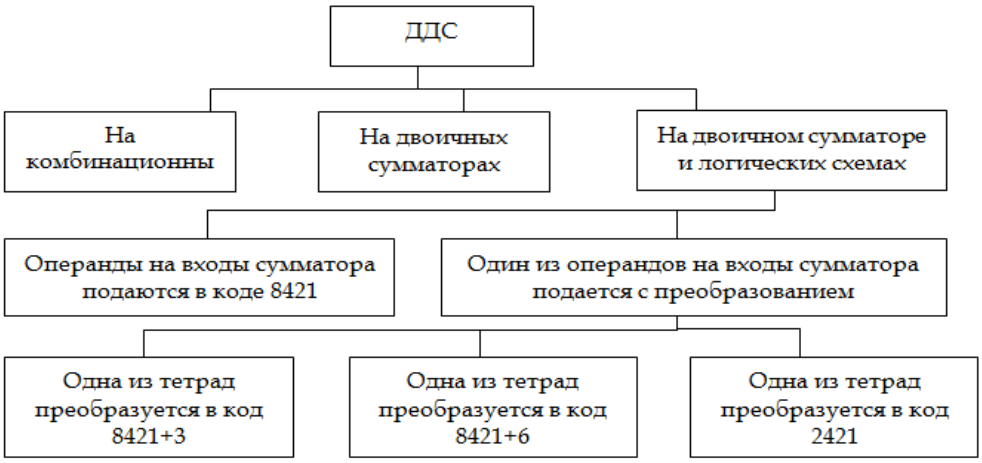

Рис. 1. Классификация ДДС

При сложении двух тетрад двоично-десятичных чисел $A_8A_4A_2A_1$ и $B_8B_4B_2B_1$ с учетом переноса из младшей тетрады (Свх) на первом этапе они суммируются на четырехразрядном сумматоре (SMA). При этом на выходах сумматора SMA формируется нескорректированная сумма $S_8S_4S_2S_1$ и нескорректированный импульс переноса C_{16}. Затем полученная сумма корректируется для получения скорректированной суммы $S_8' S_4' S_2' S_1'$ и десятичного переноса C_{10}. Сигнал для выработки коррекции формировался, как правило, на логических элементах, образующих схему выработки сигнала коррекции (СВК). В ранних разработках для коррекции суммы $S_8S_4S_2S_1$ использовались двоичные сумматоры (SMB). Такие ДДС были медленно-действующими. Для увеличения быстродействия в последующих разработках двоичный сумматор SMB коррекции суммы заменили простыми логическими схемами. При этом, для упрощения цепей коррекции, тетрады слагаемых вступали в операцию в коде прямого замещения 8421 или в других кодах: 8421+3, 8421+6, 2421 и т.д. На рис. 1 приведена

классификация ДДС, учитывающая все основные подходы в построении ДДС.

Рассмотрим сравнительную оценку различных вариантов построения ДДС по сложности и быстродействию.

При построении ДДС с использованием двух сумматоров SMA и SMB и схеме выработки сигнала коррекции (СВК) переносы в сумматорах могут быть организованы параллельно (обозначим такие сумматоры SMA1 и SMB1), последовательно (SMA2, SMB2), параллельно-последовательно (SMA3, SMB3) [1].

Ниже в табл. 1 приведены значения N и T для SMA и SMB при различных способах организации переносов в них. Для чего были построены функциональные схемы сумматоров в базисе Шеффера.

Таблица 1

Параметры сумматоров SMA и SMB при различных способах организации переносов

Основной сумматор SMA	N (вх)	T (Тл.э)	Сумматор коррекции SMB	N (вх)	T (Тл.э)
SMA1	128	5	SMB 1	86	5
SMA2	100	16	SMB2	75	12
SMA3	106	10	SMB3	78	9

В базисе Шеффера сигнал коррекции (К) определяется по следующей формуле:

$$K = \overline{\overline{S_4 S_8}\,\overline{S_8 S_2}\,\overline{C_{16}}}\,.$$

Из этой формулы видно, что $N_{СВК}=8_{вх}$, $T_{СВК}=2$Тл.э;

Комбинируя каждый тип сумматора SMA (SMA1, SMA2, SMA3) с каждым типом сумматора SMB (SMB1, SMB2, SMB3) получим девять типов ДДС: ДДС1÷ДДС9.

ДДС1 строится на основе сумматоров SMA1 и SMB1; ДДС2 – на основе SMA1 и SMB2 и т.д. В табл. 2 приводятся значения N и T для сумматоров ДДС1÷ДДС9:

$$N= N_{SMA}+ N_{SMB}+ N_{СВК}\,;\; T= T_{SMA}+ T_{SMB}+ T_{СВК}.$$

Таблица 2

Значения N и T для сумматоров ДДС1÷ДДС9

ДДС	$N_{ДДСi}$	$T_{ДДСi}$
ДДС1	128+86+8 = 222 вх	5+5+2 =12 Тл.э
ДДС2	128+75+8=211 вх	5+12+2=19 Тл.э
ДДС3	128+78+8=214 вх	5+9+2=16 Тл.э
ДДС4	100+86+8=194 вх	12+5+2=19 Тл.э
ДДС5	100+75+8=183 вх	12+12+2=26 Тл.э
ДДС6	100+78+8=186 вх	12+9+2=23 Тл.э
ДДС7	106+86+8=200 вх	9+5+2=16 Тл.э
ДДС8	106+75+8=189 вх	9+12+2=23 Тл.э
ДДС9	106+78+8=192 вх	9+9+2=20 Тл.э

В ДДС на базе двоичного сумматоров и логических схем непосредственное сложение кодов осуществляется на двоичном сумматоре SMA, а преобразование входных кодов и коррекция результата производится на логических схемах.

ДДС на комбинационных схемах приведен в [2]. На этой схеме выходной сигнал формируется проходя через 12 логических схем, т.е. $T_{комб}=12\tau_{л.э.}$

Количество входов логических схем составляет $N_{комб}$= 132 входа. ДДС реализован в виде микросхемы на КМОП-транзисторах.

Рассмотрим ДДС, где операнды поступают на входы сумматора SMA в коде 8421 и ДДС, где один из операндов поступает в коде 8421+3, 8421+6, в коде 2421. Определим N и T для входных преобразователей кодов схемы коррекций суммы (СКС).

Схема ДДС, предложенная Гайтоном [3], состоит из преобразователя одной тетрады из кода 8421 в код 8421+6, сумматора SMA, а так же схемы коррекции суммы, где двоичный код нескорректированной суммы $S_8S_4S_2S_1$ преобразуется в двоично-десятичный код окончательной суммы S_8' S_4' S_2' S_1'.

В ДДС Гайтона преобразователь кода (Пр) тетрады 8421 в код 8421+6 функционирует согласно следующим формулам, в которых X_8, X_4, X_2, X_1, - выходы преобразователя:

$$\begin{cases} X_8 = B_8 \vee B_4 \vee B_2 = \overline{\overline{B_8}\,\overline{B_4}\,\overline{B_2}}; \\ X_4 = B_4B_2 \vee \overline{B_4}\,\overline{B_2} = \overline{\overline{B_4B_2}\,\vee\,\overline{B_4}\,\overline{B_2}}; \\ X_2 = \overline{B_2}; \\ X_1 = B_1. \end{cases} \qquad (1)$$

Схема коррекции суммы функционирует согласно следующим формулам:

$$\begin{cases} S_8^{'} = \overline{\overline{S_8}\,\overline{S_4}\,\overline{S_8}\,\overline{S_4}\,\overline{S_2}}; \\ S_8 = \overline{\overline{C_0}\,\overline{S_4}\,\overline{S_2}\,\overline{S_4}\,\overline{C_0}\,\overline{S_2}\,\overline{S_4}}; \\ S_2 = \overline{\overline{C_0}\,\overline{S_2}\,\overline{C_0}\,\overline{S_2}}; \\ S_1^{'} = S_1. \end{cases} \qquad (2)$$

Согласно формул (1), (3) с учетом получения значений $\overline{B_2}, \overline{B_4}, \overline{B_2}$:

$N_{пр}$ =12вх, $T_{пр}$=3Тл.э, а так же $N_{скс}$=26вх и $T_{скс}$=3Тл.э.

Составив аналогичные формулы для ДДС, использующего преобразователь одного из операндов из кода 8421 в код 8421+6, получим:

$N_{пр}$ =27вх, $T_{пр}$=3Тл.э, $N_{скс}$=27вх и $T_{скс}$=3Тл.э.

Для ДДС, где один из операндов вступает в операцию в коде 2421, получены следующие оценки для преобразователя кодов и схемы коррекции суммы:

$N_{пр}$ =25вх, $T_{пр}$=3Тл.э, $N_{скс}$=32вх и $T_{скс}$=3Тл.э.

В работе [4] приведена схема ДДС, где сигналы подаются непосредственно в кодах 8421. Выходы двоичного сумматора SMA поступают на входы схемы коррекции суммы.

Функционирование СКС описывается формулами:

$$\begin{aligned} C_0 &= \overline{\overline{C_{16}S_8}\overline{S_4S_8}\overline{S_2}}; \\ S_8' &= \overline{\overline{C_{16}S_2}\overline{S_8}\overline{S_4}\overline{S_2}}; \\ S_4' &= \overline{\overline{C_{16}}\overline{S_2}\overline{S_4S_2}\overline{S_8}\overline{S_4}}; \\ S_2 &= \overline{S_{16}\overline{S_2}S_8S_4\overline{S_2}\overline{C_{16}S_8}S_2}; \\ S_1' &= S_1. \end{aligned} \qquad (3)$$

Из формулы (3) с учетом затрат для получения значения $\overline{S_2}, \overline{S_4}, \overline{S_8}, \overline{C_{16}}$ подсчитаем: $N_{СКС}$ =32вх, $T_{СКС}$=2Тл.э.

В любом из рассмотренных выше ДДС один из операндов вступает в операцию в коде 8421. Учитывая возможность использования различных типов сумматора SMA, отличающихся способом организации переноса (SMA1, SMA2, SMA3) и различных кодов для одного из операндов (8421+3, 8421+6, 2421, 8421), получаем различные варианты ДДС (ДДС10÷ДДС21), дополнительно к уже имеющимся ДДС1÷ДДС9 (см. табл. 1).

Следует отметить, что ДДС Агравала не рассматривается, поскольку при значениях суммы кодов на выходах сумматора от 16 до 19 схема работает некорректно.

Для каждого из вариантов ДДС10÷ДДС21 можно подсчитать сложность $N= N_{SMA}+ N_{ПР}+ N_{СКС}$ и быстродействие $T= T_{SMA}+ T_{ПР}+ T_{СКС}$, используя различные значения N_{SMA} и T_{SMA} (см. табл.1) для различных типов сумматоров. Для ДДС19÷ДДС21 $N_{ПР}=0$ и $T_{ПР}=0$ в связи с отсутствием преобразователя кодов.

Для сравнительной оценки различных вариантов построения ДДС, для каждого из них, вычислим коэффициент эффективности значения:

$$Q = \frac{N_б T_б}{N_x T_x};$$

где $N_б*T_б$ – интегральный параметр базового ДДС и N_x*T_x – интегральный параметр сравниваемого ДДС. В качестве базового ДДС выберем ДДС, у которого N и T является максимальным. Эффективным будем считать тот ДДС, у которого Q является максимальным.

В табл. 3 и табл. 4 приведены параметры N,T, N*T и Q для различных вариантов построения ДДС1÷ДДС21. В качестве базового ДДС выберем ДДС5, у которого N*T=4758.

Таблица 3

Параметры N, T и Q для ДДС1÷ДДС10

Параметры	ДДС1	ДДС2	ДДС3	ДДС4	ДДС5	ДДС6	ДДС7	ДДС8	ДДС9	ДДС10
N	222	211	214	194	183	186	200	189	192	166
T	12	19	16	19	26	23	16	23	20	11
NT	2664	4009	3424	3686	4758	4278	3232	4347	3840	1848
Q	1,78	1,18	1,38	1,29	1	1,1	1,47	1,09	1,23	2,57

Таблица 4

Параметры N, T и Q для ДДС11÷ДДС21

Параметры	ДДС 11	ДДС 12	ДДС 13	ДДС 14	ДДС 15	ДДС 16	ДДС 17	ДДС 18	ДДС 19	ДДС 20	ДДС 21
N	138	144	182	154	160	185	157	163	160	132	138
T	18	15	11	18	15	11	18	15	7	14	11
NT	2484	2160	2002	2772	2400	2035	2826	2445	1120	1848	1518
Q	1,9	2,2	2,3	1,7	1,98	2,3	1,68	1,9	4,2	2,5	3,1

ДДС, построенный полностью на комбинационных схемах, имеет следующие параметры: $N_{комб}*T_{комб}$=1200*12=1584. В этом случае: $Q_{комб}$=4758 :1584=3,9.

Из табл. 3 и 4 видно, что самым эффективным (Q=4,2) является ДДС19, в котором используется код 8421 для обоих операндов. В качестве сумматора SMA в ДДС19 служит двоичный сумматор с параллельным переносом (SMA1), а в качестве схемы коррекции суммы служит преобразователь двоичного кода в двоично-десятичный код. Функциональная схема двоично-десятичного сумматора ДДС19 приведена в [4].

Выводы

В работе проведен сравнительный анализ сумматоров двоично-десятичных чисел по критериям: сложности (суммарное число входов логических схем), быстродействию (суммарная задержка входных сигналов на логических элементах И-НЕ, ИЛИ-НЕ, НЕ), эффективности (отношения интегрального параметра базового ДДС к интегральному параметру сравниваемого ДДС). Результаты работы могут быть использованы при аппаратной реализации криптографических алгоритмов с заданными ограничениями по сложности и быстродействию.

Литература

[1] Угрюмов Е.П. Цифровая схемотехника. 2-ое издание. — СПб.: БХВ-Петербург 2005. — 800 с.

[2] Компьютеры: Справочное руководство под редакцией Г.Хелмса. — М.: Мир, 1986. — 416 с.

[3] Гайтон Р.Д. Упрощение операции сложения двух двоично-десятичных чисел. — Электроника №11. — 1974 г.

[4] Тынымбаев С., Махпунова Н. Синтез быстродействующих сумматоров для двоично-десятичных кодов. Труды международной научной конференций «Высокие технологии – залог устойчивого развития». — Алматы: КазНТУ им. Сатпаева 2011. — 434 с.

УДК 681.3 (045)

Тинимбаєв С., Айтхожаєва Е.Ж., Жангісіна Г.Д., Щербина В.П. Порівняльний аналіз суматорів двійково-десяткових чисел при реалізації криптографічних алгоритів

Анотація. *Сьогодні експлуатація інформаційних систем неможлива без застосування сучасних засобів і методів захисту інформації, серед яких основна роль в забезпеченні безпеки традиційно відводиться криптографії. Більшість систем шифрування даних, а також систем цифрового підпису використовують цілочислову арифметику за модулем великого позитивного числа. З огляду на це, для забезпечення кращої продуктивності систем захисту інформації необхідні ефективні методи реалізації операцій множення і зведення до ступеня для чисел великої розрядності. Високу продуктивність, простоту, захищеність, надійність можна забезпечити при апаратній реалізації криптографічних алгоритмів з використанням суматорів двійково-десяткових чисел. У статті проводиться порівняльний аналіз існуючих суматорів двійково-десяткових чисел. Виявляються різні варіанти побудови і проводиться оцінка суматорів двійково-десяткових чисел за швидкодією та складністю реалізації.*

Ключові слова: *криптографічні алгоритми, двійково-десяткові суматори, складність, загальна затримка, ефективний спосіб, криптографія.*

Tinimbaev S., Aytkhozhaeva E.Zh, Zhangissina G.D., Scherbyna V.P. Comparative analysis of binary-decimal numbers summers on cryptography algorithms realizations

Abstract. *Nowadays the maintenance of information systems without modern information security methods and means is impossible. Among them the primary role for security providing is assigned to cryptography. Most of encryption systems and digital signature systems use integer arithmetic modulo a large positive number. Therefore, to ensure the best performance of information security systems need effective methods of implementation of operations and multiply exponentiation for a large number of precision. High performance, simplicity, security and reliability can be achieved by hardware implementations of cryptographic algorithms using binary-decimal numbers summers. In the paper thecomparative analysis of existing binary-decimal numbers summers is carried out. Different variants of its making are identifying and binary-decimal numbers summers' speed and complexity of implementation are estimating.*

Key words: *cryptographic algorithms, binary-decimal summers, complexity, total delay, effective method, cryptography.*

Отримано *01 вересня 2013 року*, затверджено редколегією *17 жовтня 2013 року*