УДК 004.056.55 https://doi.org/10.51301/vest.su.2021.i3.23

[1]Е.Ж. Айтхожаева, [2]С. Тынымбаев, [2]А.К. Мукашева, [2]Р.Ш. Бердибаев, [1]С. Әділбеккызы*
[1]Satbayev University, Алматы, Казахстан
[2]Алматинский университет энергетики и связи имени Г. Даукеева, Алматы, Казахстан
*e-mail: sairan.02.95@mail.ru

БЫСТРОДЕЙСТВУЮЩЕЕ УСТРОЙСТВО ПРИВЕДЕНИЯ ЧИСЕЛ ПО МОДУЛЮ С ИСПОЛЬЗОВАНИЕМ КРАТНЫХ МОДУЛЯ

Аннотация. Рассматривается аппаратная реализация быстродействующего устройства приведения чисел по модулю. Использован модифицированный алгоритм деления со сдвигом делимого, где на каждом шаге участвуют n+3 старших разрядов сначала делимого, а затем получаемых остатков. Сдвиг приводимого числа на каждом шаге на три разряда влево в сторону старших разрядов позволяет ускорить процесс приведения по модулю за счет уменьшения количества шагов приведения по модулю. Основным блоком устройства является блок формирователей частичных остатков, в которых используется вычитание модуля P и кратных модуля P. Для сокращения аппаратных затрат и получения большего быстродействия в ФЧО для определения вычитаемых кратных модуля применены схемы сравнения, что позволяет минимизировать число сумматоров.

Ключевые слова: приведение по модулю, кратные модуля, формирователь частичных остатков

Введение. Разработка быстродействующих операционных блоков аппаратных криптопроцессоров для ассиметричного шифрования является актуальной задачей, несмотря на их высокую стоимость. Аппаратная реализация любых криптографических систем является лучшим решением по сравнению с программной реализацией этих же систем. Ниже приведены основные объясняющие причины [1]:

- аппаратные криптопроцессоры характеризуются более высокой производительностью, так как аппаратная реализация криптографических алгоритмов, как и любых других алгоритмов, обеспечивает лучшее быстродействие, чем программная реализация. При этом повышается и производительность центрального процессора компьютера, который не тратит свои ресурсы на криптографические преобразования;

защитить аппаратные устройства всегда гораздо проще от проникновения извне, чем программы, аппаратная реализация криптоалгоритма гарантирует его целостность;

- шифрование и хранение ключей осуществляются не в оперативной памяти компьютера (передатчика информации), в которую могут проникнуть злоумышленники, а в самой плате шифратора.

Этот перечень далеко не полный, поэтому предпочтительнее реализовывать средства криптографической защиты информации в виде специализированных аппаратных процессоров. Эти процессоры встраиваются в линию связи. Вся передаваемая по линии связи информация будет проходить через криптопроцессор, который выполняет шифрование. Таким образом, на выходе криптопроцессора будет зашифрованная информация, которая подлежит передаче по линии связи.

Низкое быстродействие асимметричных систем по сравнению с симметричными системами сужает их область применения, несмотря на такое преимущество, как отсутствие необходимости передачи секретного ключа. Низкое быстродействие – это следствие необходимости выполнения сложных операций. Одним из решений этой проблемы является является разработка методов ускорения базовых операций асимметричных криптоалгоритмов. При этом наиболее критичной по времени и наименее разработанной базовой операцией является операция приведения по модулю. При аппаратной реализации приведения по модулю для увеличения быстродействия можно использовать различные теоретико-числовые методы вычисления остатка при делении на модуль P, что приводит к различным структурам устройств [2÷13].

Основная часть. На рисунке 1 приведена структурная схема устройства, реализующего данный подход. Используется модифицированный алгоритм деления со сдвигом делимого, где на каждом шаге участвуют n+3 старших разрядов сначала делимого, а затем получаемых остатков. В состав устройства входит (2n+3)-разрядный сдвигающий регистр на три разряда влево РгА (2n разрядов основных, 3 разряда дополнительных), блок формирования кратных модуля Р, формирователь частичных остатков (ФЧО), блок синхронизации Бл.СИНХ, в состав которого входит вычитающий счетчик СчТИ. На входы Бл.СИНХ подается сигнал «ПУСК», тактовый сигнал ТИ, двоичный код числа сдвигов K=n/3, где n разрядность модуля.

Устройство работает следующим образом. По сигналу «ПУСК» приводимое 2n-разрядное число принимается в старшие разряды регистра РгА, а n-разрядный модуль Р принимается в блок формирования кратных модуля Р, где вырабатываются Р÷7Р и $\overline{Р}$÷7$\overline{Р}$, в счетчик записывается код К. Содержимое старших n разрядов РгА представляет собой начальный остаток R_0.

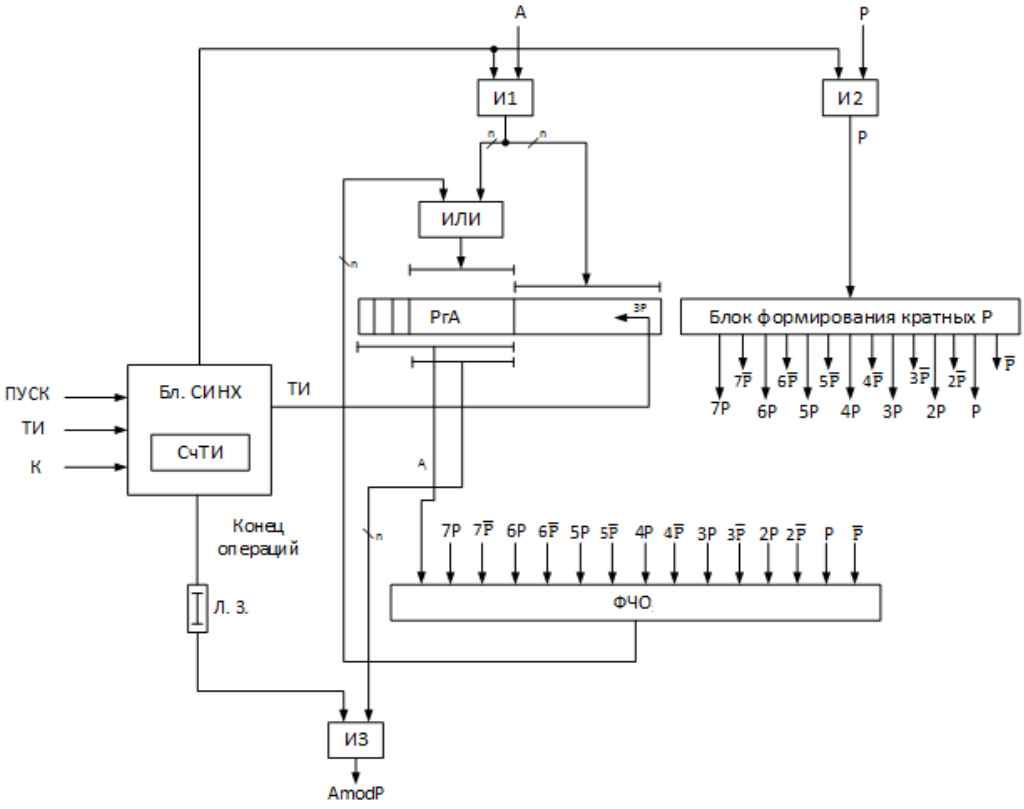

Рисунок 1. Структурная схема устройства приведения числа по модулю со сдвигом приводимого числа на три разряда за такт

После приема операндов с выхода Бл.СИНХ на вход сдвига РгА подается первый тактовый импульс ТИ1, который сдвигает на три разряда содержимое регистра РгА. И в старших n+3 разрядах РгА формируется значение $A_1=8R_0+a_{n-1}a_{n-2}a_{n-3}$, которое передается на входы ФЧО. На другие входы передаются значения кратных модуля Р÷7Р и $\overline{Р}$÷7$\overline{Р}$. На выходах ФЧО формируется остаток R_1, который передается через схему ИЛИ в старшие основные разряды регистра РгА.

К моменту окончания формирования частичного остатка R_1 из Бл.СИНХ поступает тактовый импульс ТИ2, который сдвигает содержимое регистра РгА на три разряда влево, формируя значение A_2, которое подается на входы ФЧО и на выходе формируется частичный остаток R_2. С приходом каждого тактового импульса формируется A_i и выполняется формирование очередного остатка R_i.

После поступления каждого ТИ показания счетчика СчТИ уменьшается на единицу. При СчТИ=0 Бл.СИНХ вырабатывает сигнал «Конец операции», который задерживается на элементе задержки Л.З. на время записи последнего частичного остатка РгА. Этот частичный остаток является результатом. Результат из регистра РгА выводится на выход блока схем И3, задержанным сигналом «Конец операции».

Функциональная схема блока формирования кратных модуля Р, состоящая из одного регистра, трех сумматоров и трех блоков инверторов, приведена на рисунке 2. Код модуля Р до начала операции принимается в регистр РгР. Сумматоры СМ1, СМ2, СМ3 служат для вычисления, соответственно, значений кратных 3Р, 5Р и 7Р. Соответствующие блоки инверторов 1, 2, 3 служат для формирования инверсных кодов $3\overline{P}$, $5\overline{P}$ и $7\overline{P}$. Значения 2Р и $2\overline{P}$ получаются путем сдвига Р и $\overline{P}$ на один разряд влево в сторону старших разрядов, а значение 4Р и $4\overline{P}$ путем сдвига Р и $\overline{P}$ на два разряда влево в сторону старших разрядов. Значения 6Р и $6\overline{P}$ получаются путем сдвига 3Р и $3\overline{P}$ на один разряд влево в сторону старшего разряда.

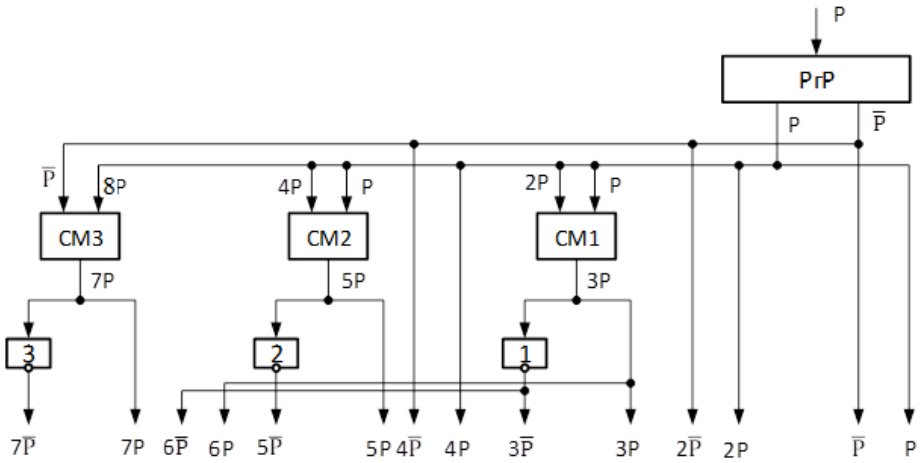

Рисунок 2. Функциональная схема блока формирования кратных модуля Р

Основным блоком устройства является ФЧО, который формирует остаток R_i. На рисунке 3 приведена функциональная схема ФЧО.

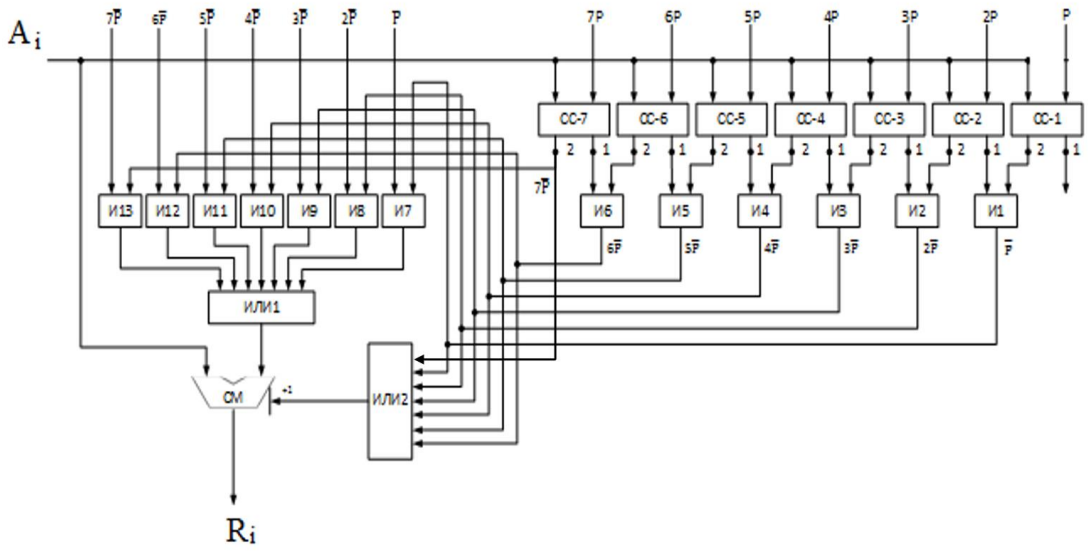

Рисунок 3. Функциональная схема ФЧО

ФЧО состоит из семи схем сравнения СС1÷СС7, сумматора СМ, логических схем И1÷И6, блоков логических схем ИЛИ1, И7÷И13, схемы ИЛИ2. Значение предыдущего остатка R_{i-1}, сдвинутое влево на три разряда с сторону старших разрядов, с присоединенным к нему очередными тремя младшими битами приводимого числа А, определяет значение

$$A_i = 8R_{i-1} + a_{n-2i+1}a_{n-2i}a_{n-2i-1}\,.$$

Предыдущим остатком в начале операции является значение n основных старших разрядов 2n-разрядного приводимого числа А. Значение A_i подается на левые входы сумматора СМ и на левые входы схем СС1÷СС7, где A_i сравнивается одновременно со значениями Р÷7Р, соответственно. В зависимости от результата сравнения на сумматоре СМ выполняется вычитание или Р, или одного из кратных модулей Р, что позволяет получить остаток R_i <Р.

При выполнении операции приведения по модулю на каждом шаге возможен случай, когда текущее приводимое число A_i будет меньше модуля Р.

Ниже описывается работа ФЧО, когда текущее приводимое число A_i меньше модуля Р.

Если A_i меньше модуля Р текущий вычисляемый остаток R_i будет равен A_i. И текущее приводимое число A_i, подаваемое на вход СМ, должно быть выдано на выход сумматора СМ (выход R_i) без изменения. Исключение изменения A_i (вычитания Р÷7Р) на сумматоре СМ обеспечивается тем, что при сравнении на выходах 2 всех схем СС-1÷СС-7 формируются сигналы «0». Эти сигналы через схемы И1÷И6 блокируют передачу инверсных значений Р÷7Р через блоки схем И7÷И13 на правые входы сумматора СМ. На выходе схемы ИЛИ2 также формируется сигнал «0». Вычитание на сумматоре СМ не выполняется. A_i без изменения поступает на выход ФЧО.

Но если A_i не меньше модуля Р, то необходимо на сумматоре СМ обеспечить выполнение вычитания одного из кратных модуля Р. Должно вычитаться то значение кратное модулю Р, которое даст наименьший положительный остаток. Для этого используются схемы сравнения СС-1÷СС-7, на которых выполняется одновременно сравнение текущего A_i с Р÷7Р, соответственно. В зависимости от значений сигналов на выходах 1 и 2 схем сравнения СС-1÷СС-7 определяется нужное для вычитания кратное модуля Р.

Ниже описывается работа ФЧО, когда текущее приводимое число A_i больше модуля Р.

Схема СС-1 сравнивает A_i с Р и формирует на выходе 2 сигнал «1». Схема СС-2 сравнивает A_i с 2Р. Если A_i меньше 2Р, то формируется на выходе 2 сигнал «0», а на выходе 1 сигнал «1». В этом случае все остальные схемы СС-3÷СС7 формируют на выходах 2 сигнал «0», а на выходе 1 сигнал «1». Таким образом, только на входах схемы И1 все сигналы равны «1», что приводит к тому, что на выходе И1 сигнал равен «1». Этот единичный сигнал подается на управляющий вход блока схем И7, разрешая прохождение $\overline{P}$ на правый вход сумматора СМ. Этот же единичный сигнал формирует через схему ИЛИ2 сигнал «1», который подается на вход «+1» сумматора. На сумматоре СМ выполняется вычитание A_i-Р (операция $R_i=A_i+\overline{P}+1$).

Когда на выходе 2 схемы СС-2 сигнал «1», а на выходе 1 сигнал «0», то это означает, что A_i больше 2Р. И в этом случае необходимо определить, какое из кратных модуля Р (2Р÷7Р) должно использоваться при вычитании на сумматоре СМ для определения текущего частичного остатка R_i, который должен быть меньше A_i. Работа схем сравнения СС-3÷СС-7 позволяет это сделать. Если на выходе 1 схемы СС-3 сигнал «1», а на выходе 2 сигнал «0», то это означает, что A_i меньше 3Р. И, с учетом того, что на выходе 2 схемы СС-2 сигнал «1», на оба входа схемы И2 подаются единичные сигналы. При этом с выходов 2 схем СС-3÷СС-7 и с выхода 1 схемы СС-2 нулевые сигналы блокируют работу схем И7, И9÷И13 через схемы И1, И3÷И6. Единичный сигнал с выхода схемы И2 подается на управляющий вход блока схем И8, разрешая прохождение только $2\overline{P}$ на правый вход сумматора СМ. Этот же единичный сигнал формирует через схему ИЛИ2 сигнал «1», который подается на вход «+1» сумматора. На сумматоре СМ выполняется вычитание A_i-2Р (операция $R_i=A_i+2\overline{P}+1$).

Если A_i не только больше 2P, но и больше 3P, то и на выходе 2 схемы СС-3 сигнал «1», а на выходе 1 сигнал «0». И в этом случае необходимо определить, какое из кратных модуля P (3P÷7P) должно использоваться при вычитании на сумматоре СМ для определения текущего частичного остатка R_i, который должен быть меньше A_i. Схемы сравнения СС-4÷СС-7, сравнивая A_i с 4P÷7P, соответственно, определяют необходимое кратное модуля P для вычитания. Если на выходе 1 схемы СС-4 сигнал «1», а на выходе 2 сигнал «0», то это означает, что A_i меньше 4P. И, с учетом того, что на выходе 2 схемы СС-3 сигнал «1», на оба входа схемы И3 подаются единичные сигналы. При этом с выходов 2 схем СС-4÷СС-7 и с выходов 1 схем СС-2 и СС-3 нулевые сигналы блокируют работу схем И7, И8, И10÷И13 через схемы И1, И2, И4÷И6. Единичный сигнал с выхода схемы И3 подается на управляющий вход блока схем И9, разрешая прохождение только $3\overline{P}$ на правый вход сумматора СМ. Этот же единичный сигнал формирует через схему ИЛИ2 сигнал «1», который подается на вход «+1» сумматора. На сумматоре СМ выполняется вычитание A_i-3P (операция $R_i=A_i+3\overline{P}+1$).

Если A_i не только больше 2P, 3P, но и больше 4P, то и на выходе 2 схемы СС-4 сигнал «1», а на выходе 1 сигнал «0». Схемы сравнения СС-5÷СС-7, сравнивая A_i с 5P÷7P, соответственно, определяют необходимое кратное модуля P для вычитания на сумматоре СМ для определения текущего частичного остатка R_i, который должен быть меньше A_i. Если на выходе 1 схемы СС-5 сигнал «1», а на выходе 2 сигнал «0», то это означает, что A_i меньше 5P. И, с учетом того, что на выходе 2 схемы СС-4 сигнал «1», на оба входа схемы И4 подаются единичные сигналы. При этом с выходов 2 схем СС-5÷СС-7 и с выходов 1 схем СС-2÷СС-4 нулевые сигналы блокируют работу схем И7÷И9, И11÷И13 через схемы И1÷И3, И5÷И6. Единичный сигнал с выхода схемы И4 подается на управляющий вход блока схем И10, разрешая прохождение только $4\overline{P}$ на правый вход сумматора СМ. Этот же единичный сигнал формирует через схему ИЛИ2 сигнал «1», который подается на вход «+1» сумматора. На сумматоре СМ выполняется вычитание A_i-4P (операция $R_i=A_i+4\overline{P}+1$).

Если A_i не только больше 2P, 3P, 4P, но и больше 5P, то и на выходе 2 схемы СС-5 сигнал «1», а на выходе 1 сигнал «0». Схемы сравнения СС-6÷СС-7, сравнивая A_i с 6P÷7P, соответственно, определяют кратное модуля P, вычитаемое из A_i. Если на выходе 1 схемы СС-6 сигнал «1», а на выходе 2 сигнал «0», то это означает, что A_i меньше 6P. И, с учетом того, что на выходе 2 схемы СС-5 сигнал «1», на оба входа схемы И5 подаются единичные сигналы. При этом с выходов 2 схем СС-6÷СС-7 и с выходов 1 схем СС-2÷СС-5 нулевые сигналы блокируют работу схем И7÷И10, И12,И13 через схемы И1÷И4, И6. Единичный сигнал с выхода схемы И5 подается на управляющий вход блока схем И11, разрешая прохождение только $5\overline{P}$ на правый вход сумматора СМ. Этот же единичный сигнал формирует через схему ИЛИ2 сигнал «1», который подается на вход «+1» сумматора. На сумматоре СМ выполняется вычитание A_i-5P (операция $R_i=A_i+5\overline{P}+1$).

Если A_i больше 6P, то на выходах 2 схем СС-1÷СС6 единичные сигналы, а на выходах 1 нулевые сигналы. Кратное модуля P, необходимое для вычитания из A_i, определяется по результату сравнения на схеме СС-7. Если на выходе 1 схемы СС-7 сигнал «1», а на выходе 2 сигнал «0», то это означает, что A_i меньше 7P. И, с учетом того, что на выходе 2 схемы СС-6 сигнал «1», на оба входа схемы И6 подаются единичные сигналы. При этом с выхода 2 схемы СС-7 и с выходов 1 схем СС-2÷СС-6 нулевые сигналы блокируют работу схем И7÷И11, И13 через схемы И1÷И5. Единичный сигнал с выхода схемы И6 подается на управляющий вход блока схем И12, разрешая прохождение только $6\overline{P}$ на правый вход сумматора СМ. Этот же единичный сигнал формирует через схему ИЛИ2 сигнал «1», который подается на вход «+1» сумматора. На сумматоре СМ выполняется вычитание A_i-6P (операция $R_i=A_i+6\overline{P}+1$).

При условии A_i больше 7P на выходе 2 СС-7 формируется сигнал «1», который подается на вход схемы ИЛИ2 и на управляющий вход блока схем И13, что приводит к выполнению сумматором СМ операции $R_i=A_i+7\overline{P}+1$. При этом с с выходов 1 схем СС-2÷СС-7 нулевые сигналы блокируют работу схем И7÷И12 через схемы И1÷И6.

Для лучшего понимания и наглядности все рассмотренные выше случаи сведены в таблицу 1, в которой приведены условия выполнения и выполняемые сумматором СМ в ФЧО операции по результатам сравнения на схемах СС-1÷СС-7 текущего приводимого числа A_i со значением кратных модуля Р (Р÷7Р).

Таблица 1. **Выполнение операции по результатам сравнения A_i с кратными модуля Р÷7Р**

№ п/п	Соотношения	Сигналы «1» на выходах схем СС-1÷СС-7	Выполняемые операции в СМ
1	$A_i<P$	СС-1, выход 1 ($A_i<P$)	$R_i=A_i$
2	$P\le A_i<2P$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 1 ($A_i<2P$)	$R_i=A_i+\overline{P}+1$
3	$2P\le A_i<3P$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 2 ($A_i\ge 2P$) СС-3, выход 1 ($A_i<3P$)	$R_i=A_i+2\overline{P}+1$
4	$3P\le A_i<4P$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 2 ($A_i\ge 2P$) СС-3, выход 2 ($A_i\ge 3P$) СС-4, выход 1 ($A_i<4P$)	$R_i=A_i+3\overline{P}+1$
5	$4P\le A_i<5P$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 2 ($A_i\ge 2P$) СС-3, выход 2 ($A_i\ge 3P$) СС-4, выход 2 ($A_i\ge 4P$) СС-5, выход 1 ($A_i<5P$)	$R_i=A_i+4\overline{P}+1$
6	$5P\le A_i<6P$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 2 ($A_i\ge 2P$) СС-3, выход 2 ($A_i\ge 3P$) СС-4, выход 2 ($A_i\ge 4P$) СС-5, выход 2 ($A_i\ge 5P$) СС-6, выход 1 ($A_i<6P$)	$R_i=A_i+5\overline{P}+1$
7	$6P\le A_i<7P$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 2 ($A_i\ge 2P$) СС-3, выход 2 ($A_i\ge 3P$) СС-4, выход 2 ($A_i\ge 4P$) СС-5, выход 2 ($A_i\ge 5P$) СС-6, выход 2 ($A_i\ge 6P$) СС-7, выход 1 ($A_i<7P$)	$R_i=A_i+6\overline{P}+1$
8	$7P\ge A_i$	СС-1, выход 2 ($A_i\ge P$) СС-2, выход 2 ($A_i\ge 2P$) СС-3, выход 2 ($A_i\ge 3P$) СС-4, выход 2 ($A_i\ge 4P$) СС-5, выход 2 ($A_i\ge 5P$) СС-6, выход 2 ($A_i\ge 6P$) СС-7, выход 2 ($A_i\ge 7P$)	$R_i=A_i+7\overline{P}+1$

Пример.

Пусть $A = 2602_{10} = \begin{cases} a_{11}a_{10}a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0 \\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0_2 \end{cases}$;

$P=55_{10}=110111_2$; $2P=110_{10}$, $3P=165_{10}$; $4P=220_{10}$; $5P=275_{10}$; $6P=330_{10}$; $7P=385_{10}$.

n=12, n=6. Первоначальное значение СчТИ равно $K=n/3=2_{10}=10_2$.

Значение нулевого (начального) остатка R_0 составляют старшие шесть разрядов числа А, т.е. $R_0=101000_2=40_{10}$. Для наглядности вычисления по определению остатка выполнены в десятичной системе счисления и приведены в таблице 2.

Таблица 2. **Вычисления по приведению числа А по модулю Р**

Тактовые импульсы	Изменения значения СчТИ	Выполняемые действия в регистре А и в формирователе частичных остатков (ФЧО)
ТИ1	СчТИ – 1_{10} = 10_2-01_2 = 01_2=1_{10}	В регистре А: A_1=$8R_0$+$a_5a_4a_3$=8·40+5=325_{10}. В ФЧО: так как 275<325<330 (5Р<A_1<6Р), то R_1=A_1-5Р=325-275=50_{10}
ТИ2	СчТИ – 1 = 01_2-01_2 = 00_2=0_{10} Конец операции	В регистре А: А2= 8R1+$a_2a_1a_0$=8·50+2=402_{10}. В ФЧО: так как 385<402 (7Р<A_2), то R_2 =R= A_2-7Р=402-385=17_{10}

Проверка:

$$R = A -]\frac{A}{P}[\cdot P = 2602 -]\frac{2602}{55}[\cdot 55 = 2602 - 47 \cdot 55 = 2602 - 2585 == 17_{10}$$

Заключение. Устройство приведения чисел по модулю с использованием кратных модуля и сдвигом приводимого числа на каждом шаге на три разряда влево в сторону старших разрядов позволяет ускорить приведение по модулю за счет уменьшения в три раза количества шагов приведения по модулю, но при этом увеличиваются аппаратные затраты. Для сокращения аппаратных затрат и получения большего быстродействия в ФЧО для определения вычитаемых кратных модуля применены вместо сумматоров схемы сравнения. Если для этих целей в ФЧО применить сумматоры, то для этого потребовалось бы семь сумматоров, что приводит к большим аппаратным затратам.

Дальнейшим направлением исследования является моделирование разработанного устройства приведения по модулю. В качестве среды для проектирования и отладки проекта могут быть использованы программные продукты САПР (Quartus Prime Lite Edition или Vivado Design Suite), которые позволяют построить модели устройства и проверить его работоспособность с иллюстрацией на временных диаграммах, а также получить временные характеристики моделируемого устройства. САПР позволяют выполнить, как функциональное, так и временное моделирование, т.е. проверить правильность работы цифрового устройства и работу с учетом задержки распространения сигналов в реальной программируемой логической интегральной схеме.

Быстродействующее устройство может использоваться как в криптопроцессорах, так и в цифровых вычислительных устройствах.

ЛИТЕРАТУРА

[1] Айтхожаева, Е.Ж. Аспекты аппаратного приведения по модулю в асимметричной криптографии [Текст] / Е.Ж. Айтхожаева, С.Т. Тынымбаев // Вестник Национальной Академии Наук Республики Казахстан. -2014. -№5 (375). -С. 88-93.

[2] Панкратова, И.А. Теоретико-числовые методы криптографии [Текст]: Учебное пособие. / И.А. Панкратова // Томский государственный университет. Томск: ТГУ, 2009. -120 с.

[3] Ковтун, М. Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений / М. Ковтун, В. Ковтун // Компания Сайфер. -2017. (http://docplayer.ru/30671408-Obzor-i-klassifikaciya-algoritmov- deleniya-i-privedeniya-po-modulyu-bolshih-celyh-chisel-dlya-kriptograficheskih-prilozheniy.html).

[4] Умножитель по модулю: пат. 2299461 С1 Рос. Федерация. МПК G06F 7/523, G06F 7/72 / Петренко В.И., Кузьминов Ю.В.; заявитель и патентообладатель Петренко В.И., Кузьминов Ю.В. -№2005130895/09; заявл. 05.10.2005; опубл. 20.05.2007, Бюл. №14.

[5] Устройство для формирования остатка по произвольному модулю: пат. 2368942 С2 Рос. Федерация. МПК G06F 7/72, H03M 7/18 / Петренко В.И., Сидорчук А.В., Кузьминов Ю.В.; заявитель и патентообладатель Государственное образовательное учреждение высшего профессионального образования "Ставропольский военный институт связи РВ"- № 2007124282/09; заявл. 27.06.2007; опубл. 27.09.2009. Бюл. №27.

[6] Устройство для формирования остатка по произвольному модулю от числа: пат. 2445730 С2

Рос. Федерация. МПК H03M 7/18, G06F 7/72 / Копытов В.В., Петренко В.И., Сидорчук А.В.; заявитель и патентообладатель Государственное образовательное учреждение высшего профессионального образования "Ставропольский военный институт связи РВ"- № 2010106685/08; заявл. 24.02.2010; опубл. 20.03.2012 Бюл. № 8.

[7] Орлов, С. А. Организация ЭВМ и систем [Текст]: фундаментальный курс по архитектуре и структуре современных компьютерных средств 3-изд / С.А. Орлов, Б.Я. Цилькер -. СПб.: Питер Пресс, 2014. -688 с.: ил.

[8] Устройство для формирования остатка по заданному модулю: пат 2421781 С1 Рос. Федерация. МПК G06F 7/72, H03M 7/18 / Захаров В.М., Столов Е.Л., Шалагин С.В.; заявитель и патентообладатель Государственное образовательное учреждение высшего профессионального образования Казанский государственный технический университет им. А.Н. Туполева - №2009138613/08; заявл. 19.10.2009; опубл. 20.06.2011, Бюл. №17.

[9] Method and apparatus for efficient modulo multiplication: pat. 8417756 B2 United States. Int. Cl. G06F 7/38 / Pisek E., Henige T.M.; Assignee: Samsung Electronics Co., Ltd., - № 12/216,896; Filed 11.07.2008; Date of Patent 09.04.2013.

[10] Method and apparatus for modulus reduction: pat. 8862651 B2 United States. Int. Cl. G06F 7/38, G06F 7/72, H04L 9M32, H04L 9/30/ Lambert R.J.; Assignee: Certicom Corp., Mississauga -№ 12/609,772; Filed 30.10.2009; Date of Patent 14.10.2014.

[11] Method for arbitrary-precision division or modular reduction: pat. 9042543 B2 United States. Int. Cl. H04L 9/00, H04L 9M32 / Bockes M., Pulkus J.; Assignee: GIESECKE & DEVRIENT GMBH, Munich - № 13/885, 878; Filed 16.11.2011; Date of Patent 26.05.2015.

[12] Yu, H. Efficient Modular Reduction Algorithm Without Correction Phase [Текст] / H. Yu, G. Bai, H. Hao In: Wang J., Yap C. (eds) // Frontiers in Algorithmics FAW 2015. Lecture Notes in Computer Science. -2015. -№9130. -P. 304-313. doi: 10.1007/978-3-319-19647-3_28.

[13] Tynymbayev, S. High speed device for modular reduction [Text] / S. Tynymbayev, Y.Zh. Aitkhozhayeva, S. Adilbekkyzy // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. -2018. -№6(376). -P.147-152. doi: 10.32014/2018.2518-1467.38

[14] Tynymbayev, S. Modular reduction based on the divider by blocking negative remainders [Text] / S. Tynymbayev, S.A. Gnatyuk, Y.Zh. Aitkhozhayeva, R.Sh. Berdibayev, T.A. Namazbayev // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences. - 2019. №2(434). -P. 238-248. doi: 10.32014/2018.2518-1467.38.

[15] Tynymbaev, S. High-speed devices for modular reduction with minimal hardware costs [Text] / S. Tynymbaev, R.Sh. Berdibayev, T.K. Omar, Y.Zh. Aitkhozhayeva, A.A. Shaikulova, S. Adilbekkyzy // Cogent Engineering. -2019. -№6 (1), -P. 1–12. doi: 10.1080/23311916.2019.1697555

REFERENCES

[1] Ajthozhaeva, E.Zh. Aspekty apparatnogo privedenija po modulju v asimmetrichnoj kriptografii [Tekst] / E.Zh. Ajthozhaeva, S.T. Tynymbaev // Vestnik Nacional'noj Akademii Nauk Respubliki Kazahstan. -2014. -№5 (375). -S. 88-93.

[2] Pankratova, I.A. Teoretiko-chislovye metody kriptografii [Tekst]: Uchebnoe posobie. / I.A. Pankratova // Tomskij gosudarstvennyj universitet. Tomsk: TGU, 2009. -120 s.

[3] Kovtun, M. Obzor i klassifikacija algoritmov delenija i privedenija po modulju bol'shih celyh chisel dlja kriptograficheskih prilozhenij / M. Kovtun, V. Kovtun // Kompanija Sajfer. -2017. (http://docplayer.ru/30671408-Obzor-i-klassifikaciya-algoritmov- deleniya-i-privedeniya-po-modulyu-bolshih-celyh-chisel-dlya-kriptograficheskih-prilozheniy.html).

[4] Umnozhitel' po modulju: pat. 2299461 C1 Ros. Federacija. MPK G06F 7/523, G06F 7/72 / Petrenko V.I., Kuz'minov Ju.V.; zajavitel' i patentoobladatel' Petrenko V.I., Kuz'minov Ju.V. - №2005130895/09; zajavl. 05.10.2005; opubl. 20.05.2007, Bjul. №14.

[5] Ustrojstvo dlja formirovanija ostatka po proizvol'nomu modulju: pat. 2368942 S2 Ros. Federacija. MPK G06F 7/72, H03M 7/18 / Petrenko V.I., Sidorchuk A.V., Kuz'minov Ju.V.; zajavitel' i patentoobladatel' Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Stavropol'skij voennyj institut svjazi RV"- № 2007124282/09; zajavl. 27.06.2007; opubl. 27.09.2009. Bjul. №27.

[6] Ustrojstvo dlja formirovanija ostatka po proizvol'nomu modulju ot chisla: pat. 2445730 S2 Ros. Federacija. MPK H03M 7/18, G06F 7/72 / Kopytov V.V., Petrenko V.I., Sidorchuk A.V.; zajavitel' i patentoobladatel' Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Stavropol'skij voennyj institut svjazi RV"- № 2010106685/08; zajavl. 24.02.2010; opubl. 20.03.2012 Bjul. № 8.

[7] Orlov, S. A. Organizacija JeVM i sistem [Tekst]: fundamental'nyj kurs po arhitekture i strukture sovremennyh komp'juternyh sredstv 3-izd / S.A. Orlov, B.Ja. Cil'ker -. SPb.: Piter Press, 2014. -688 s.: il.

[8] Ustrojstvo dlja formirovanija ostatka po zadannomu modulju: pat 2421781 S1 Ros. Federacija. MPK G06F 7/72, H03M 7/18 / Zaharov V.M., Stolov E.L., Shalagin S.V.; zajavitel' i patentoobladatel' Gosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija Kazanskij gosudarstvennyj tehnicheskij universitet im. A.N. Tupoleva - №2009138613/08; zajavl. 19.10.2009; opubl. 20.06.2011, Bjul. №17.

[9] Method and apparatus for efficient modulo multiplication: pat. 8417756 B2 United States. Int. Cl. G06F 7/38 / Pisek E., Henige T.M.; Assignee: Samsung Electronics Co., Ltd., - № 12/216,896; Filed 11.07.2008; Date of Patent 09.04.2013.

[10] Method and apparatus for modulus reduction: pat. 8862651 B2 United States. Int. Cl. G06F 7/38, G06F 7/72, H04L 9M32, H04L 9/30/ Lambert R.J.; Assignee: Certicom Corp., Mississauga -№ 12/609,772; Filed 30.10.2009; Date of Patent 14.10.2014.

[11] Method for arbitrary-precision division or modular reduction: pat. 9042543 B2 United States. Int. Cl. H04L 9/00, H04L 9M32 / Bockes M., Pulkus J.; Assignee: GIESECKE & DEVRIENT GMBH, Munich - № 13/885, 878; Filed 16.11.2011; Date of Patent 26.05.2015.

[12] Yu, H. Efficient Modular Reduction Algorithm Without Correction Phase [Tekst] / H. Yu, G. Bai, H. Hao In: Wang J., Yap C. (eds) // Frontiers in Algorithmics FAW 2015. Lecture Notes in Computer Science. -2015. -№9130. -R. 304-313. doi: 10.1007/978-3-319-19647-3_28.

[13] Tynymbayev, S. High speed device for modular reduction [Text] / S. Tynymbayev, Y.Zh. Aitkhozhayeva, S. Adilbekkyzy // Bulletin of National Academy of Sciences of the Republic of Kazakhstan. -2018. -№6(376). -P.147-152. doi: 10.32014/2018.2518-1467.38

[14] Tynymbayev, S. Modular reduction based on the divider by blocking negative remainders [Text] / S. Tynymbayev, S.A. Gnatyuk, Y.Zh. Aitkhozhayeva, R.Sh. Berdibayev, T.A. Namazbayev // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences. -2019. №2(434). -P. 238-248. doi: 10.32014/2018.2518-1467.38.

[15] Tynymbaev, S. High-speed devices for modular reduction with minimal hardware costs [Text] / S. Tynymbaev, R.Sh. Berdibayev, T.K. Omar, Y.Zh. Aitkhozhayeva, A.A. Shaikulova, S. Adilbekkyzy // Cogent Engineering. -2019. -№6 (1), -P. 1–12. doi: 10.1080/23311916.2019.1697555

[1]Е.Ж. Айтхожаева, [2]С. Тынымбаев, [2]А.К. Мұқашева,
[2]Р.Ш. Бердибаев, [1]С. Әділбеккызы*
[1]Satbayev University, Алматы, Қазақстан
[2]Г. Даукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан
*e-mail: sairan.02.95@mail.ru

МОДУЛЬДІҢ БІРНЕШЕ ЕСЕЛІКТЕРІН ҚОЛДАНА ОТЫРЫП, МОДУЛЬ БОЙЫНША САНДАРДЫ КЕЛТІРУДІҢ ЖЫЛДАМ ӘРЕКЕТ ЕТЕТІН ҚҰРЫЛҒЫСЫ

Аңдатпа. Сандарды модуль бойынша келтіруге арналған жылдам әрекет ететін құрылғының аппаратты жолмен жүзеге асырылуы қарастылуда. Модификацияланған бөлінгіштің ығысумен бөлу алгоритмі қолданылды, әр қадамда алдымен бөлінгіштің n+3 жоғарғы разряды, содан кейін алынған қалдықтардың қатысады. Келтірілетін санды әр қадамда үш разрядқа солға қарай жоғары разрядқа ығыстыру модульге келтіру қадамдарының санын азайту арқылы модуль келтіру процесін жылдамдатуға мүмкіндік береді. Құрылғының негізгі блогы - жекелеген қалдықдарды қалтастырғыш блогы (ЖҚҚ), олар P модулін және P модулінің еселігін азайту қолданады. Аппараттық шығындарды азайту және жақсы өнімділікке жету үшін ЖҚҚ-де модульдің алынып тасталған еселіктерін анықтау үшін салыстыру схемалары қолданылады, бұл сумматор санын азайтуға мүмкіндік береді.

Негізгі сөздер: модуль бойынша келтіру, модульдің еселігі, жекелеген қалдықдарды қалтастырғыш

[1]Y.Zh. Aitkhozhayeva, [2]S.Tynymbayev, [2]A.K Mukasheva,
[2]R.Sh. Berdybaev, [1]S. Adilbekkyzy*
[1]Satbayev University, Almaty, Kazakhstan
[2]Almaty university of power engineering and telecommunications named after G.Daukeev, Almaty, Kazakhstan
*e-mail: sairan.02.95@mail.ru

HIGH-SPEED MODULAR REDUCTION DEVICE USING MULTIPLES OF MODULE

Abstract. A hardware implementation of a high-speed device for reducing numbers modulo is considered. We used a modified division algorithm with a shift of the dividend, where at each step n + 3 most significant bits of the dividend, and then the resulting remainders, participate. The shift of the reduced number at each step by three bits to the left towards the higher bits shifted and it makes it possible to speed up the process of reduction in modulus by reducing the number of modular reduction steps. The main unit of the device is a block of partial remainder formers (PRFs), which use subtraction of the P modulus and multiples of the P modulus.

Keywords: modulo reduction, modulus multiples, partial remainder formers