О создании эффективной аппаратной реализации ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 на основе ПЛИС

Родионов А.Ю.

РусКрипто’2014

Требования к алгоритмам для аппаратной реализации:

1. алгоритм редукции по простому модулю *M*, должен поддерживать общий случай, т.е. когда *M* не является псевдо числом Мерсена;
2. алгоритмы должны поддерживать конфигурируемый параметр итераций для реализации 256 и 512 битной схемы ЭЦП;
3. алгоритмы должны использовать небольшой объем памяти для хранения предвычисленных значений;
4. алгоритмы должны поддерживать возможность распараллеливания вычислений.

Список необходимых алгоритмов:

<table>
<tr><td>Алгоритмы PKI</td><td>Генерация ключевой пары</td><td>Генерация ЭЦП</td><td>Проверка ЭЦП</td><td>Вычисление ключа ДХ</td></tr>
<tr><td rowspan="2">Операции в группе точек эллиптической кривой</td><td colspan="4">Скалярное умножение точки на число</td></tr>
<tr><td colspan="2">Удвоение точки</td><td colspan="2">Сложение точек</td></tr>
<tr><td>Операции в конечном поле</td><td>Модулярное умножение</td><td>Модулярное сложение</td><td>Модулярное вычитание</td><td>Модулярное деление на 2</td><td>Нахождение обратного по модулю</td></tr>
</table>

Список необходимых алгоритмов:

<table>
<tr><td>Алгоритмы PKI</td><td>Генерация ключевой пары</td><td>Генерация ЭЦП</td><td>Проверка ЭЦП</td><td>Вычисление ключа ДХ</td></tr>
<tr><td rowspan="2">Операции в группе точек эллиптической кривой</td><td colspan="4">Скалярное умножение точки на число</td></tr>
<tr><td colspan="2">Удвоение точки</td><td colspan="2">Сложение точек</td></tr>
<tr><td>Операции в конечном поле</td><td>Модулярное умножение</td><td>Модулярное сложение</td><td>Модулярное вычитание</td><td>Модулярное деление на 2</td><td>Нахождение обратного по модулю</td></tr>
</table>

Список необходимых алгоритмов:

<table>
<tr><td>Алгоритмы PKI</td><td>Генерация ключевой пары</td><td>Генерация ЭЦП</td><td>Проверка ЭЦП</td><td>Вычисление ключа ДХ</td></tr>
<tr><td rowspan="2">Операции в группе точек эллиптической кривой</td><td colspan="4">Скалярное умножение точки на число</td></tr>
<tr><td colspan="2">Удвоение точки</td><td colspan="2">Сложение точек</td></tr>
<tr><td>Операции в конечном поле</td><td>Модулярное умножение</td><td>Модулярное сложение</td><td>Модулярное вычитание</td><td>Модулярное деление на 2</td><td>Нахождение обратного по модулю</td></tr>
</table>

Алгоритм умножения Монтгомери:

Входные данные алгоритма: $A, B < M; M < 2^{kn};$

$M' = -M^{-1} \bmod 2^k;$ $R = 2^{kn}$, *при НОД(M, R)=1.*

Выходные данные алгоритма: $S \equiv ABR^{-1} (\bmod M), 0 \le S < 2M$.

1) $S_0 = 0;$

2) для $i = 0 \ldots n-1$ выполнить 3) – 4);

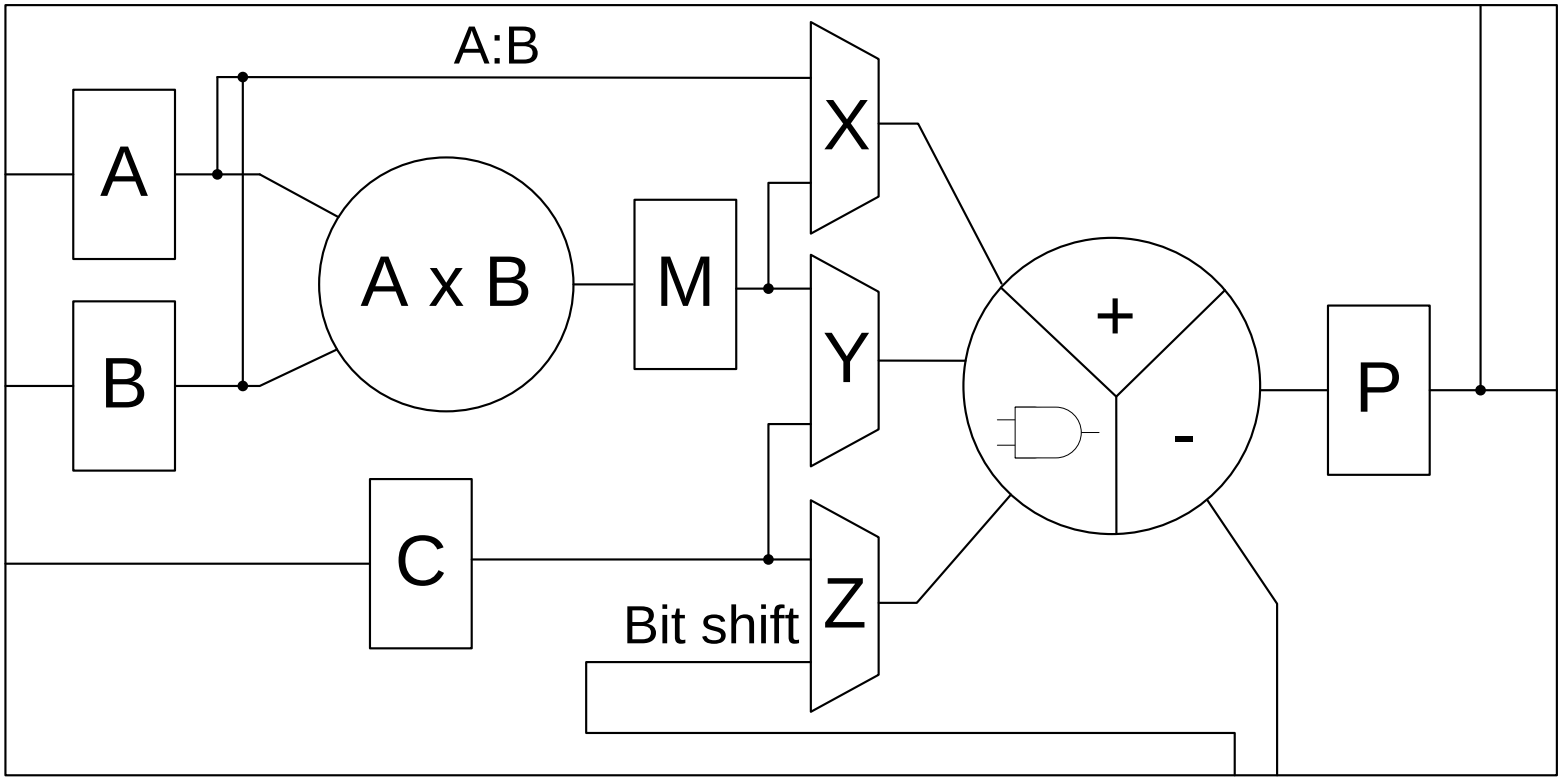
3) $q_i = (((S_i + a_i B) \bmod 2^k) M') \bmod 2^k;$

4) $S_{i+1} = (S_i + q_i M + a_i B) / 2^k;$

5) *если* $S \ge M$, *то* $S = S - M;$

6) конец.

Обобщенная схема DSP блока



Алгоритм умножения Монтгомери:

Входные данные алгоритма: $A, B < M; M < 2^{kn};$

$M' = -M^{-1} \bmod 2^k;$ $R = 2^{kn}$, *при НОД(M, R)=1.*

Выходные данные алгоритма: $S \equiv ABR^{-1} (\bmod M), 0 \le S < 2M$.

1) $S_0 = 0;$

2) для $i = 0 \ldots n-1$ выполнить 3) – 4);

3) $q_i = (((S_i + a_i B) \bmod 2^k) M') \bmod 2^k;$

4) $S_{i+1} = (S_i + q_i M + a_i B) / 2^k;$

5) *если* $S \ge M$, *то* $S = S - M;$

6) конец.

Алгоритм умножения Монтгомери без финального вычитания:

Входные данные алгоритма: $A, B < 2M$; $M < 2^{k(n+1)}$;

$M' = -M^{-1} \bmod 2^k$; $R = 2^{k(n+1)}$, *при НОД(M, R)=1.*

Выходные данные алгоритма: $S \equiv ABR^{-1} (\bmod M)$, $0 \le S < 2M$.

1) $S_0 = 0$;

2) для $i = 0 \ldots n$ выполнить 3) – 4);

3) $q_i = (((S_i + a_i b_0) \bmod 2^k) M') \bmod 2^k$;

4) $S_{i+1} = (S_i + q_i M + a_i B) / 2^k$;

5) конец.

Список необходимых алгоритмов:

<table>
<tr><td>Алгоритмы PKI</td><td>Генерация ключевой пары</td><td>Генерация ЭЦП</td><td>Проверка ЭЦП</td><td>Вычисление ключа ДХ</td></tr>
<tr><td rowspan="2">Операции в группе точек эллиптической кривой</td><td colspan="4">Скалярное умножение точки на число</td></tr>
<tr><td colspan="2">Удвоение точки</td><td colspan="2">Сложение точек</td></tr>
<tr><td>Операции в конечном поле</td><td>Модулярное умножение</td><td>Модулярное сложение</td><td>Модулярное вычитание</td><td>Модулярное деление на 2</td><td>Нахождение обратного по модулю</td></tr>
</table>

Алгоритм удвоения точки с использованием 4-х аппаратных блоков умножения Монтгомери:

$P_2(X_2, Y_2, Z_2, Z_2^4) = 2P_1(X_1, Y_1, Z_1, Z_1^4)$

Конечный автомат	Умножитель Монтгомери №1	Умножитель Монтгомери №2	Умножитель Монтгомери №3	Умножитель Монтгомери №4
$Y_2 = 2Y_1$			$T_3 = aZ_1^4$	$T_0 = X_1^2$
	$Y_2 = Y_2^2$	$Z_2 = Y_2 Z_1$	…	…
	…	…	…	…
$T_2 = 2T_0$	…	…		
$T_0 = T_0 + T_2$	$T_1 = Y_2^2$	$T_3 = Z_2^2$	$Y_2 = X_1 Y_2$	
$T_0 = T_0 + T_3$	…	…	…	
	…	…	…	$X_2 = T_0^2$
$T_2 = 2Y_2$				…
$Y_2 = T_2 + Y_2$				…
$Y_2 = Y_2 - X_2$				
$X_2 = X_2 - T_2$		$Z_2^4 = T_3^2$	$Y_2 = T_0 Y_2$	
$T_1 = T_1 / 2$		…	…	
		…	…	
$Y_2 = Y_2 - T_1$				

Алгоритм сложения точек с использованием 4-х аппаратных блоков умножения Монтгомери:

$$P_2(X_2, Y_2, Z_2, Z_2^4) = P_0(X_0, Y_0, Z_0, Z_0^4) + P_1(X_1, Y_1, Z_1, Z_1^4)$$

Конечный автомат	Умножитель Монтгомери №1	Умножитель Монтгомери №2	Умножитель Монтгомери №3	Умножитель Монтгомери №4
	$T_4 = Z_0^2$	$T_0 = Z_1^2$	$T_2 = Z_0 Z_1$	
	$T_1 = T_4 Z_0$	$T_3 = T_0 Z_1$	$X_2 = X_0 T_0$	$T_4 = T_4 X_1$
$T_4 = T_4 - X_2$	$T_1 = T_1 Y_1$	$Y_2 = T_3 Y_0$		
	…	…	$T_0 = T_4^2$	$Z_2 = T_2 T_4$
	…	…	…	…
$T_1 = T_1 - Y_2$			…	…
$Y_2 = T_1 - Y_2$	$X_2 = T_1 T_1$	$T_0 = T_0 X_2$	$T_2 = T_4 T_0$	$T_4 = Z_2 Z_2$
	…	…	…	…
	…	…	…	…
$T_3 = 2T_0$				
$T_0 = T_0 + T_3$				
$T_0 = T_0 - X_2$				
$X_2 = X_2 - T_3$		$T_0 = T_0 T_1$	$Y_2 = Y_2 T_2$	$Z_2^4 = T_4^2$
$X_2 = X_2 - T_2$		…	…	…
$Y_2 = Y_2 + T_0$				

Вычислительная сложность групповых операций над точками эллиптической кривой в Якобиевом представлении в количестве модулярных умножений

	С использованием 1 блока умножения	С использованием 4 блоков умножения
Удвоение точки	8	3
Сложение точки	16	5

Список необходимых алгоритмов:

<table>
<tr><td>Алгоритмы PKI</td><td>Генерация ключевой пары</td><td>Генерация ЭЦП</td><td>Проверка ЭЦП</td><td>Вычисление ключа ДХ</td></tr>
<tr><td rowspan="2">Операции в группе точек эллиптической кривой</td><td colspan="4">Скалярное умножение точки на число</td></tr>
<tr><td colspan="2">Удвоение точки</td><td colspan="2">Сложение точек</td></tr>
<tr><td>Операции в конечном поле</td><td>Модулярное умножение</td><td>Модулярное сложение</td><td>Модулярное вычитание</td><td>Модулярное деление на 2</td><td>Нахождение обратного по модулю</td></tr>
</table>

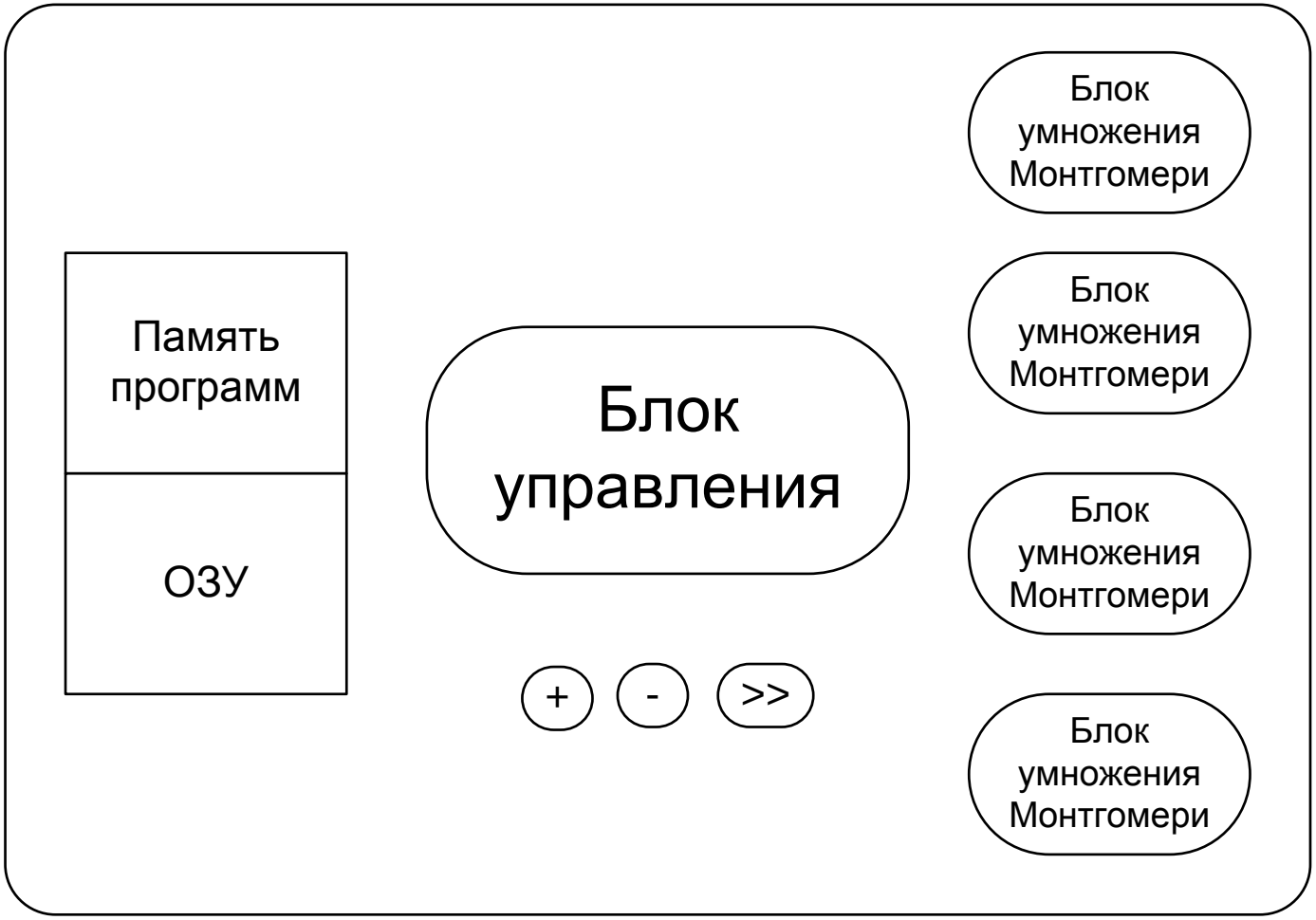
Вычислительная сложность скалярного произведения для произвольных точек эллиптической кривой

Алгоритм	Длина чисел в битах	K	Количество модулярных умножений	Размер таблицы предвычисленных значений, КБ
SimMul	256	2	763	2,1
wNAF	256	5	1020	1
SimMul	512	2	1467	4,1
wNAF	512	6	1980	4

Вычислительная сложность скалярного произведения для фиксированных точек эллиптической кривой

Алгоритм	Длина чисел в битах	K	Количество модулярных умножений	Размер таблицы предвычисленных значений, КБ
SimMul	256	2	704	2,1
wNAF	256	5	928	4,25
SimMul	512	2	1408	4,1
wNAF	512	6	1902	4,1

Блок, реализующий ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012



Результаты

	Время генерации ЭЦП, мс	Время проверки ЭЦП, мс	Logic Elements	DSP	BRAM
ГОСТ Р 34.10-2001	3,33	6,25	3256	8	5
ГОСТ Р 34.10-2012	16,66	31,25			

Вопросы