Эффективная реализация перспективного алгоритма блочного шифрования, функции хэширования ГОСТ Р 34.11-2012 и ЭЦП ГОСТ Р 34.10-2012

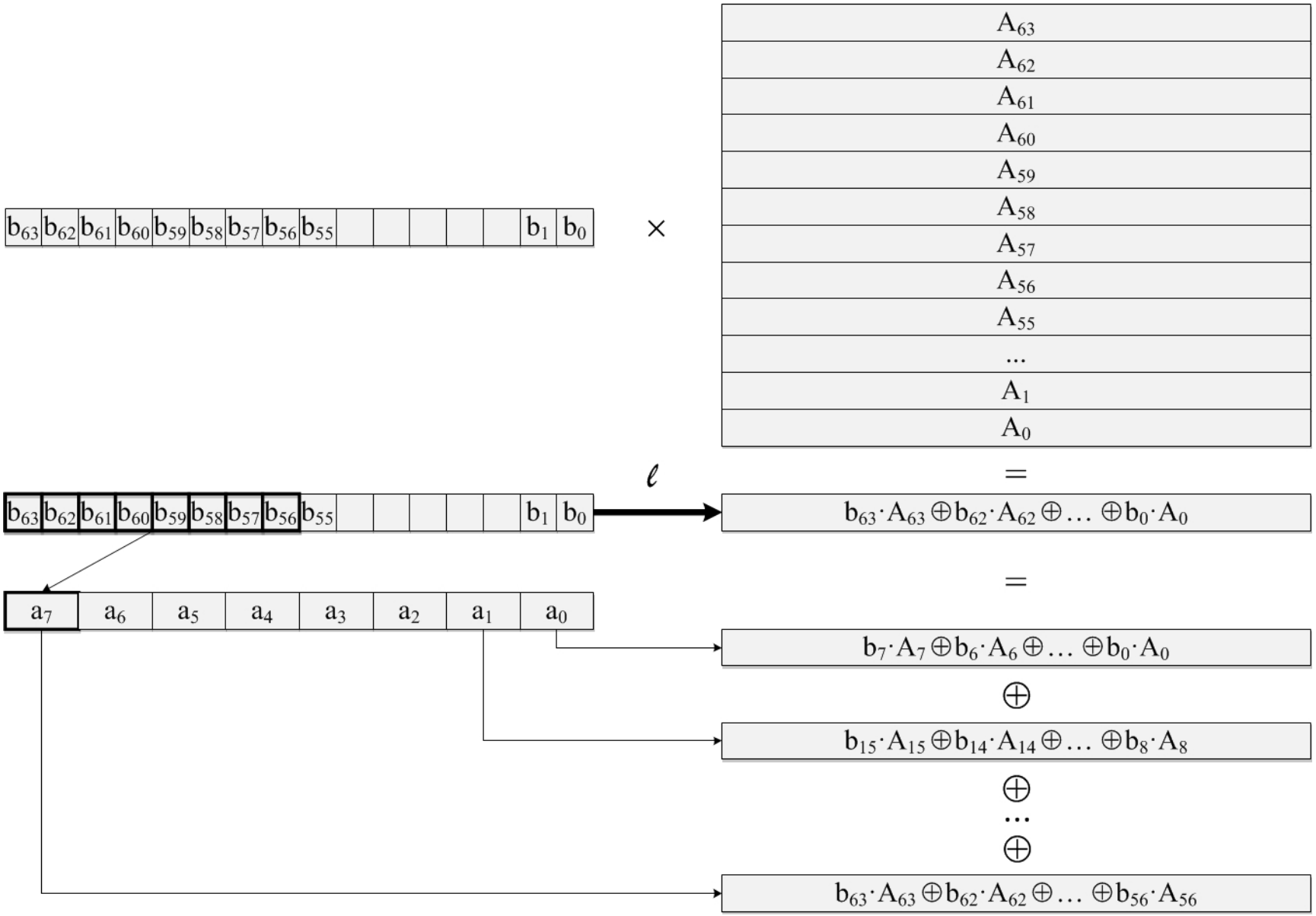
М.А. Бородин, А.С. Рыбкин

ОАО ИнфоТеКС
{mikhail.borodin, andrey.rybkin}@infotecs.ru

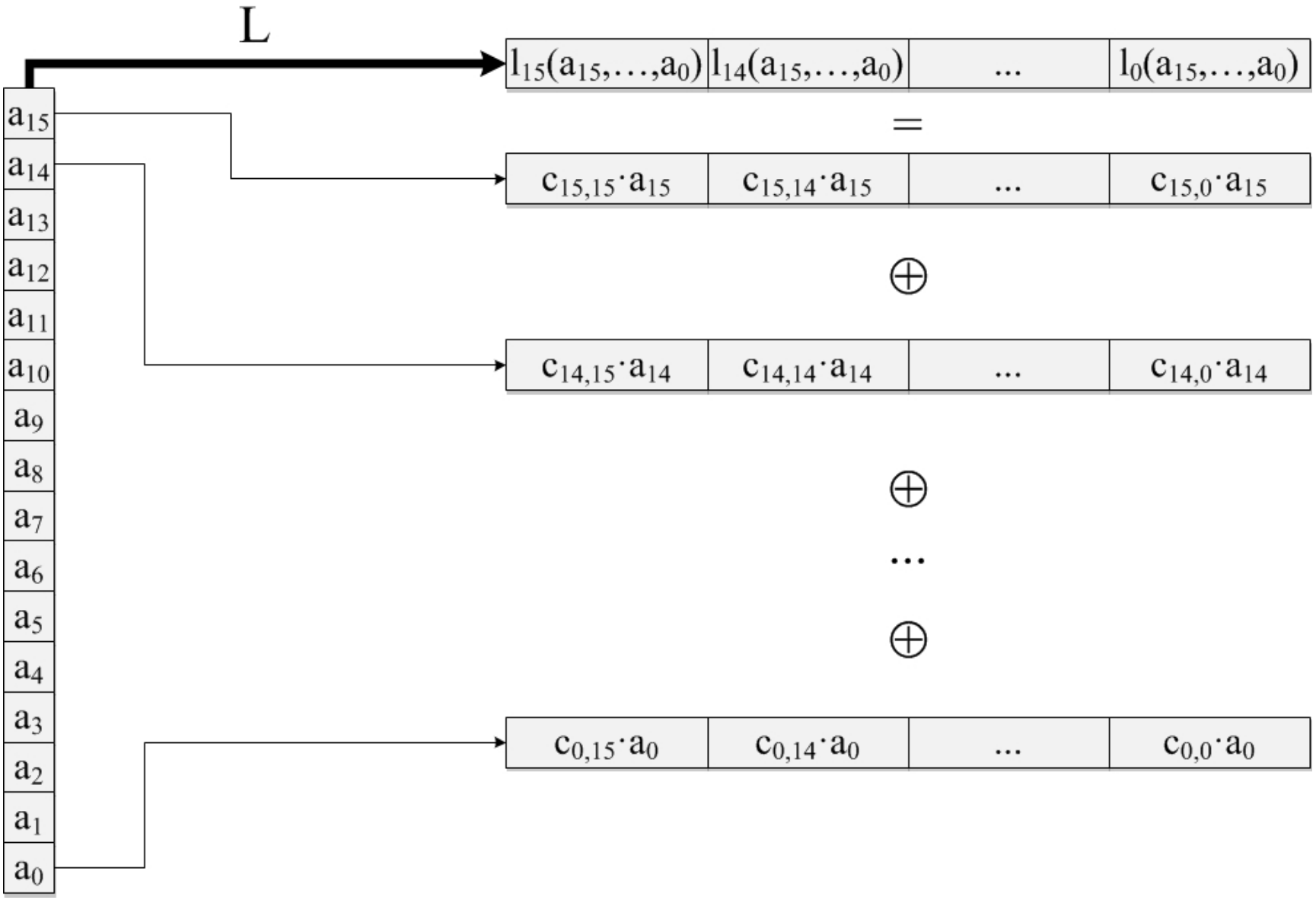
Москва, 2014

Стрибог ГОСТ Р 34.11-2012	Перспективный блочный шифр
LPSX	*LSX*
Основные преобразования	
$g_N(h, m) = E(LPSX[N](h), m) \oplus h \oplus m;$	
$E(K, m) = X[K_{13}]LPSX[K_{12}] \dots LPSX[K_1](m).$	$E(a) = X[K_{10}]LSX[K_9] \dots LSX[K_1](a);$
	$D(a) = X[K_1]S^{-1}L^{-1}X[K_2] \dots S^{-1}L^{-1}X[K_{10}](a).$
Вычисление ключей	
$K_1 = K;$	$(K_1, K_2) = K;$
$K_i = LPSX[C_{i-1}](K_{i-1}),\ i = 2, .., 13.$	$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}] \dots F[C_{8(i-1)+1}](K_{2i-1}, K_{2i}),$
	$i = 1, 2, 3, 4;$
	$F[C](a_1, a_0) = (LSX[C](a_1) \oplus a_0, a_1).$
Операции	
$X[K](a) = K \oplus a;$	$X[K](a) = K \oplus a;$
$S(a) = S(a_{63}\| \dots \|a_0) = \pi(a_{63})\| \dots \|\pi(a_0);$	$S(a) = S(a_{15}\| \dots \|a_0) = \pi(a_{15})\| \dots \|\pi(a_0);$
$L(a) = L(a_7\| \dots \|a_0) = l(a_7)\| \dots \|l(a_0);$	$L(a) = R^{16}(a);$
$P(a) = P(a_{63}\| \dots \|a_0) = a_{\tau(63)}\| \dots \|a_{\tau(0)}.$	$R(a) = R(a_{15}\| \dots \|a_0) = l(a_{15}, \dots, a_0)\|a_{15}\| \dots \|a_1.$

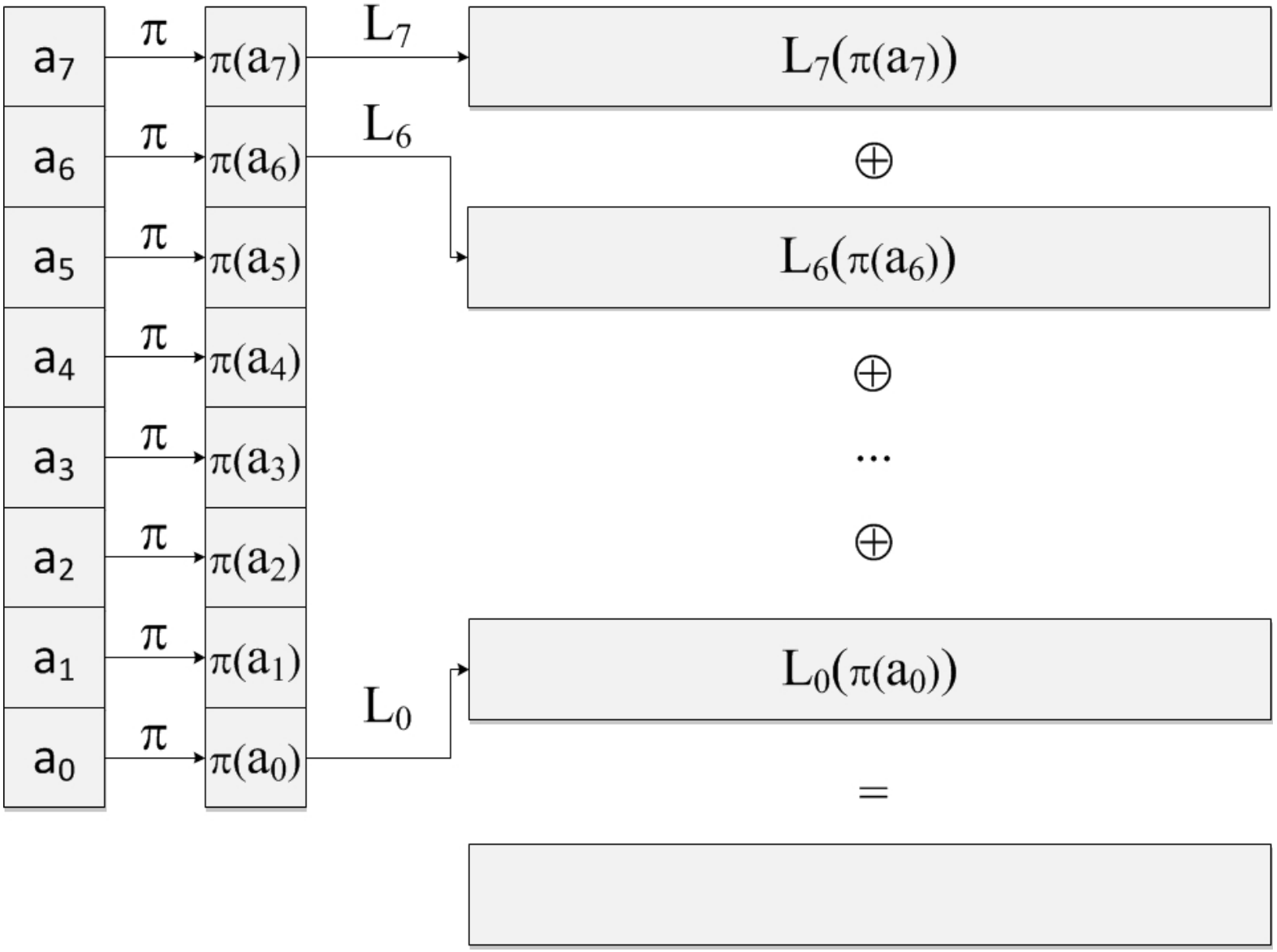
Преобразование l в алгоритме Стрибог



Преобразование L в ПБШ



Преобразования S и L



Преобразование *LS*

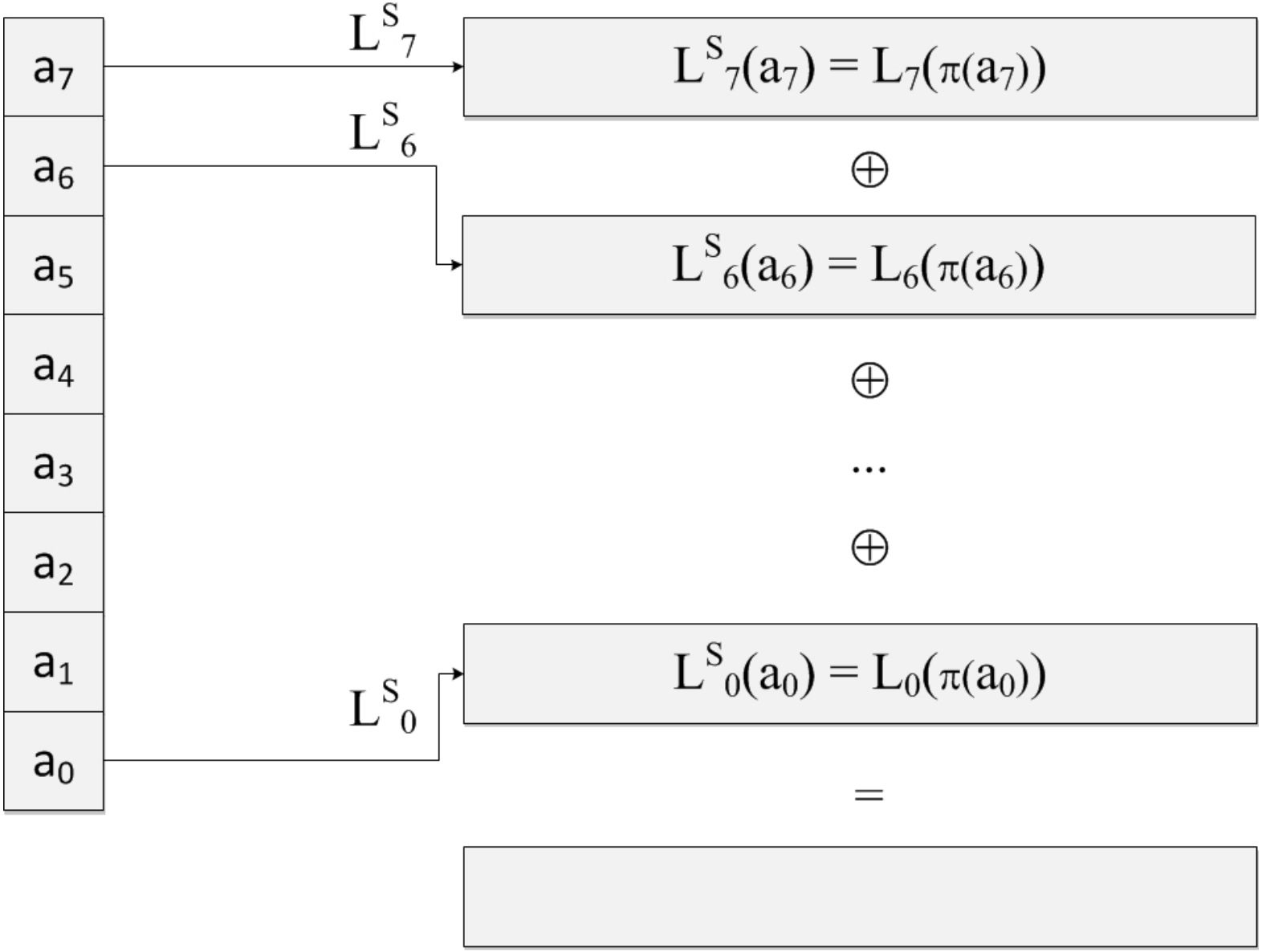
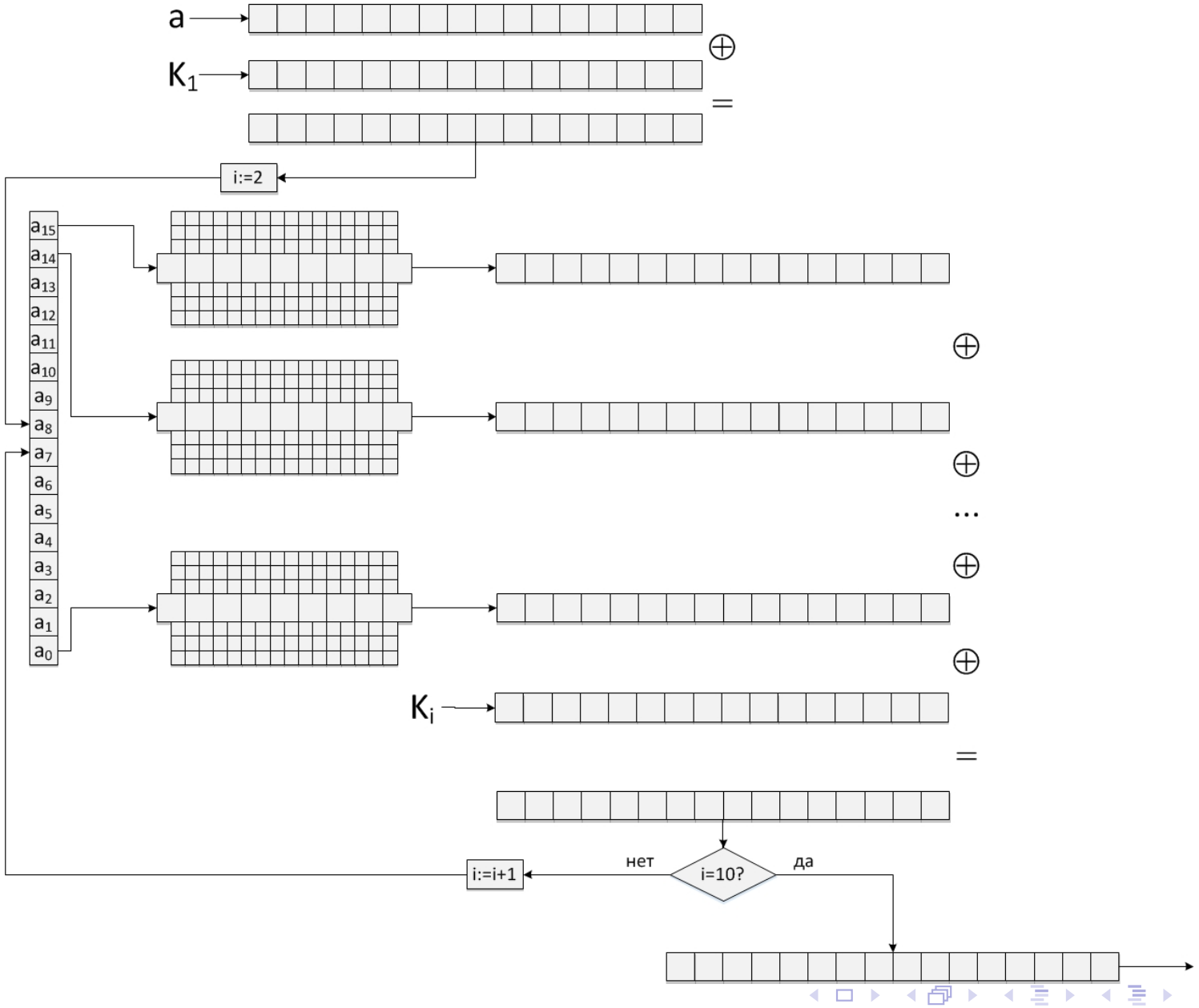


Схема зашифрования ПБШ



Алгоритмы расшифрования ПБШ

Исходный алгоритм расшифрования

$$D_{K_1,\ldots,K_{10}}(a) = X[K_1]S^{-1}L^{-1}X[K_2]\ldots S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a).$$

Заметим, что в силу линейности преобразования L^{-1} для любого $a \in V_{128}$ справедливо соотношение

$$L^{-1}X[K_i]S^{-1}(a) = L^{-1}(S^{-1}(a) \oplus K_i) = L^{-1}(S^{-1}(a)) \oplus L^{-1}(K_i) = \\ = L^{-1}S^{-1}(a) \oplus L^{-1}(K_i) = X[L^{-1}(K_i)]L^{-1}S^{-1}(a).$$

Новый алгоритм расшифрования

$$D_{K_1,\ldots,K_{10}}(a) = X[K_1]S^{-1}X[L^{-1}(K_2)]L^{-1}S^{-1}\ldots \\ \ldots X[L^{-1}(K_9)]L^{-1}S^{-1}X[L^{-1}(K_{10})]L^{-1}S^{-1}S(a).$$

Производительность исследуемых алгоритмов

	Скорость Мбайт/с	Трудоемкость такты/байт	Платформа	Особенности реализации
Стрибог-512				
Казимиров	38	67		
Авторы	92	35	i7-2600 @ 3.4ГГц, Win7	
Лебедев	94	27	i7-920 @ 2.67ГГц	SSE4, ASM
Дегтярев	121	28	i7-2600 @ 3.4ГГц	SSE4
Перспективный блочный шифр				
Зашифрование	125	26	i7-2600 @ 3.4ГГц, Win7	
Расшифрование	105	31	i7-2600 @ 3.4ГГц, Win7	

ЭЦП ГОСТ Р 34.10-2012

Формирование

Шаг 1. Вычислить хэш-код сообщения $\bar{h} = h(M)$.

Шаг 2. Вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить $e = \alpha \pmod{q}$.

Шаг 3. Сгенерировать случайное целое число k.

Шаг 4. Вычислить точку ЭК $C = kP$ и определить $r = x_C \pmod{q}$.

Шаг 5. Вычислить значение $s = (rd + ke) \pmod{q}$.

Шаг 6. Вернуть в качестве подписи $\bar{r}||\bar{s}$.

Проверка

Шаг 1. Вычислить по подписи значения r и s.

Шаг 2. Вычислить хэш-код сообщения $\bar{h} = h(M)$.

Шаг 3. Вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить $e = \alpha \pmod{q}$.

Шаг 4. Вычислить значение $v = e^{-1} \pmod{q}$.

Шаг 5. Вычислить значения $z_1 = sv \pmod{q}$ и $z_2 = -rv \pmod{q}$.

Шаг 6. Вычислить точку ЭК $C = z_1 P + z_2 Q$ и определить $R = x_C (mod\ q)$.

Шаг 7. Проверить равенство $R = r$.

Основные особенности создания высокоскоростной реализации

Операции в простом поле

Нахождение обратного элемента	—Бинарный алгоритм Евклида;
Взятие по модулю	—Алгоритм Баррета, модуль спец. вида $p = 2^n \pm const$;
Умножение	—Умножение "в столбик";
Возведение в квадрат	—Умножение с учетом идентичности аргументов.

Операции в группе точек эллиптической кривой

Переход в не аффинные координаты (координаты Якоби);

Особенности параметров ЭК (например, $a = -3$).

Вычисление кратной точки

w-NAF-представление;

Одновременное вычисление двух кратных точек при проверке подписи;

Предварительный подсчет.

Производительность различных реализаций формирования подписи

Без предварительного подсчета			
Время работы программы (10^{-6}с)		Количество подписей в секунду	
Модуль p специального вида			
146		6849	
Модуль p произвольный			
307		3257	
С предварительным подсчетом			
Модуль p специального вида			
Размер блока (биты)	Память на таблицы (МБ)	Время работы программы(10^{-6}с)	Кол-во подписей в секунду
2	0.03	56	17857
8	0.5	26	38462
19	416	20	50000

Спасибо за внимание!

Список литературы


V.A. Shishkin. Principles of synthesis of prospective block cipher algorithm with a block length of 128 bits(Rus). RusCrypto'2013.


O. Kazymyrov, V. Kazymyrova, Algebraic Aspects of the Russian Hash Standard GOST R 34.11-2012, 2nd Workshop on Current Trends in Cryptology(CTCrypt 2013) June 23-25, 2013,160-176..


P.A. Lebedev. Comparison of old and new cryptographic hash function national standards of Russian Federation on CPUs and NVIDIA GPUs, Mathematical Aspects of Cryptography. 2013. Vol. 4. No. 2. P. 73-80.


https://www.streebog.net/


Brown M. et al. Software implementation of the NIST elliptic curves over prime fields. – Springer Berlin Heidelberg, 2001. – P. 250-265.


Dolmatov, V., Ed., GOST R 34.10-2012: Digital Signature Algorithm, RFC 7091, December, 2013.


Hankerson D., Hernandez J. L., Menezes A. Software implementation of elliptic curve cryptography over binary fields //Cryptographic Hardware and Embedded Systems—CHES 2000. – Springer Berlin Heidelberg, 2000. – P. 1-24.


Bosselaers A., Govaerts R., Vandewalle J. Comparison of three modular reduction functions //Advances in Cryptology—CRYPTO'93. – Springer Berlin Heidelberg, 1994. – P. 175-186.


Johnson M. et al. Modular Reduction of Large Integers Using Classical, Barrett, Montgomery Algorithms.