УДК 681.3.06: 519.248.681

М.Ф. БОНДАРЕНКО, д-р техн. наук, И.Д. ГОРБЕНКО, д-р техн. наук, А.В. ПОТИЙ, канд. техн. наук, О.И. ОЛЕШКО, С.А. ГОЛОВАШИЧ, А.С. БОНДАРЕНКО

УЛУЧШЕННЫЙ СТАНДАРТ СИММЕТРИЧНОГО ШИФРОВАНИЯ XXI ВЕКА: КОНЦЕПЦИЯ СОЗДАНИЯ И СВОЙСТВА КАНДИДАТОВ

Введение

Сегодня в области информационной безопасности решается важная проблема создания улучшенного стандарта симметричного шифрования – криптографического алгоритма XXI века. Ее решение инициировал Национальный Институт Стандартов и Технологий (NIST) США [1, 2]. Для этого в 1997 году NIST объявил конкурс алгоритмов, претендующих на то, чтобы стать стандартом, а также сформировал минимальные требования, которые должны быть выполнены при разработке и представлении на конкурс таких алгоритмов. Предполагается, что в следующем столетии стандарт симметричного шифрования AES (Advanced Encryption Standard) будет описывать общедоступный, распространяемый без ограничений по всему миру симметричный криптоалгоритм, который сможет осуществлять надежную защиту правительственной информации.

Было спланировано три этапа рассмотрения представленных алгоритмов. На первой конференции, посвященной стандарту AES, в 1998 г. вынесено решение о принятии к открытому обсуждению 15 пакетов описаний алгоритмов симметричного шифрования. На втором этапе осуществляется публичный анализ соответствия каждого стандарта требованиям и оценка качества криптографических преобразований в целом. В августе 1999 г. проведена вторая конференция, целью которой было обобщение оценок, полученных государственными организациями и в результате открытого обсуждения, уменьшение количества алгоритмов-кандидатов до 5, которые затем уже будут рассматриваться на третьей конференции в апреле 2000 года. Из всего вышеизложенного вытекает, что NIST рассматривает проблему создания перспективного стандарта шифрования как очень важную, сложную и в значительной степени неопределенную.

Целью этого доклада является изложение концепции создания улучшенного стандарта шифрования, анализ хода и противоречий ее реализации, изложение и обсуждение сформированных требований и ограничений, дополнение и уточнение требований к стандарту, а также проведение сравнительного анализа кандидатов в AES и выбор лучших или лучшего. Кроме того, мы хотим доказать, что приобретенный на сегодня опыт указывает на серьезность проблемы и невозможность ее решения без объединения общих усилий, а главное – использование приобретенного опыта и полученных результатов в интересах Украины.

1. Основные требования.
Основные требования к процедуре представления и свойствам кандидатов AES

Первой конференцией были принятые к дальнейшему рассмотрению только те алгоритмы, на которые были представлены «полные» пакеты документации. «Полные» пакеты должны были содержать:

- сопроводительное письмо;
- описание алгоритма и соответствующую документацию;
- магнитный носитель со всеми материалами;
- заявление о принятии к рассмотрению криптографического алгоритма, включая отказ от прав интеллектуальной собственности на алгоритм.

Полное описание должно было включать в себя все необходимые математические уравнения и выражения, таблицы, диаграммы, обоснование выбора и описание параметров, обоснование

количества циклов и т.п. Некоторые сведения об AES приведены в таблице 1. Криптоалгоритмы проранжированы по эффективности авторами.

Разработчик должен представить свои оценки относительно вычислительной сложности программного и аппаратного обеспечения, а также вычислительную эффективность алгоритма, в том числе и для 8-битовых процессоров. Причем для оценки аппаратного обеспечения рекомендуется использовать в качестве показателя число логических элементов, для программного обеспечения – тип процессора, тактовую частоту его работы, объем памяти, операционную систему, и т.п.

Таблица 1

Наименование алгоритма	Страна	Разработчики
RC6	США	RSA Laboratories (represented by Matthew Robshaw)
MARS	США	IBM (represented by Nevenko Zunic)
Twofish	США	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
Rijndael	Бельгия	Joan Daemen and Vincent Rijmen
CRYPTON	Корея	Future Systems, Inc. (represented by Chae Hoon Lim)
CAST-256	Канада	Entrust Technologies, Inc. (represented by Carlisle Adams)
E2	Япония	Nippon Telegraph and Telephone Corporation (NTT) (represented by Masayuki Kanda)
SERPENT	Великобритания, Израиль, Норвегия	Ross Anderson, Eli Biham, Lars Knudsen
HPC	США	Rich Schroeppel
DFC	Франция	Centre National pour la Recherche Scientifique (CNRS) (represented by Serge Vaudenay)
SAFER+	США	Cylink Corporation (represented by Lily Chen)
LOKI97	Австралия	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
DEAL	США	Richard Outerbridge and Lars Knudsen
FROG	Коста-Рика	TecApro Internacional S.A. (represented by Dianelos Georges Georgoudis)
Magenta	Германия	Deutsche Telekom AG (represented by Klaus Huber)

Оценка скорости работы алгоритма должна быть представлена в виде числа тактов работы, необходимой для:

- шифрования одного блока данных;
- дешифрования одного блока данных;
- разворачивания (настройки) ключа;
- настройки алгоритма или его части (например, формирования таблиц);
- смены ключа для каждой из рабочих длин.

Описание должно содержать все возможные компромиссные варианты, позволяющие выбирать необходимую скорость работы при требуемой устойчивости.

- Для каждого алгоритма должны быть разработаны серии тестов – тесты известных ответов и тесты Монте-Карло.

2. Минимальные требования к кандидатам AES

При создании перспективного стандарта определены и зафиксированы требования к нему. Минимальные требования, которым должны были отвечать на первом этапе алгоритмы-кандидаты AES, таковы:

3.1. Криптоалгоритм должен строиться на использовании криптографии симметричных (секретных) ключей. То есть ключи источника криптограмм и получателя должны или совпадать или рассчитываться один из другого не выше чем с полиномиальной сложностью.

3.2. Криптоалгоритм должен строиться с использованием блочного симметричного шифра с длиной блока $l_б$=128 бит.

3.3. Длины начальных ключей должны быть $l_к$=128, 192 и 256 бит.

3.4. Криптоалгоритм должен работать для различных комбинаций длина сообщения/длина ключа, но обязательно для комбинаций длина блока / длина ключа 128/128, 128/192, 128/256 бит.

3. Критерии и показатели оценки качества

Отбор AES алгоритмов осуществляется с учетом выполнения минимальных требований. Кроме того учитывается:

1. Реальная защищенность от криптоаналитических атак. При этом основными методами криптоанализа являются:
   - дифференциальный криптоанализ;
   - расширения для дифференциального криптоанализа;
   - поиск наилучшей дифференциальной характеристики;
   - линейный криптоанализ;
   - интерполяционное вторжение;
   - вторжение с частичным угадыванием ключа;
   - вторжение с использованием связанного ключа;
   - вторжение на основе обработки сбоев;
   - поиск лазеек.
2. Статистическая безопасность криптографических алгоритмов.
3. Надежность математической базы криптографических алгоритмов.
4. Расчетная сложность криптографических алгоритмов для программной и аппаратной реализаций (может оцениваться скоростью преобразований).
5. Требования к памяти при программной и аппаратной реализациях. При аппаратной реализации оценивается числом логических элементов, при программной – количеством необходимой оперативной и постоянной памяти, в том числе для различных платформ и сред.
6. Гибкость алгоритма, то есть:
   - возможность работы с иными длинами начальных ключей и информационных блоков;
   - безопасность реализации в широком диапазоне различных платформ и приложений, включая 8-битовые процессоры;
   - возможность использования криптографического алгоритма в качестве поточного шифра или генератора псевдослучайных чисел, алгоритма хеширования, для обеспечения подлинности сообщений (выработка кодов аутентификации) и т.п.;
   - одинаковой сложности как аппаратной, так и программной реализации, а также программно-аппаратной реализации.

Анализ основных публикаций относительно исследования свойств алгоритмов-кандидатов AES [3] и полученные авторами результаты позволяют сравнить представленные алгоритмы согласно основным требованиям.

4. Реальная защищенность от криптоаналитических атак

В третьем пункте определены основные методы криптоанализа, которые должны применяться к алгоритмам-кандидатам. Это достаточно сложная проблема. Сегодня необходимо рассматривать и оценивать устойчивость алгоритмов к атакам обычного и расширенного дифференциального криптоанализа, поиска наилучшей дифференциальной характеристики, линейного криптоанализа,

интерполяционного и итерационного вторжения, вторжения с частичным угадыванием ключа и с использованием связанного ключа, вторжения на основе обработки сбоев, поиска лазеек и т.д.

Основные результаты оценки защищенности приведены в таблице 2. В столбце «Блок» указана длина блока, в столбце «Ключ» – длина начального ключа, в столбце «Циклы» – число циклов, реализованных в алгоритме, при которых выполнялся криптоанализ.

В колонке «Тип» указаны типы (условия) атак:

K – наилучшая атака при известном тексте с 2^a парами открытый текст/шифрованный текст, для осуществления которой необходимо 2^b операций шифрования и 2^c слов памяти;

C – наилучшая атака при выборе шифртекста с 2^a парами открытый текст/шифртекст, для осуществления которой необходимо выполнить 2^b операций шифрований и 2^c слов памяти;

? – неизвестна никакая атака, кроме «грубой силы»;

CP – наилучшая атака при выбранном открытом тексте с 2^a парами открытый текст/шифрованный текст, для осуществления которой необходимо выполнить 2^b операций шифрования и 2^c слов памяти;

«–» – означает, что соответствующие значения нам неизвестны.

r – дополнительный параметр

Анализ данных из таблицы 2 показывает, что среди алгоритмов-кандидатов AES (с точки зрения стойкости к атакам криптоанализа) наихудшими являются алгоритмы DEAL, Magenta и Frog. Так, для DEAL при длине блока 128 бит и длине ключа 128 бит существует аналитическая атака при выборе шифртекста, для выполнения которой необходимо 2^{70} пар открытый текст/шифртекст и 2^{72} операций шифрования, что намного меньше, чем при атаке «грубая сила» (2^{128}). Для алгоритма Magenta разработан метод криптоанализа при выборе шифртекста, который требует 2^{64} операций шифрования и 2^{64} пар открытый текст/шифртекст. Для алгоритма Frog разработана атака, которая требует $2^{56,7}$ операций шифрования и 2^{36} пар открытый текст/шифртекст. Указанное исключает алгоритмы DEAL, Magenta и Frog как не обеспечивающие стойкости против аналитических атак, сложность которых намного меньше атаки типа «грубая сила».

Необходимо отметить, что эффективные атаки разработаны также и для существующих и используемых криптоалгоритмов DES, IDEA, Loki(90), Safer(93) и RC5(94). Соответствующие данные приведены в таблице 2.

Таблица 2

Название	Версия	Блок	Ключ	Циклы	Атаки				
					Тип	a	b	c	r
DES	77	64	56	16	K	43	19	13	
	3-DES (77)	64	168	48	K	2	112	56	
	2k3-DES (78)	64	112	4	C	56	56	56	
IDEA	(91)	64	128	8,5	C	56	67	32	3,5
Loki	(90)	64	64	16	C	54	–	–	14
	(91)	64	64	16	C	58	–	–	13
Safer	K(93)	64	64, 128	6, 10	S	45	–	32	5
	SK(95)	64	40, 64, 128	8, 10	?				
Blowfish	(93)	64	32-448	16	?				
RC5	32/12/K (94)	64	8S, S<256	12	C	54	–	–	
	64/16/16(94)	128	8S, S<256	16	C	83	–	–	24
CAST-128	(95)	64	40-128	12, 16	?				
SHARK	(96)	64	128	6	?				
SQUARE	(97)	128	128	8	?				
MISTY	1(97)	64	128	8	?				
	2(97)	64	128	16	?				

Продолжение таблицы 2

ICE	(97)	64	64	16	CP	62	62	30	
Rainbow	(98)	128	128	7	?				
RC6	(98)	128	128, 192, 256						
Mars	(98)	128	128-1248	6					
Twofish	(98)	128	128, 192, 256						
Rinjdael	(98)	128	128, 192, 256						
Crypton	(98)	128	128, 192, 256						
CAST	(98)	128	128, 192, 256						
E2	(98)	128	128, 192, 256						
Serpent	(98)	128	128, 192, 256						
HPC	(98)	128	128, 192, 256						
DFC	(98)	128	128, 192, 256						
Safer	(98)	128	128, 192, 256						
Loki	(98)	128	128, 192, 256						
		128	56	6,8	C	70	72		6
		128	56	6,8	C	32,5	144,5		6
DEAL		192			C	70	136		6
		256			C	32,5	145		6
Magenta		128	128	6	C	64	64		2
		128	128	6	C	33	97		2
		128	192	6	C	128	128		2
		128	192	6	C	33	161		2
		128	256	6	C	128	192		2
		128	256	6	C	33	225		2
FROG		128	128			58			
		128				56			
		128	192			64			
		128	256			36	56,7		

5. Статистическая безопасность криптографических алгоритмов

Основными методами определения статистической безопасности криптографических алгоритмов являются методы, связанные с расчетом связанности (корреляции блоков) криптограмм между собой и со входными блоками открытых текстов, а также определение избыточности криптограмм. Избыточность связана с зависимостью символов сообщений соответствующего алфавита и неодинаковой вероятностью их появления.

Пусть M_1, M_2, ..., M_i, ..., M_n - входные блоки открытого текста, а C_1, C_2, ..., C_i, ..., C_n - блоки криптограмм, полученные при применении ключа K. Символы M_i и C_i являются двоичными, то есть принимают значения (0,1). Связанность Mi и Ci определим функцией:

$$F_1 = f(M_i, C_i) = \sum_{j=1}^{l_d} M_i \oplus C_i , \qquad (1)$$

а C_i и C_k

$$F_2 = f(C_i, C_k) = \sum_{j=1}^{l_d} C_i \oplus C_k . \qquad (2)$$

Будем рассматривать значения F_1 и F_2 как случайные числа. Обрабатывая случайные последовательности F_1 и F_2, например вычислением математического ожидания

$m(F_1)$ и $m(F_2)$

и соответствующих моментов

$$m^s(F_1) \text{ и } m^s(F_2),$$

получим количественные показатели зависимости и связанности M_i и C_i, C_i и C_k.

В дальнейшем будем предполагать M_i и C_i, C_i и C_k независимыми (некоррелированными), если

$$F_1 = {}^{l_á}\!/_2 \text{ и } F_2 = {}^{l_á}\!/_2$$

соответственно.

Оценка статистической безопасности для всех AES кандидатов проведена при следующих начальных данных:

1. случайный ключ, случайные данные, ключ постоянный
2. единичный ключ, случайные данные, ключ постоянный
3. случайный ключ, единичные данные, ключ постоянный
4. случайный ключ, нулевые данные, ключ изменяется
5. случайный ключ, случайные данные, ключ изменяется

В процессе оценки F_2 рассчитывалось на основе C_i и C_k, причем M_i и M_k, для блоков криптограмм, отличаются на один бит.

В таблице 3 приведены значения $m(F_1)$, $m(F_2)$, $m^2(F_i)$, $m^2(F_2)$, а также max F_1, max F_2 и min F_1, min F_2, которые рассчитывались на выборке размера n (n = 5000). В таблице 3 оценкой для математического ожидания служит среднее арифметическое наблюдаемых значений случайных величин F_1 и F_2 в n независимых наблюдениях.

Приведенные в таблице 3 некоторые данные подтвердили вывод о том, что все кандидаты AES обеспечивают статистическую безопасность криптографических преобразований. Вместе с тем, значения $m^2(F_1) = 30.75$, $m^2(F_2) = 30.81$ для Twofish, $m^2(F_1) = 30.67$, $m^2(F_2) = 33.47$ для Rijndael, $m^2(F_1) = 30.86$ для DEAL, $m^2(F_2) = 33.64$ для FROG, $m^2(F_2) = 30.19$ для Magenta позволяют сделать вывод о необходимости проведения дополнительных исследований для названных алгоритмов.

Таблица 3

Название AES	$m(F_1)$	$m^2(F_1)$	min F_1	max F_1	$m(F_2)$	$m^2(F_2)$	min F_2	max F_2	Вариант
RC6	63,87	32,27	45	84	64,20	32,96	41	85	5.1
	64,11	31,97	45	88	64,02	32,09	41	86	5.2
	63,97	32,62	45	88	63,98	31,61	41	86	5.3
	63,94	31,87	43	88	63,95	32,28	41	86	5.4
	64,20	32,21	43	89	64,04	31,41	41	86	5.5
Mars	63,95	31,28	43	84	64,06	31,85	45	87	5.1
	64,08	32,28	43	84	63,99	31,81	41	87	5.2
	63,98	33,27	38	86	64,04	31,15	41	87	5.3
	64,04	31,41	38	86	64,02	32,33	41	87	5.4
	63,94	31,77	38	86	64,10	32,82	41	87	5.5
Twofish	64,05	31,97	42	84	64,01	32,35	46	86	5.1
	64,06	30,75	42	84	64,01	30,81	42	86	5.2
	64,21	32,74	40	85	63,91	32,30	40	86	5.3
	64,01	31,52	40	85	64,18	31,52	40	86	5.4
	63,90	31,89	40	85	63,88	32,06	40	86	5.5
Rijndael	64,16	32,25	44	90	63,95	32,12	44	85	5.1
	63,79	31,86	39	90	64,03	31,07	44	85	5.2
	63,99	32,40	39	90	63,97	32,30	42	86	5.3
	63,98	33,47	39	90	64,05	31,92	42	86	5.4
	63,88	31,70	39	90	64,00	30,67	42	86	5.5

	64,17	32,45	45	85	64,14	32,87	44	84	5.1
	63,94	31,63	40	86	64,05	33,04	41	84	5.2
Crypton	63,96	31,88	40	86	63,91	32,84	41	86	5.3
	63,93	32,35	40	88	63,97	31,42	41	86	5.4
	64,01	32,02	40	88	64,01	32,45	40	86	5.5
	63,99	32,49	46	83	63,98	32,48	44	85	5.1
	64,09	31,29	45	86	64,17	32,96	43	85	5.2
DEAL	63,83	31,73	43	86	63,92	31,80	43	85	5.3
	63,94	30,86	41	86	64,07	32,55	43	85	5.4
	64,00	31,42	41	86	63,99	32,26	43	85	5.5
	64,04	32,42	42	87	64,09	33,64	42	86	5.1
	64,02	31,92	42	87	64,09	32,20	42	86	5.2
Frog	64,01	31,52	42	87	64,19	31,34	42	86	5.3
	64,06	31,72	42	88	64,04	31,08	42	86	5.4
	64,07	31,53	42	88	63,87	31,52	42	86	5.5
	63,92	31,10	42	82	63,93	32,82	45	84	5.1
	64,01	31,60	42	86	64,08	32,16	44	85	5.2
Magenta	64,05	32,61	42	86	64,04	32,20	43	86	5.3
	64,12	30,19	42	86	64,07	31,91	43	86	5.4
	64,01	31,92	42	86	63,94	32,35	43	86	5.5

Существование избыточности в зашифрованных текстах исследовалось с использованием программы -архиватора RAR. В качестве входных текстов использовались:

DLL - исполняемый файл WINDOWS;

DOC - документы Microsoft WORD 6.0;

EXE - исполняемый файл MS-DOS;

PDF - документ переносимого формата;

TXT - обычный текст ASCII;

ZIP - файл - архив.

В качестве показателей сжатия при оценке кандидатов в AES использовались:

$$k_1 = \frac{l'_m}{l_m} \tag{3}$$

и

$$k_2 = \frac{l'_c}{l_m}, \tag{4}$$

где

l'_m - длина сжатого открытого текста;

l_m - длина входного открытого текста;

l'_c - длина сжатой криптограммы.

В таблице 4 в качестве примеров приведены значения k_1 и k_2 для RC6 и Magenta. Длина входного открытого текста $l_m=10^6$ байт. Шифрование осуществлялось в блочном режиме.

Таблица 4

Тип AES	Тип файла	l'_m	l'_c	k_1	k_2
RC6	DLL	463802	959901	0.464	0.960
	DOC	187578	608472	0.188	0.608
	EXE	387178	859101	0.387	0.859
	PDF	891286	961224	0.891	0.961
	TXT	290310	948754	0.290	0.949
	ZIP	1000154	1000060	1.000154	1.000060
Magenta	DLL	463802	916490	0.464	0.916
	DOC	187578	533263	0.188	0.533
	EXE	387178	809533	0.387	0.809
	PDF	891286	959658	0.891	0.960
	TXT	290310	880921	0.290	0.881
	ZIP	1000154	1000060	1.000154	1.000060

Проведенные исследования по определению k_2 для всех AES кандидатов и приведенные в таблице 4 данные для RC6 и Magenta свидетельствуют о том, что алгоритм Magenta хуже чем остальные алгоритмы. Худшим по k_2 является также и алгоритм DEAL..

Все AES кандидаты исследовались на способность сжатия криптограмм, полученных в поточном режиме. Сжатию такие криптограммы не поддаются. Результаты по k_2 близки по значениям к результатам, полученным для ZIP-файлов.

Таким образом, исследование коэффициента сжатия k_2 для AES кандидатов позволяет сделать вывод о том, что алгоритмы Magenta и DEAL относятся к «плохим» и могут быть отклонены.

6. Вычислительная сложность развертывания ключа и криптографических преобразований

В большинстве AES криптоалгоритмов рабочие ключи K_p, то есть ключи, которые используются для прямых и обратных криптографических преобразований, создаются на основе развертывания начальных $K_п$ ключей, причем

$$K_p = F_p\left(K_n, I_{AES}\right),$$

где

F_p - является функцией развертывания ключа;

$K_п$ - значение рабочего ключа;

I_{AES} - вектор - параметр функции развертывания ключа.

Анализ показал, что для большинства AES кандидатов скорость (сложность) развертывания ключа и прямых и обратных преобразований не зависит от длины ключа. Это означает, что время развертывания ключа и шифрования/дешифрования блока данных является одинаковым, независимо от длины ключа – 128, 192 или 256 бит. Девять криптоалгоритмов – RC6, MARS, CRYPTON, CAST, E2, SERPENT, HPC, DFC, FROG – являются совсем не зависящими от длины ключа. Сложность шифрования/дешифрования для алгоритмов LOKI и Twofish не зависит от длины ключа, а сложность развертывания ключа зависит от длины ключа. Причем сложность развертывания ключа для Twofish возрастает при увеличении длины ключа, а для LOKI97 наоборот - уменьшается. В алгоритмах DEAL, Magenta, Rijndael и SAFER+ сложность (скорость) шифрования/дешифрования зависит от длины ключа, это связано с разным числом циклов, выполняемых при криптографических преобразованиях.

Проведенные измерения показали, что алгоритмы DEAL и Magenta при длине ключа 128 и 192 бита выполняют криптографические преобразования на 0.33 (а Rijndael – на 0.4) медленнее, чем при

длине 256 битов. Алгоритм SAFER в два раза медленнее при длине ключа 256 битов и на 0.5 при длине ключа 192 бита.

В таблице 5 приведены результаты оценки сложности разворачивания ключа и шифрования/дешифрования в зависимости от длины ключа. Сложность оценивается количеством тактов работы компьютера.

Таблица 5

Крипто-алго-ритм	Развертывание ключа, тактов			Шифрование, тактов			Дешифрование, тактов			Ср. ско-рость,	Мин. число
	128	192	256	128	192	256	128	192	256	М бит/с.	циклов
RC6	1682	1878	1778	270	269	269	231	230	230	102.2	20
MARS	4311	4375	4344	376	376	376	370	370	370	68.6	10
Twofish	14707	20868	26438	381	381	379	379	379	384	67.4	12
Rijndael	2066	2418	2937	436	510	592	429	498	579	59.2	8
Crypton	1269	1291	1343	476	477	473	476	479	479	53.8	11?
CAST	4344	4330	4313	632	632	632	632	632	632	40.5	10
E2	9508	9531	9596	691	689	702	701	698	701	36.8	10
Serpent	2404	2365	2350	950	950	951	895	895	895	27.8	17
HPC	120631	120695	120658	1418	1418	1418	1607	1607	1591	16.9	8?
DFC	7126	6845	6929	1699	1643	1693	1668	1616	1644	15.2	9
SAFER	4278	7426	11310	1720	2553	3391	1721	2536	3374	14.9	7
LOKI	7407	7288	7147	2141	2133	2133	2187	2177	2177	11.8	>36
DEAL	8632	8647	11724	2362	2354	3093	2371	2370	3110	10.8	6
FROG	13802	14155	14107	2521	2515	2392	2282	2190	2288	10.7	8?
Magenta	31	26	36	6552	6535	8703	6550	6549	8715	3.9	>10

Данные, приведенные в таблице 5, подтверждают вывод, что первые семь криптоалгоритмов являются лучшими кандидатами в AES стандарт по сложности (скорости) прямых и обратных криптографических преобразований. Граничной мы выбрали скорость 30 Мбит/с.

Согласно требованиям к криптоалгоритму, он должен применяться и в качестве функции хеширования. Поэтому для оценки эффективности криптоалгоритма в целом необходимо давать оценки сложности хеширования, при условии, что выработка MAC (КАС) осуществляется с использованием соответствующего алгоритма. В таблице 6 приведены соответствующие данные в виде числа тактов (циклов), которые необходимо выполнить для развертывания ключа и выполнения прямого и обратного преобразований.

Таблица 6

Название криптоалгоритма	RC6	MARS	Twofish	Rijndael	CRYPTON	E2	SERPENT
Pentium	146	260	175	34	49	100	205
Pentium PRO	118	246	132	32	46	100	193

Результаты, приведенные в таблице 6, позволяют сделать вывод, что лучшими являются алгоритмы Rijndael и CRYPTON, удовлетворительными E2, RC6 и Twofish.

По сравнению со стандартными функциями хеширования, например SHA, все AES имеют большую сложность. Например SHA требует всего 13 тактов на байт.

7. Некоторые итоги второй конференции

В августе 1999 года состоялся второй раунд обсуждения кандидатов в стандарт 21 века. По результатам работы конференции принято решение оставить 5 кандидатов в AES из 15. Это криптоалгоритмы RC6, MARS, Twofish, Rijndael и Serpent. Как следует из таблицы 1 первые четыре криптоалгоритма, выделенные нами, совпали с выделенными на конференции. По результатам работы конференции на пятое место вышел алгоритм Serpent. По нашей классификации он находится на 8 месте. Дело в том, что в процессе обсуждения, разработчики изменили параметры алгоритма, уменьшив число циклов в 2 раза, что позволило повысить производительность (скорость) шифрования/дешифрования. Благодаря этому алгоритм переместился на пятое место и вошел в число претендентов в стандарт.

На наш взгляд основная борьба среди кандидатов в AES развернется между RC6, MARS и Twofish. Дело в том, что в качестве дополнительных требований, предъявленных к криптоалгоритмам, должны быть требования случайности, равновероятности и независимости развернутых ключей. Им в большей мере отвечают RC6, MARS и Twofish.

Список литературы: 1. *Announcing* Development of Federal Information Processing Standard for Advanced Encryption Standard. – Federal Register. Vol. 62, № 1, 1997, pp.93-94. **2.** *Announcing* Request for Candidate Algorithm Nomination for Advanced Encryption Standard (AES). – Federal Register. Vol. 62, №177, 1997, pp.48051-48058. 3.http://www.nist.gov/aes

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 21.03.2000