УДК 519.713

А.В. НЕЙВАНОВ, И.Д. ГОРБЕНКО

Харьковский национальный университет радиоэлектроники, Украина

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АППАРАТНЫХ ПОТОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ ПОБЕДИТЕЛЕЙ ПРОЕКТА ESTREAM

Данная работа посвящается современным достижениям в области криптографической защиты информации. В частности, перспективным на данный момент времени аппаратным поточным симметричным шифрам. Рассматриваются аппаратные поточные симметричные шифры (ПСШ) проекта eSTREAM. Изучаются их характеристики и свойства, изложенные в открытых публикациях. Обосновываются и выбираются критерии и показатели оценки свойств аппаратных ПСШ. Предлагается методика принятия решений на множестве альтернативных вариантов аппаратных ПСШ, которая позволяет сравнить аппаратные ПСШ проекта eSTREAM.

Ключевые слова: *аппаратные поточные симметричные шифры, аппаратные модули, безусловные и условные критерии оценки, нечеткие множества, защита информации.*

Введение

После более чем трех лет проект eSTREAM закончен. На электронном ресурсе проекта [1 – 11] представлены финальные статьи, которые содержат описанные и ряд оценок лучших аппаратных ПСШ и некоторые результаты открытых расчетов. Основной целью проекта eSTREAM была стимуляция работы в области поточных симметричных шифров, прежде всего в части разработки ПСШ. Составлен перечень ПСШ, которые прошли все три этапа конкурса. Наиболее стойкие из них могут быть рассмотрены как кандидаты на международные стандарты. Целью настоящей статьи является анализ аппаратных ПСШ проекта eSTREAM и разработка рекомендаций по выбору лучших по совокупности безусловных и условных критериев.

1. Оценка устойчивости аппаратных поточных симметричных шифров

Оценка и сравнительный анализ алгоритмов ПСШ осуществляется с использованием безусловных и условных критериев на основе теории нечетких множеств[1-2]. Будем использовать показатель, который может быть представлен как

$$D = C_1^{\beta_1} \cap C_2^{\beta_2} \cap ... \cap C_n^{\beta_n}, \qquad (1)$$

где C_i – числовые значения частных критериев обобщенного условного критерия, которые полученные методом экспертной оценки и представлены нечеткими множествами;

β_i – весовой коэффициент i-го критерия, полученный с помощью матрицы парных сравнений.

В целом выбор алгоритма шифрования предлагается осуществлять в такой последовательности [1 – 2].

1. Определяются числовые значения показателей $К_{б1}$, $К_{б2}$, $К_{б3}$, $К_{б4}$, $К_{б5}$, $К_{б6}$, входящих в безусловную функцию $f_{бк}(A_i)$.

2. Определяются значения функций $f_{бк}(A_i)$. Если $f_{бк}(A_i)$ i-того алгоритма принимает значение "1", то соответствующий алгоритм удовлетворяет безусловному обобщенному критерию. Об этом также свидетельствует значение функции = "1" (истина).

3. Для алгоритмов, удовлетворяющих обобщенному безусловному критерию, то есть $f_{бк}(A_i) = 1$, согласно частичных условных критериев вычисляются значения частичных условных показателей $К_{у1}$, $К_{у2}$, $К_{у3}$, $К_{у4}$ и $К_{у5}$.

4. Для каждого из альтернативных кандидатов исчисляется значение обобщенного условного показателя $К_{у.}$.

5. В заключение, на основе сравнения значений обобщенных условных показателей $К_{у}$, относительно рассматриваемых ПСШ делается вывод о предпочтении того или иного шифра над другими.

2. Методика и результаты оценки ПСШ за безусловными критериями

2.1 Сравнительный анализ алгоритмов шифрования за безусловными критериями

В табл. 1 представлены показатели скорости процедуры генерации ключевого потока в Мбит/сек, которые были взяты из [3 – 11].

Таблица 1

Показатели скорости процедуры генерации ключевого потока

Название шифра	Генерация ключевого потока (Мбит/сек)	Процессоры, микроконтроллеры и ПЛИС, на которых достигалась указанная скорость	Место	$К_{б6}$
Trivium	954	Intel Xeon CPU 1.5 GHz	2	1
Grain v1	3136	ALTERA Cyclone EP1C3T100C6	1	1
F-FCSR-H v2	298	Pentium 4 3.2 GHz	4	1
MICKEY v2	25	Pentium 4 3.4 GHz	5	1
Decim v2	0.7	Intel Xeon CPU 2.83 GHz	8	0
Edon80	3.6	Virtex4, 286 MHz	7	0
Pomaranch v3	16	Pentium 4 2.8 GHz	6	1
Moustique	380	Virtex-II 2V80FG256	3	1

В таблице шифры, которые являются худшими по скорости, получают $К_{б6} = 0$. Для остальных – $К_{б6} = 1$.

Итоговые значения безусловных показателей $К_{б1}$-$К_{б6}$ приведены в табл. 2.

Таблица 2

Итоговые значения безусловных показателей

Название шифра	$К_{б1}$	$К_{б2}$	$К_{б3}$	$К_{б4}$	$К_{б5}$	$К_{б6}$
Trivium	1	1	1	1	1	1
Grain v1	1	1	1	1	1	1
F-FCSR-H v2	0	1	1	1	1	1
MICKEY v2	1	1	1	1	1	1
Decim v2	0	1	1	1	1	0
Edon80	0	1	1	1	1	0
Pomaranch v3	0	1	1	1	1	1
Moustique	0	1	1	1	1	1

Из этой таблицы видно, что рассматривать условные критерии следует лишь для трех шифров – Trivium, Grain v1 и MICKEY v2.

2.2 Сравнительный анализ алгоритмов шифрования с условными критериями.

Первым условным критерием является частичный критерий оценки возможностей и условий распространения соответствующего алгоритма ПСШ. По этому критерию предлагается оценивать:

– условия разработки и исследования, наличие ограничений уже на этом этапе;

– отсутствие ограничений на экспорт;

– отсутствие ограничений на импорт;

– необходимость получения лицензии на использование алгоритма;

– наличие контроля за применением и обязательность отчетов;

– наличие ограничений на экспорт средств, реализующих алгоритм;

– наличие патентов на алгоритм и его составляющие.

Значения этих показателей определены на основе изучения нормативно-правовых актов, действующих на международном и национальном уровнях. На основе описанных выше показателей методом экспертных оценок устанавливаются преимущества того или иного претендента в виде весовых коэффициентов частного критерия

$$К_{у1} = \sum W_i, \qquad (2)$$

где W_i – числовые значения усредненных экспертных оценок (весового коэффициента) для каждого из ПСШ.

– Необходимо заметить, что алгоритмы Trivium, Grain v1 и MICKEY v2 являются открытыми для некоммерческого использования. В табл. 3 приведены результаты оценки по частному условному критерию распространения алгоритма. Всего по этому критерию будем использовать 7 показателей Wi, которые приведены выше.

Таблица 3

Результаты оценки по частному условному критерию распространения алгоритма

Показатели / Алгоритмы	W_1	W_2	W_3	W_4	W_5	W_6	W_7	$К_{у1}$
Trivium	2	2	2	2	2	2	2	14
Grain v	0	1	1	1	2	1	2	8
MICKEY v	2	2	2	2	2	2	2	14

Каждый из показателей может принимать три значения:

– 0 – есть ограничения;

– 1 – не определено;

2 – разрешено или не ограничено.

Критерий уровня доверия алгоритмов шифрования будем определять по сумме W_{21}, W_{22} , W_{23} (средние экспертные оценки) третьего частного условного критерия K_{y2}:

$$K_{y2} = W_{21} + W_{22} + W_{23}, \qquad (3)$$

где W_{21} – оценка степени открытости правил проектирования и прозрачности используемых методов;

W_{22} – достаточность количества и авторитет числа независимых исследователей, которые анализируют устойчивость и свойства шифра;

W_{23} – оценка отсутствия подозрений на наличие уязвимостей.

В табл. 4 приведены значения показателя K_{y2} и его составляющих W_{21}, W_{22} і W_{23}.

Оценка сделана, как и выше, по трехбальной системе $W_{3i} \in \{0, 1, 2\}$.

Таблица 4

Значения показателя K_{y2} и его составляющих

Показатели / Алгоритмы	W_{21}	W_{22}	W_{23}	K_{y2}
Trivium	1	1	1	3
Grain v1	1	1	1	3
MICKEY v2	1	1	1	3

Оценка перспективности применения алгоритма шифрования сделана с использованием частного условного критерия K_{y3} и соответствующих показателей W_{3i}:

$$K_{y3} = W_{31} + W_{32} + W_{33} + W_{34}, \qquad (4)$$

где W_{31} – числовое значение (вес) экспертной оценки о преимуществе шифра на основе сведений о его использовании в качестве международного стандарта (стандартов) и/или национального стандарта (стандартов);

W_{32} – числовое значение экспертной оценки показателя, который учитывает степень распространенности алгоритма;

W_{33} – числовое значение экспертной оценки существования (отсутствия) подозрений на теоретическую возможность осуществления крипто аналитической атаки и ее угрозы;

W_{34} – числовое значение экспертной оценки возможности применения ПСШ в перспективных информационных технологиях.

Оценка сделана по трехбальной системе показателей.

В табл. 5 приведены значения показателей и частного критерия K_{y3}.

Таблица 5

Значения показателей и частного критерия K_{y3}

Показатели / Алгоритмы	W_{31}	W_{32}	W_{33}	W_{34}	K_{y3}
Trivium	1	1	1	1	4
Grain v1	1	1	1	1	4
MICKEY v2	1	1	1	1	4

Оценка временной и пространственной сложности, программной, аппаратной и аппаратно-программной реализаций прямого и обратного преобразований выполнена с использованием частного критерия K_{y4}:

$$K_{y4} = W_{41} + W_{42} + W_{43} + W_{44}, \qquad (5)$$

где W_{41} – числовое значение экспертной оценки показателя сложности прямого криптографического преобразования;

W_{42} – числовое значение экспертной оценки показателя сложности обратного криптографического преобразования;

W_{43} – числовое значение экспертной оценки пространственной сложности;

W_{44} – числовое значение экспертной оценки размера исходного кода реализации (реализаций).

При оценке использовались результаты исследований, которые приведены в 3.1. Результаты оценки приведены в табл. 6. Оценка выполнена по трехбальной системе.

Таблица 6

Результаты оценки по критерию K_{y4}

Показатели / Алгоритмы	W_{41}	W_{42}	W_{43}	W_{44}	K_{y4}
Trivium	1	1	1	1	4
Grain v1	2	2	1	1	6
MICKEY v2	0	0	0	1	1

Анализ показателя K_{y4} показывает, что алгоритмы шифрования по этому показателю находятся в такой последовательности – Grain v1, Trivium и MICKEY v2.

Оценка степени гибкости осуществлялась согласно критерию K_{y5}:

$$K_{y5} = W_{51} + W_{52} + W_{53} + W_{54}, + W_{55}\ , \qquad (6)$$

где W_{51} – числовое значение экспертной оценки, которая отображает возможности изменения длины ключа;

W_{52} – числовое значение экспертной оценки возможности реализации на разных программных платформах;

W_{53} – числовое значение экспертной оценки возможности аппаратной реализации;

W_{54} – возможность использования для реализации криптографических протоколов.

Результаты оценки сведены в табл. 7.

Таблица 7

Результаты оценки по критерию K_{y5}

Показатели / Алгоритмы	W_{51}	W_{52}	W_{53}	W_{54}	K_{y5}
Trivium	1	2	2	2	7
Grain v1	2	0	2	2	6
MICKEY v2	2	0	2	2	6

Из табл. 7 следует, что алгоритмы шифрования по этому показателю находятся в такой последовательности Trivium, Grain v1 и MICKEY v2.

Теперь методом экспертной оценки для каждого из рассмотренных алгоритмов шифрования для каждого критерия определяем нечеткие множества [1-2]:

$$\mu_{K_{y1}} = \{1/14 + 0{,}7/8 + 0{,}6/14\};$$

$$\mu_{K_{y2}} = \{0{,}8/3 + 0{,}6/3 + 0{,}5/3\};$$

$$\mu_{K_{y3}} = \{0{,}7/4 + 0{,}5/4 + 0{,}3/4\};$$

$$\mu_{K_{y4}} = \{0{,}9/4 + 0{,}8/6 + 0{,}8/1\}; \qquad (7)$$

$$\mu_{K_{y5}} = \{0{,}5/7 + 0{,}5/6 + 0{,}4/6\};$$

Эта запись понимается так: для каждого частичного условного критерия полученные значения K_{y1}-K_{y5} – (табл. 3 – 7) преобразуются в нечеткие множества посредством свертки (1).

В нашем случае все частичные условные критерии K_{y1}-K_{y5} при выборе наиболее лучшего варианта имеют разную значимость. В связи с этим необходимо определить весовые коэффициенты β_i этих критериев. Один из возможных способов получения значений весовых коэффициентов заключается в построении матрицы парных сравнений критериев. Для частных условных критериев имеем соответствующую таблицу.

Таблица 8

Частные условные критерии

Условные критерии	K_{y1}	K_{y2}	K_{y3}	K_{y4}	K_{y5}
K_{y1}	1	1	3	1/3	3
K_{y2}	1	1	3	1/5	3
K_{y3}	1/3	1/3	1	1/5	3
K_{y4}	3	5	5	1	3
K_{y5}	1/3	3	1/3	1/3	1

Весовой коэффициент критериев β_i определяются на основании вычисленных значений правого частичного вектора матрицы парных сравнений α_i с последующим умножением на число критериев n

$$\beta_i = \alpha_i n, \qquad (8)$$

Значения α_i і β_i приведены в табл. 9.

Таблица 9

Собственный вектор матрицы парных сравнений критериев и их весовые коэффициенты

	K_{y1}	K_{y2}	K_{y3}	K_{y4}	K_{y5}
Значения α_i	0,19	0,172	0,089	0,451	0,098
Значения β_i	0,95	0,86	0,445	2,255	0,49

Множество оптимальных альтернатив D с учетом различной важности критериев эффективности определяется путем пересечения нечетких множеств согласно (1).

Найдем множество оптимальных альтернатив с учетом полученных весовых критериев по формуле (1):

$$D = \{ \min \{ 1{,}0^{0{,}95}; 0{,}8^{0{,}86}; 0{,}7^{0{,}445}; 0{,}9^{2{,}255}; 0{,}5^{0{,}49}\},$$

$$\min \{ 0{,}7^{0{,}95}; 0{,}6^{0{,}86}; 0{,}5^{0{,}445}; 0{,}8^{2{,}255}; 0{,}5^{0{,}49}\}, \qquad (9)$$

$$\min \{ 0{,}6^{0{,}95}; 0{,}5^{0{,}86}; 0{,}3^{0{,}445}; 0{,}8^{2{,}255}; 0{,}4^{0{,}49}\}\}$$

Свертка множества оптимальных вариантов для алгоритмов Trivium, MICKEY v2 и Grain v1 соответственно имеет вид:

1. По методу минимума:

$$\max_j \mu_D(a_j) = \max\{0{,}712; 0{,}217; 0{,}585\}; \qquad (10)$$

2. С учетом взвешенной оценки всех критериев:

$$\max_j \mu_D(a_j) = \max\{0,358; 0,035; 0,066\}. \quad (11)$$

Таким образом, предложенная методика позволяет провести сравнительный анализ перспективных алгоритмов шифрования.

В табл. 10 приведены значения безусловного и условного критериев оценки алгоритмов шифрования.

Таблица 10

Результаты сравнительного анализа перспективных аппаратных ПСШ

Критерии \ Алгоритмы		Trivium	MICKEY v2	Grain v1
Безусловный $K_б$		1	1	1
Условный $K_у$	Метод минимума	0,712	0,605	0,585
	Учет всех критериев	0,395	0,145	0,077

Выводы

Анализ данных табл. 10 позволяет сделать вывод, что лучшим является алгоритм Trivium. На втором месте находится алгоритм ПСШ MICKEY v2, на третьем – Grain v1. Поэтому, на наш взгляд, можно сделать вывод о том, что в Украине для решения задач обеспечения конфиденциальности информации сегодня целесообразно рекомендовать к использованию алгоритм поточного симметричного шифрования Trivium.

Trivium является одной из успешнейших конструкций проекта eSTREAM.

Данный аппаратный ПСШ не был подвержен каким-либо модификациям или дополнением. Его спецификация остается неизменной по настоящий момент.

Шифр пережил все три этапа проекта и не на одном из них не был подвергнут успешным крипто аналитическим атакам.

Кроме того, алгоритм Trivium, очень хорошо реализуется на новых микроконтроллерах и ПЛИС, а также на процессорах семейства Intel.

Литература

1. Горбенко І.Д. Аналіз властивостей алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE) / І.Д. Горбенко, Г.М. Гулак, Р.В. Олійников, В.І. Руженцев, М.С. Михаленко // Радіотехніка. – 2005. – №141.

2. Горбенко І.Д. Порівняльний аналіз алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE) / І.Д. Горбенко та ін. // Радіотехніка. – 2005. – №141.

3. De Canniere C. Trivium Specifications / C. De Canniere, B. Preneel [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/.

4. Hell M. Grain – A Stream Cipher for Constrained Environments / M. Hell, T. Johansson, W. Meier [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.cr.yp.to/.

5. Arnault F. Update on F-FCSR Stream Cipher / F. Arnault, T.P. Berger, C. Lauradoux [Электрон. ресурс]. – Режим доступа к ресурсу: http://www. citeseerx.ist.psu.edu/.

6. Babbage S. The stream cipher MICKEY 2.0 / S. Babbage, M. Dodd [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/.

7. Berbain C. DECIMv2 / C. Berbain et al. [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/.

8. Kasper M. A Compact Implementation of Edon80 / M. Kasper, S. Kumar, K. Lemke-Rust, C. Paar [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/.

9. Jansen C.J.A. Cascade Jump Controlled Sequence Generator and Pomaranch Stream Cipher / C.J.A. Jansen, T. Helleseth, A. Kholosha [Электрон. ресурс]. – Режим доступа к ресурсу: http:// www.ecrypt.eu.org/.

10. Daemen J. The self-synchronizing stream cipher Moustique // J. Daemen, P. Kitsos [Электрон. ресурс]. – Режим доступа к ресурсу: http://www. citeseerx.ist.psu.edu/.

11. Bernstein D.J. Which eSTREAM ciphers have been broken? / D.J. Bernstein [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/ stream/papers.html.

Поступила в редакцию 25.01.2010

Рецензент: д-р техн. наук А.В Потий, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

ПОРІВНЯЛЬНИЙ АНАЛІЗ АПАРАТНИХ ПОТОКОВИХ СИМЕТРИЧНИХ ШИФРІВ ПЕРЕМОЖЦІВ ПРОЕКТУ ESTREAM

А.В. Нейванов, І.Д. Горбенко

Дана робота присвячується сучасним досягненням в області криптографічного захисту інформації. Зокрема, перспективним на даний момент часу апаратним потоковим симетричним шифрам. Розглядаються апаратні потокові симетричні шифри (ПСШ) проекту eSTREAM. Вивчаються їх характеристики та властивості, викладені у відкритих публікаціях. Обґрунтовуються та вибираються критерії та показники оцінки властивостей апаратних ПСШ. Пропонується методика прийняття рішень на множині альтернативних варіантів апаратних ПСШ, яка дозволяє порівняти апаратні ПСШ проекту eSTREAM.

Ключові слова: Апаратні потокові симетричні шифри, апаратні модулі, безумовні та умовні критерії оцінки, нечіткі множини, захист інформації.

COMPERATIVE ANALISIS OF HARDWARE STREAM SYMMETRIC CIPHERS WINERS OF ESTREAM

A.V. Neyvanov, I.D. Gorbenko

This work is dedicated to latest developments in the field of cryptographic information security. In particular, a perspective at this point in time hardware stream symmetric ciphers. We consider hardware stream symmetric ciphers (SSC) of project eSTREAM. Learn their characteristics and properties set in open publications. Basing and selecting criteria and indicators to evaluate the property of hardware SSC. Describe the method of decision-making on the set of alternatives of hardware SSC, which leave compare hardware SSC of project eSTREAM.

Key words: Hardware stream symmetric ciphers, hardware modules, unconditional and conditional criteria of evaluate, fuzzy sets, information security.

Нейванов Андрей Викторович – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Харьков, Украина, e-mail: andrey.neyvanov@gmail.com.

Горбенко Иван Дмитриевич – д-р техн. наук, проф., зав. кафедрой безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина, e-mail: gorbenko@kture.kharkov.ua.