УДК 621.391.7:336.71(075.8)

МЕТОДИКА СРАВНЕНИЯ АЛГОРИТМОВ ЭЦП В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

М.Ф. БОНДАРЕНКО, Б.И. ДЕНИСЕНКО, Ю.И. ГОРБЕНКО

Данная статья посвящена решению задачи сравнения алгоритмов ЭЦП, основанных на преобразованиях в группе точек на эллиптической кривой. Нахождение такой методики является актуальной задачей, так как применение данной методики позволит сравнивать и выбирать наилучший алгоритм ЭЦП применительно к каждой конкретной ситуации.

The paper is devoted to the solution of the problem of comparing EDS algorithms based on transformations in a group of elliptic curve points. Finding such a technique is an actual problem as using the given technique will allow to compare and choose the best EDS algorithm with reference to each specific situation.

ВВЕДЕНИЕ

Одной из важнейших, и в то же время недостаточно решенных, является задача сравнения ЭЦП, различных алгоритмов, размеров и при разных ограничениях. Под критерием будем понимать признак, на основе которого осуществляется оценка, определение или классификация чего-нибудь, т.е. по сути, будем понимать критерий оценки. Предыдущие исследования позволяют сделать вывод, что сравнение ЭЦП можно осуществить с использованием двух составляющих: безусловного и условного критериев. Оценку ЭЦП будем выполнять в 2 этапа. На первом этапе будем проверять их на соответствие безусловным критериям. Сравнение алгоритмов ЭЦП предлагается проводить методом анализа иерархий [1-5].

В качестве алгоритмов ЭЦП для сравнения предлагается выбрать следующие: ECSS[6], EC-DSA[7], EC-GDSA[7], EC-KCDSA[7], ДСТУ 4145-2002[8], ГОСТ Р 34.10-2001[9].

1. ОПИСАНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ

В методе анализа иерархий элементы задачи сравниваются попарно относительно их влияния («веса» или «интенсивности») на общую для них характеристику. Проведем парные сравнения, которые приводят к матричной форме – квадратной таблице:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Эта матрица имеет свойство обратной симметричности, то есть $a_{ji} = 1/a_{ij}$.

Когда проблемы представлены иерархически, матрица составляется для сравнения относительной важности критериев на втором уровне, относительно общей цели на первом уровне. Подобные матрицы должны быть построены для парных сравнений каждой альтернативы на третьем уровне относительно критериев второго уровня и так дальше.

Заполнение квадратных матриц парных сравнений выполняется по следующему правилу. Если элемент E_1 преобладает над элементом E_2, то ячейка матрицы, которая отвечает пересечению строки E_1 и столбца E_2, заполняется целым числом, а ячейка, которая отвечает пересечению строки E_2 и столбца E_1, заполняется обратным ему числом. Если элемент E_2 преобладает над E_1, то целое число заносится в ячейку, которая отвечает строке E_2 и столбцу E_1, а дробь проставляется в ячейку, которая отвечает строке E_1 и столбцу E_2. Если элементы и преобладают одинаково, то в обе позиции матрицы заносятся единицы.

Для получения каждой матрицы эксперт выносит $n(n-1)/2$ суждений (здесь n – порядок матрицы парных сравнений).

Рассмотрим в общем виде пример формирования матрицы парных сравнений.

Пусть E_1, E_2, ..., E_n – множество из n элементов (альтернатив) и $\nu_1, \nu_2, ..., \nu_n$ – соответственно их вес, или интенсивность. Сравним попарно вес, или интенсивность каждого элемента с весом или интенсивностью любого другого элемента множества относительно общего для них свойства или цели. В этом случае матрица парных сравнений $[E]$ имеет такой вид:

$[E] =$

	E_1	E_2	...	E_n
E_1	ν_1/ν_1	ν_1/ν_2	...	ν_1/ν_n
E_2	ν_2/ν_1	ν_2/ν_2	...	ν_2/ν_n
...	...	...	...	...
E_n	ν_n/ν_1	ν_n/ν_2	...	ν_n/ν_n

При осуществлении попарных сравнений необходимо ответить на такие вопросы: который из двух сравниваемых элементов, важнее или имеет большее влияние, какой более вероятный и какой лучший. При сравнении критериев обычно определяют, какой из критериев больше важный; при сравнении альтернатив относительно критерия – которая из них лучше или более вероятна.

Парные сравнения проводятся в пределах преимущества одного элемента над другим. Полученные суждения выражаются в целых числах с учетом девятибалльной шкалы (табл. 1).

Правомерность этой шкалы доказана теоретически[1, 3] при сравнении с большим числом других шкал. При использовании указанной шкалы, сравнивая два объекта по вкладу для достижения цели, расположенной на вышестоящем уровне иерархии, необходимо поставить в соответствие этому сравнению число в интервале от 1 до 9 или обратное значение чисел. В тех случаях, когда сложно различить, сколько промежуточных градаций от абсолютного к слабому преимуществу или этого не нужно в конкретной задаче, может использоваться шкала с меньшим числом градаций. В нижней границе шкала может иметь только две оценки: 1 – объекты равнозначные; 2 – преимущество одного объекта над другим.

Из группы матриц парных сравнений мы формируем набор локальных приоритетов, которые выражают относительное влияние множества элементов на элемент уровня, который примыкает сверху. Находится относительный вес, величина, ценность, желательность или вероятность каждого отдельного объекта через решение матриц. Для этого необходимо вычислить множество собственных векторов для каждой матрицы, а потом нормализовать результат к единице. Вычисления собственных векторов – не очень сложная, однако довольно трудоемкая задача. Для ее решения наиболее простым является метод вычисления геометрического среднего. Вычислить среднее геометрическое можно путем перемножения всех элементов в каждой строке с последующим добыванием корня n – й степени, где n – количество элементов строки матрицы

$$q_j^{(r-1)} = \sqrt[n]{(v_j^{(r)} / v_1^{(r)}) \times (v_j^{(r)} / v_2^{(r)}) \times \cdots \times (v_j^{(r)} / v_n^{(r)})},$$

где r – уровень иерархии, для матрицы которого выполняется расчет, n – количество элементов в строке, j – порядковый номер строки.

Полученный таким образом столбец нормализуется делением каждого числа на сумму всех чисел

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}}.$$

Другой способ состоит в нормализации элементов каждого столбца матрицы, и потом усреднения каждой строки. Таким образом, мы можем определить не только порядок приоритетов каждого отдельного элемента, но и величину его приоритета.

После этого из всех нормированных значений формируются промежуточные матрицы, и выполняется «свертка» иерархии путем перемножения промежуточной матрицы нижнего уровня на нормированный столбец верхнего уровня. «Свертка» выполняется к тому моменту, пока не будут полученные глобальные значения степени преимущества одной альтернативы над другой.

2. БЕЗУСЛОВНЫЕ КРИТЕРИИ ОЦЕНКИ ЭЦП, ОСНОВЫВАЮЩИХСЯ НА КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЯХ В ГРУППЕ ТОЧЕК ЭК

К безусловным критериям будем относить те критерии, выполнение которых для ЭЦП основанных на криптографических преобразованиях в группе точек ЭК являются обязательным.

Анализ применения эллиптических кривых [10, 11], разработка и оценки свойств криптогра-

Таблица 1

Шкала сравнений (степени значимости величины)

Степень значимости	Определение	Пояснения
1	Одинаковая значимость	Обе величины вносят одинаковый вклад в достижение цели
3	Некоторое преимущество одной величины над другой (слабая значимость)	Существуют аргументы в пользу преимущества одной из величин, но эти аргументы недостаточно убедительные
5	Существенная или сильная значимость	Существуют надежные данные или логические суждения для того, чтобы показать преимущество одной из величин
7	Очевидная или очень сильная значимость	Убедительное свидетельство преимущества одной величины над другой
9	Абсолютная значимость	Свидетельства в пользу преимущества одной величины над другой убедительные в максимальной степени
2,4,6,8	Промежуточные значения между двумя соседними суждениями	Ситуация, когда необходимо компромиссное решение
Обратные величины приведенных выше ненулевых величин	Если величине i при сравнении с величиной j придается одно из приведенных выше ненулевых чисел, то величине j при сравнении с величиной i придается обратное значение	Если согласованность была определена при получении N числовых значений для создания матрицы

фических преобразований в группе точек ЭК [12], достигнутые результаты в практическом решении задач криптоанализа и реализации разных атак [13], позволяют выбрать в качестве основных следующие безусловные критерии оценки.

1. Надежность математической базы, в понимании отсутствия возможностей осуществлять атаки типа «универсальное раскрытие» за счет несовершенства математической базы группы точек эллиптических кривых или слабостей, которые могут быть заложены за счет специфических свойств общих параметров и ключей. При этом критерием оценки надежности математической базы является тот факт, что сложность атаки универсальное раскрытие $I_{ур}$ носит экспоненциальный характер, а критерий ненадежности – субэкспоненциальный или полиномиальный характер сложности. Обозначим этот критерий $W_{\delta 1}$.

2. Практическая защищенность криптографических преобразований в группе точек ЭК от силовых и аналитических атак, которая достигается за счет выбора размеров общих параметров и ключей. Критерием практической защищенности криптографических преобразований является выбор таких размеров общих параметров и ключей, при которых сложность атаки $I_{са}$ существенно (на необходимое число порядков) превышает существующую мощность криптоаналитических систем на уровне технологически развитых государств, в том числе с учетом прогноза увеличения мощности криптоаналитических систем за счет развития математического и программного обеспечения, а также аппаратных и программно-аппаратных средств. Обозначим этот безусловный критерий $W_{\delta 2}$.

3. Реальная защищенность от всех известных и потенциально возможных криптоаналитических атак, где под защищенностью понимается тот факт, что все известные криптоаналитические атаки типа «полное раскрытие» носят (имеют) экспоненциальную сложность $I_{ес}$, а критерием незащищенности – субэкспоненциальный $I_{се}$ характер сложности атаки «полное раскрытие». Обозначим этот безусловный критерий $W_{\delta 3}$.

4. Статистическая безопасность криптографического превращения в группе точек эллиптической кривой, под которой понимается статистическая независимость результата криптографического преобразования (выхода). Обозначим этот безусловный критерий $W_{\delta 4}$.

5. Теоретическая защищенность криптографического преобразования, в котором используются общие параметры с соответствующими свойствами и длинами, для которого не существуют теоретические аналитические атаки, сложность которых меньше чем сложность атаки типа «полное раскрытие». Этот критерий будем обозначать как $W_{\delta 5}$.

6. Отсутствие слабых личных ключей, при которых сложность криптоаналитических атак типа полное раскрытие и универсальное раскрытия меньше, чем сложность атаки полное раскрытие для других личных ключей. Обозначим этот безусловный критерий как $W_{\delta 6}$.

7. Сложность прямого $I_{пр}$ и обратного $I_{обр}$ криптографических преобразований носит полиномиальный характер и не превышает допустимых величин $I_{пр}'$ и $I_{обр}'$. Обозначим этот безусловный критерий также как $W_{\delta 7}$.

Поскольку приведенные частичные критерии являются безусловными, то критерием отбора является логическое значение да/нет (1/0), поэтому безусловный критерий можно записать

$$(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}) \in (1,0). \qquad (1)$$

С учетом приведенных выше частичных безусловных критериев $W_{\delta 1} - W_{\delta 7}$ и условия (4.1) функция соответствия ЭЦП, основанных на криптографических преобразованиях в группе точек эллиптических кривых, может быть записана как

$$f_{\text{фв}}(\ ) = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge W_{\delta 5} \wedge W_{\delta 6} \wedge W_{\delta 7}.$$

Где символ «^» обозначает операцию коньюнкции булевых переменных.

Таким образом, качество ЭЦП может быть оценено с использованием безусловного интегрального критерия – функции соответствия ЭЦП требованиям

$$f_{\text{фв}}(\ ) \in (0,1)$$

и при

$$f_{\text{фв}}(\ ) = 1$$

оцениваемая ЭЦП, отвечает требованиям.

Предложенный интегральный критерий позволяет только установить факт отвечает или нет установленным требованиям рассматриваемая ЭЦП.

3. УСЛОВНЫЕ КРИТЕРИИ ОЦЕНКИ ЭЦП, ОСНОВЫВАЮЩИХСЯ НА КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЯХ В ГРУППЕ ТОЧЕК ЭК

Качественное и количественное сравнение криптографических превращений в группе точек ЭК можно осуществить, используя метод анализа иерархий.

В качестве основных критериев оценки предлагается использовать следующие частичные условные критерии (табл. 1).

4. СРАВНЕНИЕ АЛГОРИТМОВ ЭЦП

Проведем анализ соответствия алгоритмов ЭЦП безусловным критериям. Результаты этого анализа представлены в табл. 3.

Теперь проведем сравнение алгоритмов ЭЦП относительно условных критериев, для этого построим дерево целей (рис. 1).

Оценим вклад каждого критерия в общую цель, для этого построим табл. 4.

Теперь оценим каждый критерий, для этого для каждого критерия построим матрицу попарных сравнений относительно сравниваемых алгоритмов ЭЦП.

Таблица 2

Условные критерии оценки алгоритмов ЭЦП

№	Критерии	Обозначение
1	Возможность и условия свободного распространения и применение международного или национального стандарта криптографических превращений в группе точек эллиптической кривой на Украине с учетом нормативно-правовых актов Украины на экспорт, импорт и ограничения на его применение	W_{y1}
2	Уровень доверия к международному или национальному стандарту криптографического превращения в группе точек эллиптической кривой	W_{y2}
3	Перспективность применения международного или национального стандарта на Украине	W_{y3}
4	Временная и пространственная сложность программной, программно-аппаратной и аппаратной реализаций	W_{y4}
5	Возможность и условия применения стандартов с разными параметрами и в разных режимах	W_{y5}
6	Гибкость алгоритма ЭЦП, основанного на криптографических превращениях в группе точек эллиптической кривой	W_{y6}
7	Уровень защищенности при реализации разных видов угроз, при разных условиях осуществления криптоаналитических атак и отклонение свойств общих параметров	W_{y7}

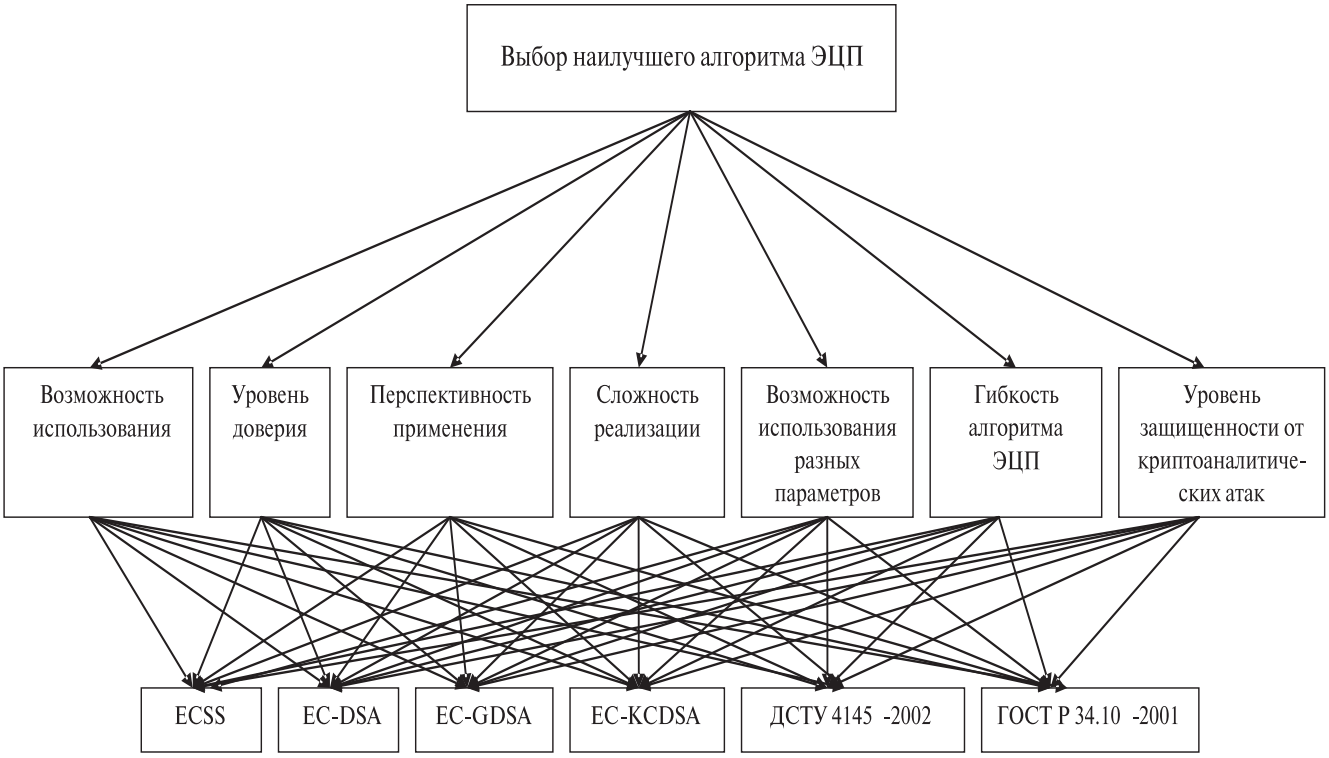

Рис. 1. Дерево целей

Таблица 3

Результаты сравнения относительно безусловных критериев

ЭЦП \ Критерий	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
ECSS	1	1	1	1	1	1	1	1
EC-DSA	1	1	1	1	1	1	1	1
EC-GDSA	1	1	1	1	1	1	1	1
EC-KCDSA	1	1	1	1	1	1	1	1
ДСТУ 4145-2002	1	1	1	1	1	1	1	1
ГОСТ Р 34.10-2001	1	1	1	1	1	1	1	1

Таблица 4

Вклад критериев в достижение общей цели, матрица попарных сравнений

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	W_{y7}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	1/7	0.4539	0.0461
W_{y2}	6	1	4	5	4	3	1/7	2.1403	0.1990
W_{y3}	1/4	1/4	1	3	2	1/2	1/7	0.5962	0.0554
W_{y4}	4	1/5	1/3	1	1/4	1/4	1/7	0.4219	0.0392
W_{y5}	2	1/4	1/2	4	1	1/3	1/7	0.6473	0.0602
W_{y6}	3	1/3	2	4	3	1	1/7	1.1925	0.1109
W_{y7}	7	7	7	7	7	7	1	5.3011	0.4930

Отношение согласованности матрицы равно %14.762, что лежит в пределах нормы.

Таблица 5

Матрица попарных сравнений критерия W_{y1}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/3	1/3	1/3	1/6	1/7	0.3097	0.0409
EC-DSA	3	1	1	1	1/3	3	1,2009	0.1585
EC-GDSA	3	1	1	1	1/3	3	1,2009	0.1585
EC-KCDSA	3	1	1	1	1/3	3	1.2009	0.1585
ДСТУ 4145-2002	6	3	3	3	1	5	3.0531	0.4030
ГОСТ Р 34.10-2001	7	1/3	1/3	1/3	1/5	1	0.6107	0.0806

Отношение согласованности равняется %4.5904.

Таблица 6

Матрица попарных сравнений критерия W_{y2}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/4	1/5	1/6	1/2	1/3	0.3340	0.0417
EC-DSA	4	1	1/3	1/4	1/3	1/3	0.5774	0.0721
EC-GDSA	5	3	1	1/3	2	3	1.7627	0.2200
EC-KCDSA	6	4	3	1	5	5	3.4878	0.4354
ДСТУ 4145-2002	2	3	1/2	1/5	1	2	1.0309	0.1287
ГОСТ Р 34.10-2001	3	3	1/3	1/5	1/2	1	0.8182	0.1021

Отношение согласованности равняется %6.6479.

Таблица 7

Матрица попарных сравнений критерия W_{y3}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/6	1/6	1/6	1/4	1/4	0.2572	0.0321
EC-DSA	6	1	1/4	1/4	1/2	1/2	0.6740	0.0840
EC-GDSA	6	4	1	1	3	4	2.5698	0.3203
EC-KCDSA	6	4	1	1	4	4	2.6960	0.3361
ДСТУ 4145-2002	4	2	1/3	1/4	1	1	0.9347	0.1165
ГОСТ Р 34.10-2001	4	2	1/4	1/4	1	1	0.8909	0.1110

Отношение согласованности равняется %3.9119.

Таблица 8

Матрица попарных сравнений критерия W_{y4}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	3	4	4	2	3	2.5698	0.3558
EC-DSA	1/3	1	3	4	2	2	1.5874	0.2198
EC-GDSA	1/4	1/3	1	3	1/2	2	0.7937	0.1099
EC-KCDSA	1/4	1/4	1/3	1	1/3	1/3	0.3637	0.0504
ДСТУ 4145-2002	1/2	1/2	2	3	1	2	1.2009	0.1663
ГОСТ Р 34.10-2001	1/3	1/2	1/2	3	1/2	1	0.7071	0.0979

Отношение согласованности равняется %5.4438

Таблица 9

Матрица попарных сравнений критерия W_{y5}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1	1	1	1	1	1.0000	0.1667
EC-DSA	1	1	1	1	1	1	1.0000	0.1667
EC-GDSA	1	1	1	1	1	1	1.0000	0.1667
EC-KCDSA	1	1	1	1	1	1	1.0000	0.1667
ДСТУ 4145-2002	1	1	1	1	1	1	1.0000	0.1667
ГОСТ Р 34.10-2001	1	1	1	1	1	1	1.0000	0.1667

Отношение согласованности равняется %0.0000.

Таблица 10

Матрица попарных сравнений критерия W_{y6}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/2	1/2	1/2	1	1	0.7071	0.1067
EC-DSA	2	1	1	1	2	2	1.4142	0.2135
EC-GDSA	2	1	1	1/2	3	3	1.4422	0.2177
EC-KCDSA	2	1	2	1	3	3	1.8171	0.2743
ДСТУ 4145-2002	1	1/2	1/3	1/3	1	1	0.6934	0.1047
ГОСТ Р 34.10-2001	1	1/2	1/3	1/3	1	1	0.5503	0.0831

Отношение согласованности равняется %2.3867.

Таблица 11

Матрица попарных сравнений критерия W_{y7}

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	2	1/3	1/3	1/3	1/3	0.5396	0.0735
EC-DSA	1/2	1	1/5	1/5	1/3	1/3	0.3612	0.0492
EC-GDSA	3	5	1	1/2	2	2	1.7627	0.2400
EC-KCDSA	3	5	2	1	3	3	2.5423	0.3461
ДСТУ 4145-2002	3	3	1/2	1/3	1	1	1.0699	0.1457
ГОСТ Р 34.10-2001	3	3	1/2	1/3	1	1	1.0699	0.1457

Отношение согласованности равняется %2.9307.

Для получения результирующего вектора приоритетов перемножим вектор приоритетов 1 уровня и матрицу полученных значений 1 уровня.

$$\begin{pmatrix} 0.0461 \\ 0.1990 \\ 0.0554 \\ 0.0392 \\ 0.0602 \\ 0.1109 \\ 0.4930 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 0.0409 & 0.0417 & 0{,}0321 & 0.3538 & 0.1667 & 0.1067 & 0.0735 \\ 0.1585 & 0.0721 & 0{,}0840 & 0.2198 & 0.1667 & 0.2135 & 0.0492 \\ 0.1585 & 0.2200 & 0{,}3203 & 0.1099 & 0.1667 & 0.2177 & 0.2400 \\ 0.1585 & 0.4354 & 0{,}3361 & 0.0504 & 0.1667 & 0.2743 & 0.3461 \\ 0.4030 & 0.1287 & 0{,}1165 & 0.1663 & 0.1667 & 0.1047 & 0.1457 \\ 0.0806 & 0.1021 & 0{,}1110 & 0.0979 & 0.1667 & 0.0831 & 0.1457 \end{pmatrix} =$$

$$= \begin{pmatrix} 0{,}0839 \\ 0{,}0929 \\ 0{,}2256 \\ 0{,}3256 \\ 0{,}1506 \\ 0{,}1251 \end{pmatrix}$$

Таким образом, проанализировав полученные результаты, можно сделать следующий вывод, что самым перспективным алгоритмом для введения в использования на Украине на сегодняшний день является алгоритм EC-KCDSA, также рекомендуется использовать алгоритм EC-GDSA, который имеет сходные характеристики, но в тоже время проще в реализации.

5. АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ СРАВНЕНИЯ

Рассмотрим полученные численные результаты, полученные в предыдущем разделе. Исследуемые алгоритмы электронной цифровой подписи, основанные на преобразованиях в группе точек эллиптической кривой, можно расположить по местам, которые они заняли по результатам сравнения (1 – наилучший, 6 – худший).

7. EC-KCDSA (0.3256)
8. EC-GDSA (0.2256)
9. ДСТУ 4145-2002 (0.1506)
10. ГОСТ Р 34.10-2001 (0.1251)
11. EC-DSA (0.0929)
12. ECSS (0.0839)

Таким образом, результаты применения методики сравнения показали эффективность стандарта ISO/IEC 15946-2 и необходимость его гармонизации на Украине.

Принятие, внедрение и применение стандарта ISO/IEC 15946-2 на Украине разрешает:

– за счет использования признанных на мировом уровне цифровых подписей обеспечивать целостность, подлинность, неопровержимость и доступность при обмене и использовании электронных данных, разнообразной информации и сообщений;

– устранить технические барьеры в международном обмене товарами и услугами;

– повысить степень соответствия комплексов и средств КЗИ, услуг КЗИ их функциональному назначению;

– оказывать содействие научно-техническому прогрессу и сотрудничеству в сфере КЗИ;

– обеспечить переносимость, совместимость и масштабируемость комплексов КЗИ;

– обеспечить технический уровень комплексов и средств КЗИ до отвечающего современному уровню развития науки, техники и технологий в сфере КЗИ;

– осуществить внедрение, в процессе стандартизации в сфере КЗИ, новейших методов исследований;

– обеспечить необходимый уровень крипостойкости и защищенности от пассивных и активных атак.

Литература.

[1] *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. – К.: «МК-Пресс», 2006 – 320с., ил.

[2] *Орловский С.А.* Проблемы принятия решений при нечёткой исходной информации. – М.: Наука, 1981. – 208 с.

[3] *Саати Т.* Принятие решений. Метод анализа иерархий: пер. с англ. М.: Радио и связь, 1989. – 316 с.

[4] *Райфа Х.* Анализ решений (введение в проблему выбора в условиях неопределённости): пер. с англ. М.: Наука, 1977.

[5] *Андрейчиков А.В., Андрейчикова О.Н.* Анализ, синтез, планирование решений в экономике. М.: Финансы и статистика, 2002. – 386 с., ил.

[6] Стандарт X9.63.

[7] Стандарт ISO/IEC 15946-2 – Электронные цифровые подписи.

[8] ДСТУ 4145 – 2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

[9] ГОСТ Р 34.10 – 2001 – «Процессы формирования и проверки электронной цифровой подписи», – 2001.

[10] Коммерческие системы шифрования: основные алгоритмы и их реализация, В. Водолазкий, – 2001.

[11] Вейскас Дж. «Технология использования цифровой подписи».-: Питер.1997-848с.

[12] Громов В.И. «Энциклопедия компьютерной безопасности», М.: Мир, 1999.-608с.

[13] Методы оценки сложности криптоанализа для криптографических приложений в группе точек эллиптической кривой, учитывающие вероятность коллизий /Д.С. Балагура. Ю.И. Горбенко, // Радиотехника: Всеукр. межвед. Научн.-техн. сб. 2005. Вып. 142. С. 205-213.

Поступила в редколлегию 19.09.2008

Бондаренко Михаил Федорович, доктор технических наук, профессор, ректор Харьковского национального университета радиоэлектроники.

Денисенко Борис Игоревич, аспирант кафедры БИТ ХНУРЕ. Область научных интересов: изучение аспектов безопасности информационных технологий и программирование различных приложений, использующих сетевые технологии.

Горбенко Юрий Иванович, кандидат технических наук, технический директор ЗАО «ИИТ», научный сотрудник НИЦ «Z» кафедры БИТ ХНУРЭ. Область научных интересов: защита информации в информационно-телекоммуникационных системах.