АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ И ИХ ПРИМЕНЕНИЕ

УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, Р.С. ГАНЗЯ

АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ АРИФМЕТИКО-ГЕОМЕТРИЧНОГО МЕТОДУ ОБЧИСЛЕННЯ КІЛЬКОСТІ ТОЧОК НА ЕЛІПТИЧНІЙ КРИВІЙ

Вступ

На даний момент в Україні надзвичайно широко використовуються такі електронні довірчі послуги як електронний цифровий підпис, електронна печатка та мітка часу. Суттєве місце для реалізації електронних довірчих послуг в Україні займає асиметрична криптографія та криптографія на еліптичних кривих як її складова, проте швидкий розвиток квантових технологій та існування квантового алгоритму Шора [1], що здатен вирішити проблеми факторизації та розв'язання дискретного логарифмічного рівняння із поліноміальною складністю, може створити ситуацію, коли сучасні асиметричні криптосистеми можуть бути скомпрометовані.

Одним із шляхів вирішення даної проблеми є збільшення розмірів загальносистемних параметрів криптоперетворень. Звичайно, таке збільшення не дасть підвищення стійкості проти квантового криптоаналізу, проте для проведення такого аналізу необхідний квантовий комп'ютер з великою кількістю кубітів, а, як показує аналіз [2], перспектива появи такого комп'ютера в найближчі 5 – 10 років неможлива. Також перспективним напрямком протидії є дослідження постквантових криптосистем [3].

Також враховуючи те, що в Україні були прийняті нові національні стандарти симетричного шифрування та геш-функції [4] з розмірами блоку повідомлення (виходу геш-функції) та ключа до 512 бітів, то для досягнення однакового рівня безпеки при використанні системи типу "електронний конверт" необхідно використання асиметричних криптоперетворень (електронного цифрового підпису та направленого шифрування) з розмірами загальних параметрів не менше 1024 бітів. Національний стандарт електронного цифрового підпису (ДСТУ 4145-2002) має загальносистемні параметри з розмірами до 431 біта. Тому задача генерування загальносистемних параметрів великих розмірів (1024 біта та більше) є актуальною.
В цілому задача генерування загальносистемних параметрів зводиться до складного, з точки зору обчислень, завдання – обчислення кількості точок на еліптичній кривій.

1. Аналіз методів обчислення кількості точок на еліптичній кривій

В стандарті ISO/IEC 15946-5:2009 [5], що описує методи генерування загальносистемних параметрів для еліптичних кривих, визначені напрямки генерування загальносистемних параметрів:

1. Генерування еліптичної кривої, застосовуючи алгоритми обчислення порядку (псевдо-) випадкової еліптичної кривої;
2. Генерування еліптичної кривої, застосовуючи метод комплексного множення;
3. Генерування еліптичної кривої, підіймаючи еліптичну криву, визначену над малим скінченним полем, до досить великого поля.

Суть першого напрямку полягає у виготовленні набору загальних параметрів еліптичної кривої над полем, вибираючи (псевдо-)випадково з еліптичних кривих відповідного порядку

разом з достатньою кількістю інформації для перевірки, що крива була дійсно вибрана псевдовипадково. Другий напрямок генерує загальносистемні параметри еліптичної кривої E над полем $F(p)$ відповідно до заданої кількості раціональних точок N. Третій напрямок генерує загальносистемні параметри еліптичної кривої E над полем $F(p^m)$, підіймаючи криву E над полем $F(p)$[5].

Третій напрямок є універсальним і може застосовуватись для полей з різними характеристиками. При використанні цього напрямку для генерування загальних параметрів в групі точок еліптичних кривих можуть використовуватися *l-адичні* та *p-адичні* методи. *L-адичні* методи обчислення кількості точок на еліптичній кривій можуть використовуватися для
скінчених полей будь-яких характеристик, проте вони як правило застосовується для обчисленняу кількості точок в групі точок еліптичних кривих над великими простими полями $F(p)$. Для еліптичних кривих над скінченими полями малих характеристик використовуються *p-адичні* алгоритми.

Нехай E еліптична крива задана рівнянням $y^2 + xy = x^3 + a_6$ з елементом a_6 над F_q з *j-інваріантом* $j(E) = a_6^{-1}$ та $q = p^n$. Кількість точок $\#E(F_q)$ задовольняє співвідношення $\#E(F_q) = q + 1 - t$, де t – слід ендоморфізму Фробеніуса $F : E \to E : (x, y) \to (x^q, y^q)$. За теоремою Хасе [7] отримаємо $|t| \le 2\sqrt{q}$, тому достатньо обчислити $t \bmod B$, де $B > 4\sqrt{q}$.

Схуф описав перший поліноміальний алгоритм для обчислення , використовуючи *l-адичний* підхід. Часова складність алгоритму Схуфа $O((\log q)^{3\mu+2})$ та просторова складність $O((\log q)^3)$. В подальшому цей алгоритм став основою алгоритма SEA, що має обчислювальну складність $O((\log q)^{2\mu+2})$ та просторову складність $O((\log q)^2)$. Детальний опис можна знайти у [6].

У 1999 році Т. Сато запропонував інший підхід обчислення кількості точок на еліптичній кривій, що базувався на *p-адичних* числах. Основна ідея даного методу полягала в піднятті кривої та ендоморфізму Фробеніуса до *p-адичного* кільця та відновлення значення сліду Фроебніуса $t \bmod p^N$ (де $p^N > 4\sqrt{q}$) з даних, які отримані після підняття. Підняття виконується послідовним підняттям *j-інваріантів*, коефіцієнтів кривої разом з підняттям підгруп *l-крутіння* з попереднім обчисленням циклу кривих та *j-інваріантів* j_1 [7]. Інший метод, який дуже пов'язаний з методом Сато, базується на арифметико-геометричному методі (AGM), був запропонований Местре [8] та реалізований Харлі. Харлі також показав, що даний метод може бути надзвичайно ефективним. Обчислювальна складність метода AGM, що був запропонований Местре, не відрізняється від метода Сато, проте має меншу просторову складність. Просторова та обчислювальна складність відомих *p-адичних* алгоритмів наведена у табл. 1.

Множення двох цілих чисел, що складаються з n біт, здійснено за $\mathrm{O}\left(n^{\mu}\right)$ операцій, де μ – це константа, яка визначає час виконання множення двох m бітових цілих чисел з часовою складністю $\mathrm{O}\left(m^{\mu}\right)$. Так, для класичних алгоритмів множення значення $\mu = 2$ для швидкого алгоритму Карацуби [9] $\mu = \log_2 3$.

Слід зазначити, що кожний з наведених методів знаходить лише порядок кривої та не відповідає на запитання можливості її використання в криптографічних перетвореннях. Виходячи з цього, після обчислення порядку кривої необхідно з'ясувати придатність її до

застосування в криптографічних системах. Вибрати критерії, які дозволяють обирати еліптичні криві для побудови загальносистемних параметрів необхідного рівня стійкості.

Таблиця 1

Прізвище автора (назва методу)	Характеристика поля, p	Часова складність	Просторова складність
Сато (Satoh)	$p \geq 5$	$O(n^{3+\mu})$	$O(n^3)$
Ск'єрна (Skjernaa)	$p = 2$	$O(n^{3+\mu})$	$O(n^3)$
Форквет – Гаудрі – Харлі (Fouquet – Gaudry – Harley)	$p = 2, 3$	$O(n^{3+\mu})$	$O(n^3)$
Веркаутерен (Vercauteren)	всі p	$O(n^{3+\mu})$	$O(n^2)$
Местре (Mestre, AGM)	$p = 2, 3$	$O(n^{3+\mu})$	$O(n^2)$
Карлз (Carls)	всі p, $p = 3$	$O(n^{3+\mu})$	$O(n^2)$
Кохель (Kohel)	$p \leq 11$	$O(n^{3+\mu})$	$O(n^2)$
Сато – Ск'єрна – Тагучі (Satoh – Skjernaa – Taguchi, SST)	всі p	$O(n^{2,5+\mu})$	$O(n^2)$
Кім та інші (Kim)	всі p	$O(n^{2,5+\mu})$	$O(n^2)$
Гаудрі (Gaudry)	$p = 2$	$O(n^{2,5+\mu})$	$O(n^2)$
Медсен (Madsen)	всі p	$O(n^{2,5+\mu})$	$O(n^2)$
Лерс'єр – Любич (Lercier – Lubicz)	всі p	$O(n^{2+\mu})$	$O(n^2)$
Харлі (Harley)	всі p	$O(n^{2+\mu})$	$O(n^2)$

2. Арифметико-геометричний метод обчислення кількості точок

Обчислення будь-якого *p-адичного* методу виконується у такі етапи:

1. Підняття циклу ізогінеї та коефіцієнтів кривої;
2. Проведення нормування коефіцієнтів;
3. Обчислення сліду ендоморфізму Фробеніуса, на базі якого визначається порядок кривої.

Для використання методу AGM необхідна крива E, задана рівнянням $y^2 + xy = x^3 + a_6$ з елементом a_6 над F_q з *j-інваріантом* $j(E) = a_6^{-1}$. Необхідно позначити, що елемент a_6 є довільним елементом з Z_q, що зменшений до a_6 за модулем 2. Далі отримаємо рекурсивну формулу, що дасть нам цілком вірну послідовність (A_i, B_i) елементів з Z_q:

$$A_0 = 1 + 8a_6, \quad B_0 = 1,$$
$$A_{i+1} = \frac{A_i + B_i}{2}, \quad B_{i+1} = \sqrt{A_i + B_i}, \tag{1}$$

де квадратний корінь вибирається так, що бути конгруентним до 1 по модулю 4. Таким чином у роботі [7] показано, що якщо квадратний корінь один раз був заданий конгруентним до 1 по модулю 4, то ця пропорція буде зберігатися на кроці $i+1$.

Послідовність (A_i, B_i) називається AGM-послідовністю і її можна привести до послідовності еліптичної кривої E виразом $y^2 = x(x - A_i^2)(x - B_i^2)$. Позначимо як j_1 *j-інваріант* еліптичної кривої E.

Добре відомо, що AGM пов'язаний з ізогінезисом степені 2 між еліптичними кривими. Цей крок дає на зв'язок з канонічним підйомом у наступній теоремі.

Теорема 1. Нехай j_1 буде *j-інваріантом* еліптичної кривої E пов'язаний з AGM послідовністю. Тоді послідовність j_i підтверджує:

$$\begin{aligned} j_0 &\equiv a_6^{-2} \bmod 2, \\ j_{i+1} &\equiv j_i^2 \bmod 2, \\ j_i &\equiv j_i^{\uparrow} \bmod 2^{i+2}. \end{aligned} \tag{2}$$

Перше твердження показує, що E ізоморфна зі сполученим підйомом з початковою еліптичною кривою E по модулю 2. Друге – стверджує, що всі еліптичні криві E_i також зменшуються за модулем 2 до сполучень кривої E (з точністю до ізоморфізму). Третє є основною AGM алгоритму: це означає, що, коли відбувається підйом по AGM-послідовності, ми все ближче і ближче наближаємось до канонічного підйому.

Це дає простий алгоритм для обчислення канонічного підйому. Починаючи з початкових значень (A_0, B_0), ми застосовуємо рекурсивну формулу для обчислення послідовних значень (A_i, B_i). Після k кроків, ми можемо обчислити *j-інваріант* асоційованої кривої, близький до канонічного підйому сполученої E піднятої до точності 2^k [7].

Зв'язок цієї теореми зі слідом Фробеніуса дає ефективний метод для підрахунку кількості точок еліптичної кривої E.

Теорема 2. Нехай $i > 0$ та нехай c_i буде $Norm_{Z_q / Z_p}(\frac{A_{i+1}}{A_i})$, тоді:

$$c_i + q / c_i = Tr(E) \bmod 2^{i+4}. \tag{3}$$

AGM алгоритм складається з наступних частин: спочатку обчислюється AGM-послідовність з достатньою кількістю кроків, а далі йде обчислення норми, що дає слід початкової кривої з деякою точністю, яка дорівнює числу кроків плюс константа. На перший погляд, здається, що ми повинні починати з великої точності для A_0 та B_0, тому що ми отримуємо все менше і менше значущі цифри у A_i та B_i, коли в той же час j_i стає ближче до канонічного підйому. Ця проблема може бути вирішена шляхом додавання довільного шуму до A_i та B_i перед операцією, яка "понижує" точність, як квадратний корінь або ділення на 2.

Нижче наведено кроки виконання арифметико-геометричного методу для підрахунку кількості точок на еліптичній кривій $E(F_{2^d})$, що був запропонований Местре [8].

$$
\begin{aligned}
&\textit{Вхід}: \textit{Еліптична крива } E: y^2 + xy = x^3 + \bar{c} \textit{ над } F_{2^d} \\
&\textit{Вихід}: \textit{Кількість точок кривої } E(F_{2^d}) \\
&1.\ N \leftarrow \lceil d/2 \rceil + 3 \\
&2.\ a \leftarrow 1 \textit{ and } b \leftarrow (1+8c) \bmod 2^4 \\
&3.\ \textit{for } i = 5 \textit{ to } N \textit{ do} \\
&4.\quad (a,b) \leftarrow ((a+b)/2, \sqrt{ab}) \bmod 2^i \\
&5.\ a_0 \leftarrow a \\
&6.\ \textit{for } i = 0 \textit{ to } d-1 \textit{ do} \\
&7.\quad (a,b) \leftarrow ((a+b)/2, \sqrt{ab}) \bmod 2^N \\
&8.\ t \leftarrow a_0 / a \bmod 2^{N-1} \\
&9.\ \textit{if } t^2 > 2^{d+2} \textit{ then } t \leftarrow t - 2^{N-1} \\
&10.\ \textit{return } 2^d + 1 - t
\end{aligned}
\tag{4}
$$

Другий цикл обчислень, що починається на 6 кроці, можна замінити на обчислення однієї арифметико -геометричної ітерації та обчислення норми. Тобто

$$t \equiv N_{Q_p / Q_p}(a_0 / a_1) \,(\bmod 2^N). \tag{5}$$

Для обчислення норми можна використати декілька алгоритмів: аналітичний (запропононований Сато, Ск'єрною та Тагучі), а також метод на основі результанта. Для обчислення результанта було запропоновано використати швидкий алгоритм обчислення найбільшого спільного дільника, який показав Моенк [6].

У [7] Гаудрі запропонував замінити AGM-послідовність (A_i, B_i), що є двозмінною (AGM bivariate) на однозмінну (AGM univariate). Тобто можна взяти одну зміну і визначити її наступним чином:

$$\lambda_i = \frac{A_i}{B_i}. \tag{6}$$

Відповідні еліптичні криві мають вираз $y^2 = x(x-1)(x-\lambda_i^2)$. З виразу (5) можна показати, що λ_{i+1} обчислюється наступним чином:

$$\lambda_{i+1} = \frac{1+\lambda_i}{2\sqrt{\lambda_i}}. \tag{7}$$

Однозмінний AGM алгоритм обчислення кількості точок на еліптичній кривій з заміною другого циклу обчислень на обчислення норми має наступні кроки:

$$
\begin{aligned}
&Вхід: Еліптична крива\ E: y^2 + xy = x^3 + \bar{c}\ над\ F_{2^d}\\
&Вихід: Кількість\ точок\ кривої\ E(F_{2^d})\\
&1.\ N \leftarrow \lceil d/2 \rceil + 3\\
&2.\ \lambda \leftarrow (1+8c) \bmod 2^4\\
&3.\ for\ i = 5\ to\ N\ do\\
&4.\quad \lambda \leftarrow (\frac{1+\lambda}{2\sqrt{\lambda}}) \bmod 2^i\\
&5.\ t = Norm(\frac{2\lambda}{1+\lambda}) \bmod 2^{N-1}\\
&6.\ if\ t^2 > 2^{d+2}\ then\ t \leftarrow t - 2^{N-1}\\
&7.\ return\ 2^d + 1 - t
\end{aligned}
\qquad (8)
$$

Запропонована модифікація AGM методу, тобто перехід від двох змінних до однієї, не повинна зменшити обчислювальну складність частини підйому, проте в даному випадку є незначний виграш у просторовій складності. Дана модифікація була запропонована Гаудрі для переходу до модифікованого методу SST (MSST), що являє собою модифікацію методу AGM та SST [7]. Дослідження методу MSST є наступним кроком досліджень, пов'язаних з ефективними методами формування загальносистемних параметрів для криптосистем на еліптичних кривих, в тому числі для національного стандарту ДСТУ 4145-2002.

3. Аналіз обчислювальної складності арифметико-геометричного методу

Для дослідження арифметико-геометричного методу обчислення кількості точок на еліптичній кривій було розроблено програмний засіб мовою C++ з використанням бібліотеки NTL та gmp. Дослідження щодо часу виконання алгоритму проводилися на програмі, що була скомпільована з використанням gcc 4.84 на операційний системі Ubuntu 14.04 та процесорі Intrel Core i5-2300. Так як всі операції для AGM алгоритму виконуються послідовно, то розпаралелити виконання алгоритму неможливо і кількість ядер у процесорі час виконання алгоритму не змінять.

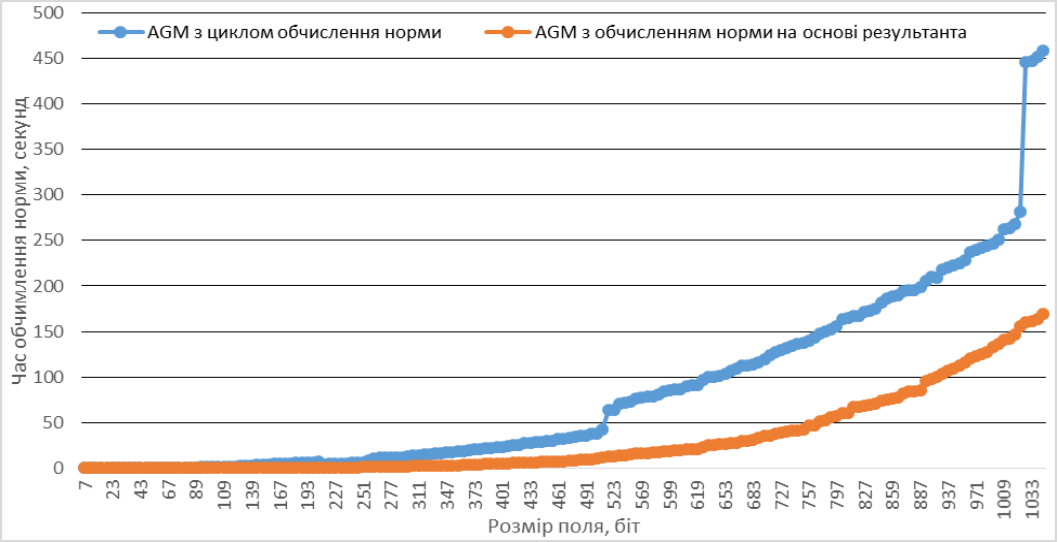
У табл. 2 наведено час обчислення фази підйому та норми для різних варіантів AGM методу (двозмінного та однозмінного).

Таблиця 2

Степінь розширення поля *d*, *біт*	Фаза підйому		Обчислення норми	
	AGM bivariate (двозмінний), *с*	AGM univariate (однозмінний), *с*	Додатковий цикл за Местре, *с*	Обчислення результанта, *с*
7	0,001038	0,000938	0,002122	0,0009
23	0,015002	0,01483	0,041987	0,002081
79	0,247437	0,255037	0,65108	0,033835
107	0,527144	0,507134	1,29144	0,078065
173	1,88726	1,92282	5,17245	0,349419
199	2,58677	2,59791	6,62534	0,508944
257	2,59583	2,59573	8,03255	1,24161
307	4,55193	4,57529	13,7089	2,09486
383	7,19335	7,2112	21,6217	4,45025
433	9,29693	9,30088	27,6736	6,2283
503	12,7932	12,7955	37,9071	10,1295
601	26,8153	26,6644	86,1802	19,2975
709	37,9417	37,5102	123,696	35,9172

787	47,648	47,8452	152,693	55,7415
827	52,9663	53,0276	171,616	68,2506
929	67,0609	67,0016	218,492	103,512
1021	82,083	81,5745	281,817	156,275
1049	131,367	131,111	458,253	169,589

За результатами аналізу табл. 2 можна стверджувати, що різниця для фази підйому для двозмінного та однозмінного алгоритму AGM не спостерігається, проте різниця для різних алгоритмів обчислення норми спостерігається. Більш детально ця різниця показана на рисунку.



Графік залежності часу обчислення норми
від розмірів розширення поля для різних алгоритмів

Загальний час обчислення кількості точок на еліптичній кривій з розміром 1031 біт, саме такий розмір еліптичних кривих необхідний для надвисокого рівня стійкості (512 біт для симетричного шифру), для однозмінного AGM алгоритму з обчисленням норми через результант складає приблизно 285 с. Для того щоб досягнути криптографічної стійкості загальносистемних параметрів визначено певний ряд умов, і якщо значення порядку кривої (кількості точок) не задовольняє хоча б однієї з цих умов, то таке значення не можливе для використання у криптосистемах для досягнення зазначеного рівня стійкості. Якщо хоча б одна умова не виконана, переходять до наступної кривої для виконання перевірки усіх вимог.

Висновки

Таким чином, на даний момент існують загрози для асиметричної криптографії, які пов'язані з квантовим алгоритмом Шора та Гровера. Для підвищення стійкості сучасних асиметричних алгоритмів на базі еліптичних кривих можна збільшити розмір базової точки. Для цього можуть використовуватися ефективні методи побудови загальносистемних параметрів, наприклад арифметико-геометричний метод та його модифікації.

Було розроблено програмну модель AGM методу та проведено аналіз обчислювальної складності оригінального AGM методу (запропонованого Местре) та однієї з його модифікації (запропонованої Гаудрі), а також декілька варіантів обчислення норми. Для побудови ефективних алгоритмів генерування загальносистемних параметрів для еліптичних кривих процес вибору алгоритмів нормування є важливим. Якщо крок підняття еліптичних кривих неможливо розпаралелити при його обчисленні, тому що даний крок є рекурсивним, то крок нормування можна розпаралелити при виборі відповідного алгоритму нормування.

На даний момент найбільш результативним буде використання методу Харлі для обчислення порядку кривої, який являє собою поступову еволюцію методу SST та AGM. Перша модифікація SST методу була запропонована Гаудрі [7] і є наступним нашим об'єктом дослідження у побудові сильних криптографічних параметрів для еліптичних кривих надвисокого рівня стійкості.

Список літератури: 1. *Shor, P. W.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor //SIAM J. Comput. – 1997. – 26 (5). – pp. 1484–1509. 2. *Ганзя, Р.С.* Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Р.С.Ганзя, Ю.І.Горбенко // Восточно-Европейский журнал передовых технологий. –2014. – Т. 6, №1(67). – 8-15 с. 3. *Горбенко, Ю.І.* Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ганзя Р.С., Горбенко Ю.І. // Вісник Національного університету "Львівська політехніка": "Комп'ютерні системи та мережі". – 2014. – № 806. – С. 40–48. 4. *Oliynykov, R.* (2015). A New Encryption Standard of Ukraine: The Kalyna Block Cipher. Mode of access: http://eprint.iacr.org/2015/650.pdf. 5. *ISO/IEC* 15946-5:2009. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation. 2014-04-10 – CH-1211 Geneva 20. – 2009 – 31 p. 6. *Cohen, H.* Elliptic and Hyperelliptic Curve Cryptography: handbook / H. Cohen, G. Frey – NW.: Chapman & Hall/CRC, 2006. – 807 p. 7. *Gaudry, P.* A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2 / P. Gaudry // ASIACRYPT 2002. 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown – New Zealand: Springer, 2002 – P.311-327. 8. *Mestre, J. F.* AGM pour le genre 1 et 2. / J. F. Mestre // Lettre à Gaudry et Harley – December 2000. 9. *Miller, V.* Uses of elliptic curves in cryptography Advances in Cryptology Proceedings of Crypto Lecture Notes in Computer Science / Miller V. Springer – Verlag New–York, 1986 – P. 417–426.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 15.04.2015