УДК 004.056.55

АНАЛІЗ СУТНОСТІ ТА МОДЕЛІ ПРОТОКОЛУ ІНКАПСУЛЯЦІЇ КЛЮЧІВ У КІЛЬЦІ ПОЛІНОМІВ НАД СКІНЧЕНИМ ПОЛЕМ

І. Д. ГОРБЕНКО, О. Г. КАЧКО, В. А. ПОНОМАР, М. В. ЄСІНА, О. С. АКОЛЬЗІНА, В. А. КУЛІБАБА

У роботі розглядається аналіз сутності та моделі протоколу інкапсуляції ключів у кільці поліномів над скінченим полем. Наводяться основні положення стосовно протоколів. Наводяться результати порівняння механізмів інкапсуляції ключів. Наводиться криптографічний протокол інкапсуляції та декапсуляції ключа в NTRU Prime Ukraine.

Ключові слова: інкапсуляція ключів, кільце поліномів, протокол.

ВСТУП

На сьогодні основні зусилля світової криптографічної спільноти зосереджені на створенні практичних квантово-стійких механізмів електронного підпису (ЕП), асиметричного шифрування (АСШ) та протоколів інкапсуляції ключів (ПІК) [1–7]. Одним з механізмів, що може бути застосований для побудови АСШ та ПІК для постквантового періоду, є різні варіанти застосування криптографічних перетворень в кільцях поліномів, випробуваним варіантом його є NTRU криптосистема [1]. У [3] запропоновано механізми побудови АСШ та ПІК, що можуть забезпечити 5 рівень квантової криптографічної стійкості (128 біт квантової та 256 класичної криптостійкості). Але, на наш погляд, важливою як теоретичною, так і практичною є проблема забезпечення включно до 7 рівня криптографічної стійкості (256 біт квантової та 512 класичної криптостійкості). З точки зору постквантових ПІК на сьогодні важливим є: аналіз стану розроблення та стандартизації ПІК; обґрунтування та розробка формального опису протоколу інкапсуляції ключів, у якому можна було б закласти формально вимоги, незалежно від математичних перетворень, що застосовуються, а також розробка пропозицій щодо побудови ПІК, включно до 7 рівня безпеки. При цьому необхідно, щоби ПІК будувався на основі тієї ж математичної бази, що і АСШ.

Метою цієї статі є аналіз стану розроблення та стандартизації ПІК взагалі, і для постквантового періоду, розробка та формальний опису ПІК, в який добре вписувались би як існуючі ПІК [2, 3], так і перспективні постквантові на основі кілець поліномів над скінченими полями, а також аналіз властивостей такого виду ПІК.

З огляду на суттєву важливість застосування алгоритмів направленого шифрування (АСШ) на міжнародному рівні під час виконання Європейського проекту NESSIE, особливу увагу було приділено реалізації висунутих вимог щодо ПІК. У подальшому на основі отриманих результатів, пропозицій та рекомендацій було прийнято міжнародний стандарт ISO/IEC 18033-2 «Інформаційна технологія – Методи захисту – Алгоритми захисту – Частина 2: Асиметричні шифри» [2]. В процесі підготовки та оголошення конкурсу NIST США як основний примітив визначив ПІК.

Аналіз механізмів та безпосередньо ПІК, що наведені в [1–6], дозволив зробити такі висновки.

– Основні зусилля на світовому рівні зосереджені на створенні механізмів інкапсуляції ключів та ПІК.

– Розроблено та подано на різні конкурси, але в основному на конкурс постквантових криптопримітивів, механізми реалізації ПІК.

– Основним призначенням ПІК є генерування та передача відправником отримувачу інкапсульованого ключа та ключових даних в інкапсульованому (захищеному) вигляді та декапсуляцію їх отримувачем відповідно.

Механізм інкапсуляції ключів у запропонованій термінології призначений для інкапсуляції та декапсуляції ключів, а також обчисленні (генеруванні) та використанні секретних ключів, під час застосування, наприклад, режимів роботи симетричних блокових і потокових шифрів [4]. У таблиці 1 наведено перелік основних кандидатів на постквантові механізми та ПІК, які розглядаються та порівнюються на конкурсі NIST США [3, 5, 6].

Таким чином, усього подано 40 кандидатів на постквантові стандарти механізмів інкапсуляції ключів. Під час їхнього розроблення використано різні математичні основи, в тому числі: алгебраїчні решітки; коди, мультиваріативні перетворення у квадратичних полях, перетворення типу ПІК тощо.

В процесі досліджень, деякі результати яких наведені в цій статті, було проведено аналіз та висунуті вимоги до механізмів ПІК та запропоновано конкретні реалізації, з урахуванням [3] та механізмів ПІК, що наведені у [2].

Також враховано, що у стандарті ISO/IEC 18033-2 наведено матеріали щодо обґрунтування нової структури для асиметричного направленого шифрування KEM-DEM [2].

Вказаний механізм реалізує АСШ, оскільки інкапсуляція виконується на відкритому ключі (кортежі) іншого абонента, а декапсуляція на особистому ключі (кортежі) абонента. При декапсуляції перевіря-

Таблиця 1

Механізми постквантових кандидатів на ПІК

Математичні методи	Кандидати в стандарти	Число кандидатів
Алгебраїчні решітки	CRYSTALS-KYBER, Ding Key Exchange, HILA5, EMBLEM та R.EMBLEM, FrodoKEM, KINDI, LAC, LIMA, Lizard, NewHope, NTRU Encrypt, NTRU-HRSS-KEM, NTRU Prime, Odd Manhattan's, KCL (pka OKCN/AKCN/CNKE), Round2, SABER, Titanium	18
Коди	BIG QUAKE, BIKE, Classic McEliece, DAGS, HQC, LAKE, LEDEkem, Lepton, NTS-KEM, QC-MDPC KEM, RLCE-KEM, RQC	12
Мульти варіативні перетворення	CFPKM, DME	2
Геш-перетворення	==========	0
Інші перетворення	Mersenne-756839, Post-quantum RSA-Encryption, Ramstake, SIKE, Three Bears	5
Відкликані кандидати	HK17, RVB, Edon-K	3
Атаковані але виправлені		0
Усього кандидатів		40

ється цілісність і справжність відкритого ключа та перевіряється справжність (автентичність) іншого абонента.

Можна говорити про неспростовність абонента, що генерує особисті ключі. Наприклад, у нашому випадку неспростовність абонента В може бути реалізована способом передачі відкритого кортежу С через третю довірену сторону тощо.

У цій статті наводяться початкові результати досліджень щодо механізмів та ПІК, у тому числі:

1. Попередні результати порівняння механізмів та протоколів інкапсуляції ключів. При порівняльному аналізі використовувалася сукупність безумовних та умовних критеріїв.

2. Формальний опис механізму та протоколу інкапсуляції ключів.

3. Обґрунтування та аналіз моделі безпеки щодо постквантових механізмів і ПІК.

4. Попередні дослідження дозволили як найбільш перспективні виділити механізм NTRUPrime.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕХАНІЗМІВ ТА ПРОТОКОЛІВ ІНКАПСУЛЯЦІЇ КЛЮЧІВ

1.1. Попередні результати порівняння механізмів та протоколів інкапсуляції ключів

Під час порівняльного аналізу використовувалася сукупність безумовних та умовних критеріїв. Як безумовні критерії запропоновано наступні [7, 8]:

1) Іст. – рівень криптографічної стійкості;

2) lв.к – довжина відкритого ключа;

3) lо.к – довжина особистого ключа;

4) lрез. – довжина результату криптоперетворення;

5) Тпр. – швидкість прямого криптоперетворення;

6) Тзв. – швидкість зворотного криптоперетворення.

Експертні оцінки використовувалися для оцінки важливості кожної з наведених характеристик, а безпосередньо при порівнянні алгоритмів використовувалися об'єктивні числові значення, шкала оцінки та вагові коефіцієнти важливості характеристик, що були отримані в ході експертного оцінювання (таблиця 2).

Таблиця 2

Експертні оцінки характеристик криптоалгоритмів

Показники / Експерти	$I_{ст.}$	$l_{в.к}$	$l_{о.к}$
1	0,070	0,047	0,033
2	0,066	0,066	0,032
3	0,081	0,039	0,039
4	0,094	0,048	0,026
5	0,078	0,078	0,036
W	0,078	0,056	0,033
Показники / Експерти	**$l_{рез.}$**	**$T_{пр.}$**	**$T_{зв.}$**
1	0,283	0,283	0,283
2	0,202	0,316	0,316
3	0,367	0,237	0,237
4	0,424	0,204	0,204
5	0,420	0,193	0,193
W	0,339	0,247	0,247

Оскільки в NIST було викладено велику кількість алгоритмів, що використовують перетворення в решітках числових полів та математичні коди (порівняно з іншими), то було вирішено спочатку порівняти алгоритми кожного з цих типів, а потім алгоритми, що займуть 1–2 місця з іншими. В даному дослідженні при виборі алгоритмів висувалися додаткові безумовні вимоги:

1) алгоритм має гарантувати, що найменше 3 рівень безпеки за класифікацією NIST;

2) якщо існує декілька варіантів наборів параметрів для одного алгоритму, то порівняно бере участь варіант, що гарантує найбільшу безпеку.

В таблиці 3 наведено характеристики обраних для порівняння алгоритмів, що засновані на використані перетворень в алгебраїчних решітках.

Таблиця 3

Характеристики алгоритмів інкапсуляції ключів на алгебраїчних решітках

Алгоритми	$I_{ст.}$	$I_{в.к}$	$I_{о.к}$	$I_{рез.}$	$T_{пр.}$	$T_{зв.}$
CRYSTALS-KYBER	5	5 422	5 422	5 422	2 112 734	15 843 611
Ding Key Exchange	5	4 964	4 964	4 964	9 541 851	13 413 988
FrodoKEM	3	10 449	15 673	6 763	7 419 629	2 933 863
HILA5	5	2 758	2 758	2 758	7 921 744	5 408 625
KINDI	5	11 616	2 973 704	2 144	1 035 852	151 282 021
LAC.CCA KEM	5	2 064	3 072	2 176	998 494	7 617 506
LIMA	5	1 680	32	1 568	914 137	1 698 920
Lizard	5	840	32	1 184	1 734 600	397 902 189
NewHope	5	9 616	19 872	9 736	1 525 623	4 428 250
NTRUEncrypt	5	7 989	8 029	15 962	299 133	456 199
Odd Manhattan’s	5	5 884	5 924	11 752	132 351 915	3 827 502
Round2	5	1 456	1 712	2 544	767 892	780 283
SABER	5	1 184	1 472	1 824	1 825 775	518 385
ThreeBears	5	1 056	2 080	1 536	241 051	912 083
Titanium	5	544	1 056	1 024	3 469 480	257 284
NTRUPrime_AVX	5	1 600	1 218	1 047	99 149	125 820

На рис. 1 відображено гістограму відносної переваги алгоритмів. Як видно найбільшу перевагу має алгоритм NTRUPrime_AVX, на другому місці – Titanium, на третьому ThreeBears, на четвертому NTRUEncrypt, на п’ятому SABER тощо.

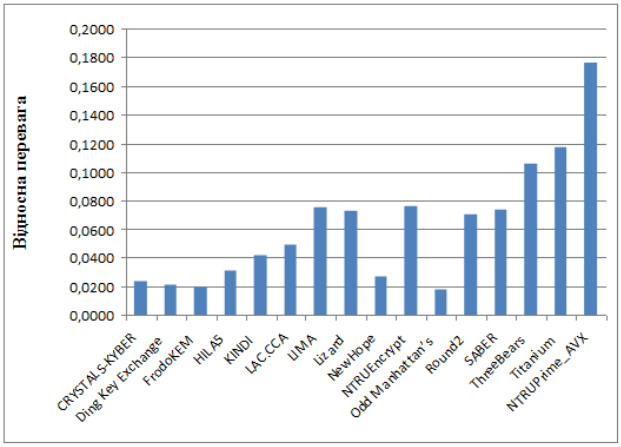

Рис. 1. Відносна перевага алгоритмів на основі перетворень в алгебраїчних решітках

На рис. 2 відображено гістограму відносної переваги алгоритмів. Як видно, найбільшу перевагу має алгоритм LAKE, на другому місці з невеликим відривом – RLCE-KEM.

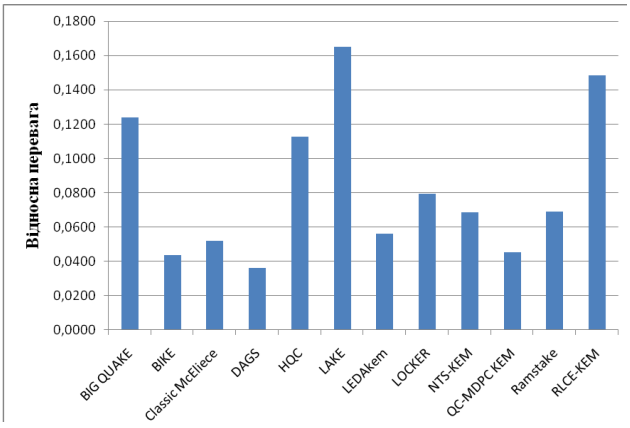

Рис. 2. Відносна перевага алгоритмів на основі математичних кодів

В таблиці 4 наведено характеристики обраних для порівняння алгоритмів, що засновані на використанні математичних кодів.

Таблиця 4

Характеристики алгоритмів інкапсуляції ключів на математичних кодах

Алгоритми	$l_{ст.}$	$l_{в.к}$	$l_{о.к}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$
BIG QUAKE	5	149 800	41 804	492	12 772 072	51 333 539
BIKE	5	9 034	9 034	9 034	1 967 128	43 842 551
Classic McEliece	5	8 188	8 188	8 188	1 786 760	37 247 437
DAGS	5	4 964	4 964	4 964	109 932 700	15 652 888
HQC	5	1 440	3 168	1 504	3 529 138	2 703 872
LAKE	5	1 040	1 536	1 088	604 031	4 774 104
LEDAkem	5	2 256	32	3 120	106 848 011	28 161 595
LOCKER	5	9 523	19936	10 023	850 000	5 372 000
NTS-KEM	5	7 417	7 457	14 818	1 081 765	5 564 976
QC-MDPC KEM	5	5 115	5 155	10 214	28 662 874	3 254 700
Ramstake	5	2 819	2 859	5 622	159 129 068	1 575 641
RLCE-KEM	5	1 696	1 664	2 083	21 850 039	168 952

В таблиці 5 наведено характеристики алгоритмів, що засновані на різних криптографічних перетвореннях.

Таблиця 5

Характеристики алгоритмів інкапсуляції ключів

Алгоритми	$l_{ст.}$	$l_{в.к}$	$l_{о.к}$
Titanium (решето числового поля)	5	544	1 056
NTRUPrime_AVX (решето числового поля)	5	1 600	1 218
LAKE (математичні коди)	5	1 040	1 536
RLCE-KEM (математичні коди)	5	1 696	1 664
Edon-K (геш)	3	10 449	15 673
SIKE (ізогенії)	3	1 023	1 173
Алгоритми	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$
Titanium (решето числового поля)	1 024	3 469 480	257 284
NTRUPrime_AVX (решето числового поля)	1 047	99 149	125 820
LAKE (математичні коди)	1 088	604 031	4 774 104
RLCE-KEM (математичні коди)	2 083	21 850 039	168 952
Edon-K (геш)	6 251	419 330	691 377
SIKE (ізогенії)	1 023	565 483 974	767 267

На рис. 3 відображено гістограму відносної переваги алгоритмів. Як видно, найбільшу перевагу має алгоритм NTRUPrime_AVX, на другому місці – Titanium, тобто перші місця посіли алгоритми на решеті числового поля.

Таким чином, за результатами порівняльного аналізу можна зробити такий висновок щодо переваг кандидатів на постквантовий стандарт ПІК на першому місці – NTRUPrime_AVX, на другому – Titanium, на третьому – SIKE, на четвертому – RLCE-KEM, на п'ятому – LAKE, на шостому – Edon-K.

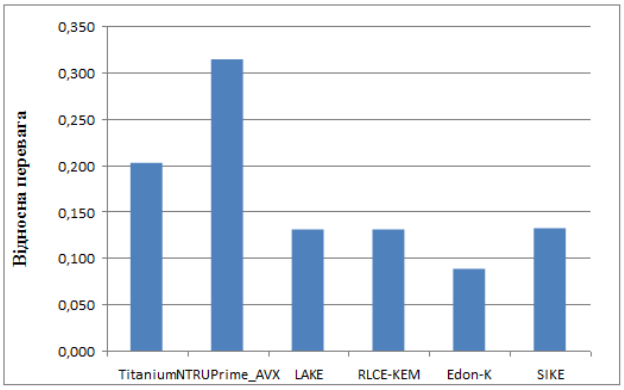

Рис. 3. Відносна перевага алгоритмів інкапсуляції ключів

2. ФОРМАЛЬНИЙ ОПИС ПРОТОКОЛУ ІНКАПСУЛЯЦІЇ КЛЮЧІВ

Призначення ПІК – інкапсуляція ключа відправником та передача його отримувачу в інкапсульованому (захищеному) вигляді.

Для реалізації протоколу інкапсуляції необхідно:

– узгодити стандарт асиметричного шифрування та інших необхідних стандартів криптографічних перетворень;

– узгодити чи відповідним чином згенерувати та захищеним способом розподілити загальні для подальшого здійснення захищеного зв'язку типу клієнт–клієнт чи клієнт–сервер;

– встановити загально-системі чи загальні параметри відповідної асиметричної криптосистеми;

– отримувач асиметрично зашифрованих повідомлень та інкапсульованих ключів від інших клієнтів генерує свою асиметричну ключову пару – секрет-

ний (особистий) та відкритий ключі. Особистий (секретний) зберігається і доступний тільки цьому отримувачу, а відкритий робиться доступним захищеним способом відправнику;

– клієнт-відправник генерує сеансів ключ інкапсуляції у вигляді асиметричної пари (можливо асиметричних пар) – секретного та відкритого ключів інкапсуляції та вводить їх у дію;

– клієнт-відправник захищає відкритий ключ інкапсуляції засобом його безпосередньої інкапсуляції та підготовляє його для відправки у захищеному вигляді клієнту-отримувачу;

– клієнт-отримувач приймає захищене повідомлення та здійснює його декапсуляцію і одночасно визначає його цілісність та справжність;

– клієнт-відправник використовує асиметричний ключ інкапсуляції – секретний та відкритий ключі обчислює секретний ключ для його використання при зашифруванні та автентифікації тощо повідомлень для клієнта чи сервера;

– клієнт-отримувач використовує декапсульований ключ та, можливо, свої загальні параметри та секретний ключ обчислює секретний ключ для його використання при розшифруванні та автентифікації отриманих зашифрованих чи одного зашифрованого повідомлення;

– за необхідності робиться підтвердження отриманих захищених повідомлень.

Попередні результати досліджень з урахуванням [2, 3, 7] дозволили у найбільш загальному випадку запропонувати механізм та ПІК. Сутність ПІК у наступному.

В ході генерації (обчисленні) асиметричної ключової пари отримувача необхідно:

1. Обчислити (згенерувати) асиметричну пару асиметричного шифрування – відкритий P_k та секретний (особистий) S_k ключі.

2. Зробити доступними для відправника компоненти відкритого ключа, наприклад, у вигляді:

$$P_k := (ЗП, W, \lambda), \quad (1)$$

де *ЗП* – значення загальних параметрів АСШ; W – відкритий ключ (можливо його сертифікат); λ – рівень безпеки.

3. Записати та зберігати для використання особистий ключ S із забезпеченням його конфіденційності, цілісності, справжності та доступності тощо, наприклад, у вигляді:

$$S_k := (S, P_k), \quad (2)$$

де S – секретний ключ розшифрування отримувача, а P_k – відкритий ключ (1).

Відправник (наприклад, клієнт-сервер чи клієнт) може інкапсулювати свій сеансовий асиметричний ключ, якщо він має доступ до відкритого ключа отримувача (1). Для цього він виконує такі операції.

Перед генерацією асиметричної ключової пари відправник повинен:

– узгодити та налаштувати механізм та засіб асиметричного шифрування;

– узгодити та налаштувати загальні параметри засобів механізму шифрування, в тому числі алгоритм вироблення ключа $KDF(\bullet)$ на основі спільної таємниці.

Алгоритм інкапсуляції відправником виконується в такій послідовності (при невідомому S_k):

1. Згідно з прийнятим механізмом генерується ключ сеансу r відправника.

2. Згідно з прийнятим механізмом обчислюється відкритий ключ сеансу C відправника, наприклад, у вигляді

$$C := F(r, ЗП). \quad (3)$$

3. Відправником обчислюється спільна таємниця інкапсуляції ключа $Q \neq 0$ відправника

$$Q := F(C, r, ЗП, W). \quad (4)$$

4. Відправником обчислюється значення секретного (особистого) ключа

$$K := KDF(Q), \quad (5)$$

наприклад, для подальшого його застосування як ключ симетричного шифрування.

5. На останок відправник має секретний сеансів ключ K_C для подальшого використання, наприклад, у вигляді симетричного ключа сеансу, а також, інкапсульований у відкритий ключ C свій секретний ключ сеансу r.

Далі відправник свій відкритий ключ сеансу C, забезпечуючи його цілісність, справжність та доступність, робить доступним отримувачу. Використовуючи відкритий ключ сеансу C та свій секретний (особистий) ключ S, отримувач може зробити декапсуляцію, а також обчислити секретний ключ наступного сеансу K_C.

Вхідними даними для алгоритму декапсуляції є відкритий ключ C, що отриманий від відправника, та особистий (секретний) ключ S_k, конкретно секретний ключ S із (2).

Декапсуляція ключа отримувачем здійснюється в такій послідовності:

1. Отримувач, використовуючи свій секретний ключ S, обчислює спільну таємницю

$$Q := F(C, ЗП, S). \quad (6)$$

За необхідності перевіряється, що $Q \neq 0$.

2. Відправником обчислюється значення секретного ключа

$$K := KDF(Q). \quad (7)$$

3. Відправник та отримувач мають секретний ключ K_C для подальшого використання його, наприклад, у вигляді симетричного ключа сеансу шифрування та автентифікації.

3. МОДЕЛЬ БЕЗПЕКИ ЩОДО ПЕРСПЕКТИВНИХ ТА ПОСТКВАНТОВИХ МЕХАНІЗМІВ І ПРОТОКОЛІВ ІНКАПСУЛЯЦІЇ КЛЮЧІВ

Модель безпеки щодо перспективних та постквантових механізмів і протоколів інкапсуляції ключів розглядається з урахуванням основних положень та пропозицій, що викладені за даною тематикою в [9, 10].

За основу було взято модель безпеки Canetti-Krawczyk (CK) використовується для автентифікації обміну ключами (AKE) [9].

Також використано неформально поняття "досконала пряма секретність (безпека)" (PFS) [9, 10] зазначається як властивість, що "компрометування довгострокових ключів не компрометує минулі ключі сеансу".

Коли доводять, що протокол має бути SK-безпечним, автоматично отримується доказ того, що цей протокол гарантує PFS.

Також вважатимемо, що протокол KE задовольняє SK-безпеку без PFS, якщо він використовує SK-безпеку відносно будь-якого KE-зловмисника в UM, що не допускає припинення дії ключів [9, 10].

На основі CK моделі були визначені загальні положення щодо вимог до ПІК та до моделі безпеки. Їхня сутність у тому, що [7]:

– *повнота* протоколу, сутність якої полягає в тому, що якщо *S* істинне, то суб'єкт/об'єкт *P* з великою ймовірністю переконає про це перевірника і той згодиться, що *S* істинне;

– *коректність* протоколу, яка проявляється в тому, що, якщо *S* хибне, то суб'єкт *V* виявить це з великою ймовірністю, тобто *P* не переконає *V*, що *S* істинне.

Крім вимог повноти й коректності, протокол з нульовим розголошенням має задовольняти ще й таку умову – нульове розголошення інформації про *S* – у результаті виконання протоколу (*P,V,S*) перевірник не зменшує свою апріорну невизначеність відносно твердження *S*, тобто він не отримує ніякої інформації про те, чому *S* істинне.

Дослідження показали, що забезпечення нульового розголошення на практиці може бути здійснене, якщо [7]:

– кожен суб'єкт, який має намір діяти або як пред'явник *P*, або як перевірник *V*, повинен мати засоби генерації випадкових чисел;

– абоненти групи мають дійти згоди щодо того, яка функція гешування використовуватиметься;

– кожен об'єкт, який має намір діяти як пред'явник, має бути забезпечений асиметричною ключовою парою, обраною згідно з рекомендаціями, які наведено вище;

– кожен об'єкт, який має намір діяти як перевірник, має бути забезпечений засобами обчислення довірчих копій відкритих ключів перевірки для об'єктів, чия ідентичність перевіряється.

Сутність моделі CK. Модель безпеки CK стосується безпеки ключа сеансу, що використовується на сеансі зв'язку. В ході її оцінки використовується формальна модель для протоколів обміну ключами та можливостей криптоаналітика (зловмисника). Поняття безпеки, яке називається *безпекою ключа сеансу* (або *SK-security*), направлене на забезпеченні безпеки окремих ключів сеансу. Її порушення є компрометацією сеансового ключа. У випадку безпечності ключа зловмисник "нічого не дізнається про значення ключа", коли він перехоплює дані протоколу обміну ключами та здійснює атаки на інші сеанси та сторони, що взаємодіють. Такий підхід є стандартним для моделі семантичної безпеки, коли криптоаналітик не може відрізнити реальне значення ключа від незалежного випадкового значення. В даному випадку говорять про реалізацію криптографічного протоколу «нульових знань». Водночас таке визначення SK-безпеки необхідно використовувати обережно, тому що забезпечення необхідного рівня стійкості під час встановлення та використання протоколів обміну ключами для реалізації захищених каналів, мета може досягатися без складних вимог.

Детальний аналіз, що проведений з метою визначення критеріїв та показників оцінки, та порівняння ПІК, дозволив обґрунтувати та запропонувати поділ наведених критеріїв на безумовні та умовні критерії оцінки безпечності ПІК.

Таким чином, до безумовних критеріїв оцінки ПІК належатимуть.

1. Рівень реалізації моделі безпеки IK-CPA/CCA2.

2. Криптографічна стійкість (складність криптографічного аналізу) щодо криптоперетворення АСШ – $W_{асш}$ (ЕП – $W_{еп}$), що застосовуються у протоколі ПІК.

3. Криптографічна стійкість (складність криптографічного аналізу) щодо криптоперетворення інкапсуляції – $W_{пік}$, що застосовуються у протоколі інкапсуляції;

4. Криптоживучість ключів щодо криптоперетворення АСШ – $G_{асш}$ (ЕП – $G_{еп}$), що застосовуються у протоколі ПІК.

5. Криптоживучість ключів, що застосовуються у протоколі ПІК – $G_{пік}$;

6. Захищеність криптопротоколу від раніше переданих повідомлень – $W_{рпп}$.

7. Неспростовність криптоперетворень АСШ – $N_{асш}$, що встановлені для криптографічного захисту;

8. Неспростовність криптоперетворень ЕП – $N_{еп}$, що встановлені для криптографічного захисту;

9. Новизна ключів АСШ(ЕП) – $W_{кл}$, що застосовуються в протоколі інкапсуляції ПІК;

10. Характеристика степеня нерозрізнюваності для ключів АСШ, ЕП та ПІК.

4. АНАЛІЗ ТА РОЗРОБКА ПІК NTRU PRIME

4.1. Загальні положення

У цьому розділі наводяться результати аналізу та обґрунтування перспективного підходу до реалізації протоколу інкапсуляції ключів на основі застосування NTRU Prime. По суті пропонується модернізований нами NTRUPrime з використанням кілець поліномів.

Використовуватимемо такі математичні перетворення [1, 3, 8–10]:

1. «Класичний NTRU»: кільця виду $(Z/q)[x]/\left(x^p-1\right)$, де p – просте число і q – є степенем 2, використовуються в класичній криптосистемі NTRU [1]. Він не рекомендується для застосування, оскільки на нього існують атаки.

2. «NTRU NTT»: кільця форми $(Z/q)[x]/\left(x^p+1\right)$, де p – є степенем 2 і $q \in 1+2pZ$ – просте. Він використовується в типових криптосистемах на основі Ring-LWE, забезпечує захист від атак сторонніми каналами, але також не рекомендується до застосування [3].

3. «NTRU Prime» та «Модифікована NTRU Prime»: в ньому також використовуються поля виду $(Z/q)[x]/\left(x^p-x-1\right)$, де p просте. Він удосконалений та використовується в «Модифікованому NTRU Prime». Обґрунтування переваг та застосування наведені в [3].

Конкретно в [3] запропоновано та використовується криптосистема з відкритим ключем «Модернізований NTRU Prime 4591^{761}», там також доводиться, що з цим полем забезпечується модель безпеки IND-CCA2 зі стійкістю з постквантовим рівнем стійкості 2^{128}. Причому, в модернізованому NTRU Prime 4591^{761} інкапсуляція (зашифрування) 256-бітного сеансового ключа вимагає 59600 циклів, а декапсуляція (розшифрування) – лише 97452 цикли.

Модернізований NTRU Prime має, порівнянно з вибором кільця NTRU, декілька переваг щодо реалізації та криптографічної стійкості. Наприклад, відсутня небажана вірогідність виникнення помилок розшифрування, яка з'являється у більшості криптосистем на решітках. Крім того модернізований NTRU Prime 4591^{761} насправді забезпечує великий запас стійкості, що важливо в перспективі, коли можуть з'явитися більш ефективні атаки.

В таблиці 6 наведено результати порівняння множення поліномів – основної операції в NTRU Prime.

Таблиця 6

Порівняння результатів множення

Рек	Константа	Цикли	Кільце	Метод
ні	Так	11722	$(Z/8192)[x]/\left(x^{701}-x-1\right)$	Karatsuba та ін.
так	Так	28682	$(Z/4591)[x]/\left(x^{761}-x-1\right)$	Karatsuba та ін.
ні	Так	31000	$(Z/12289)[x]/\left(x^{1024}+1\right)$	NTT
ні	Ні	>91056	$(Z/2048)[x]/\left(x^{743}-1\right)$	Розріджений вхід (sprase input)

Загальноприйнятим є те, що кільця наведеного типу особливо ефективні. Так, кільця NTT допускають множення за рахунок трьох теоретико-числових перетворень, тобто швидких перетворень Фур'є над скінченими полями, причому з невеликими витратами ресурсів для «множення». Якщо відмовитись від NTT та перемножувати по-іншому, то можна використати оптимізовану комбінацію з декількох частин методу Карацуби та методу Тоома. Наведено більш ефективний алгоритм множення поліномів кілець над скінченим полем.

Аналіз показав, що перехід до криптографії на решітках з простими модулями запропоновано у 2014 року [3]. В 2016 році було опубліковано чорновий варіант [3], у якому запропоновані варіанти стандартного NTRU з використанням кілець виду $A = Z[X]/(X^N - X - 1)$.

4.2. Параметри механізму NTRU Prime Ukraine

Модернізований механізм NTRU Prime Ukraine [9–10] механізм належить до криптосистем, що задаються додатними цілими (p, q, t), причому:

– p – просте ціле таке, що

$$p \geq \max\{2t, 3\}; \tag{8}$$

– q – просте ціле таке, що

$$q \geq 48t + 1; \tag{9}$$

– $x^p–x–1$ – незвідний у кільці поліномів

$$(Z/q)[x]. \tag{10}$$

Позначимо кільце виду $Z[x]/(x^p - x - 1)$, кільце з модулем 3 виду $(Z/3)[x]/(x^p - z - 1)$, та поле з модулем q $(Z/q)[x]/(x^p–x–1)$ як відповідно R, $R/3$ та R/q. Причому, вважатимемо, що елемент R є малим, якщо всі його коефіцієнти приймають значення {–1, 0, 1}.

Крім того, говоритимемо, що елемент є t-малим, якщо точно $2t$ його коефіцієнтів є ненульовими. Вага Хеммінга буде $2t$.

Предметом наших подальших досліджень є удосконалений механізм NTRU Prime Ukraine 5-го та 7-го рівнів стійкості.

4.3. Особливості генерування ключа шифрування в NTRU Prime Ukraine

Довгостроковий ключ АСШ генерує отримувач. В удосконаленому механізмі NTRU Prime Ukraine отримувач генерує ключ наступним чином.

1. Генерація рівноймовірного, випадкового «маленького» (у змісті t ненульових елементів) елементу $g \in R$. Цей крок повторюється доти, доки g буде оборотним у $R/3$.

2. Генерація постійного випадкового також t-маленького елементу – секретного ключа $f \in R$. Слід відмітити, що f – ненульовий, та оборотний у R/q, причому $t \geq 1$.

3. Обчислення відкритого ключа у вигляді

$$h=g/(3f) \text{ у } R/q. \qquad (11)$$

В (11) q – просте та більше за 3, тому 3 – оборотне в R/q, а також і $3f$ – оборотне в R/q.

4. Закодувати h у рядок $\underline{h}$. Відкритий ключ буде – $\underline{h}$.

5. Зберегти секретні поліноми f в R, та $1/g$ в $R/3$ надійним чином.

4.4. Загальні положення щодо протоколу інкапсуляції ключів

Механізм (протокол) інкапсуляції ключів подається у такій послідовності:

- побудування загальних параметрів протоколу;
- генерування асиметричних пар ключів протоколу;
- протокол інкапсуляції ключів;
- протокол декапсуляції ключів.

Побудування загальних параметрів [9, 10]. Механізм АСШ NTRU Prime Ukraine є NTRU-подібною криптосистемою, що є перспективною для застосування у постквантовий період. Загальні параметри, призначення та формули для обчислень визначені у таблицях 7, 8.

Якщо елемент R належить до $R/3$ – він є «малим», це означає, що усі його коефіцієнти належать множині $\{-1,0,1\}$.

Малий елемент є t-малим, якщо в нього рівно $2t$ коефіцієнтів є ненульовими.

Далі як параметри (n, q, t) обираються параметри з [3], які відповідають стійкості k>=200.

Генерування ключів для NTRU Prime Ukraine [8–9].

Генерування ключів для NTRU PRIME Ukraine, 5-го рівня здійснюється для параметрів згідно з таблицею 7.

Таблиця 7

Загальні параметри АСШ NTRU Prime Ukraine

Позначення	Призначення	Формула
$(Z/q)[x]$	Кільце поліномів. Кожен елемент Z/q зазвичай кодується у $\lceil \log_2 q \rceil$ біт.	
n	Порядок поліному. Визначає кількість його коефіцієнтів. Просте число, для якого поліном $x^n - x - 1$ є незвідним.	$n \geq \max\{3, 2t\}$
R	Поле поліномів $Z[x]$ з модулем $x^n - x - 1$.	$Z[x]/(x^n - x - 1)$
$R/3$	Поле поліномів $(Z/q)[x]$ з модулем $x^n - x - 1$.	$(Z/3)[x]/(x^n - x - 1)$
R/q	Поле поліномів $(Z/q)[x]$ з модулем $x^n - x - 1$.	$(Z/q)[x]/(x^n - x - 1)$
p	Менший модуль	$p = 3$
q	Більший модуль, просте число, за яким зводяться усі коефіцієнти поліному R/q.	$q \geq 48t + 3$
t	Натуральне число, кількість ненульових елементів поліному залежить від цього параметру.	$t \geq 1$
k	Рівень криптостійкості.	256, 512
m	Таємне повідомлення. Кількість 0, 1 та -1 не менше, ніж t.	$m \in R/3$
M	Повідомлення після доповнення випадкового рядка b та іншої інформації.	
$octL$	Поле для завдання довжини повідомлення	1 байт
e	Зашифроване повідомлення.	$e \in R/q$

Таблиця 8

Параметри для генерації ключа

Позначення	Призначення	Формула
$G(g)$	Випадковий малий елемент (поліном). Кількість ненульових елементів дорівнює $2n/3+1$. Є секретним параметром, що використовується для обчислення відкритого ключа.	$g \in R/3$
F	Випадковий t-малий елемент (поліном). Кількість ненульових елементів полінома дорівнює $2t$. Є секретним параметром, що використовується для обчислення секретного ключа.	

Продовження таблиці 8

Позначення	Призначення	Формула
f	Малий елемент (поліном), є секретним (особистим) ключем: f=p*F+1.	f=(1+3F)mod$q$ $f \in R/q$
h	Відкритий ключ відправника. Оборотний елемент у R/q.	h=p*G/f
$\underline{h}$	Значення h, що перетворюється в рядок октетів. Довжина $\underline{h}$ дорівнює $n\lceil \log_2 q \rceil$.	

Кількість 1 та -1 у секретному ключі та у засліплюючому поліномі (значення t) визначається n та криптостійкістю k, яку потрібно забезпечити. Значення параметрів n, q, t для режимів роботи (256/128) Додаткові параметри NTRUPrime Ukraine наведено в [9].

Додаткові параметри використовуються під час зашифрування та розшифрування, залежать тільки від загальних параметрів k, n, t, q.

Генерація асиметричних ключів. Для визначення асиметричних ключів необхідні такі параметри:

n – порядок поліному, визначає кількість його коефіцієнтів. Просте число, для якого поліном $x^n - x - 1$ є незвідним, просте число,

q – більший (великий) модуль, просте число за яким зводяться усі коефіцієнти поліному R/q,

t – натуральне число, що визначає кількість ненульових коефіцієнтів поліному.

За означенням особистим ключем є поліном f:

$$f=(1+3F)\mathrm{mod}q,\ \mathrm{F,G}\in R/3,\ ||F||_1=2t,\ ||G||=2n/3+1.$$

Вихідними даними для генерації асиметричного ключа є такі:

- особистий ключ – поліном f у R/q,
- відкритий ключ – поліном h у R/q.

$$\mathrm{mod}(q) \text{ в полі } (Z/q)[x]/(x^n - x - 1).$$

5. КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ІНКАПСУЛЯЦІЇ КЛЮЧА В NTRU PRIME UKRAINE

Протокол інкапсуляції NTRU Prime Ukraine-KEM є «механізмом інкапсуляції ключа». Під час виконання протоколу інкапсуляції отримувач повинен:

1. Отримати захищеним чином у закодованому вигляді відкритий ключ, наприклад, чинний сертифікат відкритого ключа $\underline{h}$ отримувача.

2. Згенерувати t-маленький секретний ключ сеансу поліном $r \in R$ та зберегти його як секретний елемент.

3. Декодувати відкритий ключ отримувача $\underline{h}$ поліном у поліном $h \in R/q$.

4. Обчислити секретний поліном $hr \in R/q$.

5. Зробити округлення кожного коефіцієнта поліному hr, які становлять цілі числа у межах від $-(q-1)/2$ до $(q-1)/2$, до найменшого числа кратного 3. Внаслідок множення h на r та округлення отримаємо поліном – криптограму $c \in R$.

6. Здійснити кодування криптограми c у рядок $\overline{c}$ згідно з прийнятим алгоритмом кодування.

Для отримання відкритого ключа сеансу C «узгодження ключа» та секретного ключа сеансу зашифрування K здійснити гешування секретного ключа сеансу r та взяти як C старшу половину $H(r)$, а як K – молодшу половину $H(r)$ (формат little endian).

7. На основі геш-значення секретного ключа $H(r)$ сформувати відкритий ключ сеансу C та секретний ключ сеансу K. Попередньо значення r може кодуватися.

8. Засобом конкатенації формується шифротекст $C\overline{c}$, а також секретний ключ сеансу K.

9. Ключ K зберігається в подальшому як секретний та має застосовуватися для зашифрування даних, що передаються від відправника до отримувача, наприклад, під час застосування блокового чи потокового алгоритму симетричного шифрування та автентифікації.

10. Інкапсульований ключ $C\overline{c}$, що сформований відправником, має передаватися отримувачу для використання при декапсуляції ключа отримувачем та застосування ключа K у подальшому при розшифруванні зашифрованих відправником даних.

Протокол інкапсуляції ключа відправником здійснюється так:

1) формується відкритий кортеж ключа p_k та секретний кортеж ключа s_k

$$pk: = (C\overline{c}, \lambda) \text{ й } sk: = (K, pk); \qquad (12)$$

2) алгоритм зашифрування даних. При зашифруванні даних можуть використовуватися узгоджені функції, які є доступними усім абонентам. Вони включають функцію автентифікації повідомлень $MAC(\cdot,\cdot)$ та симетричний алгоритм шифрування $(Sym.Encrypt, Sym.Decrypt)$, а також функції, що наведені в [4].

Алгоритм виконується у такій послідовності:

3) надалі K використовується як E_K і M_K, де E_K – ключ для симетричної схеми шифрування і M_K – підходящий розмір ключа для схеми автентифікації повідомлення;

4) повідомлення m зашифровується з використанням симетричного шифру на ключі E_K, тобто

$$C_1: = Sym.Encrypt(m, EK); \qquad (13)$$

5) для автентифікації шифротексту C_1 на ключі автентифікації M_K, обчислюється код автентифікації повідомлення (MAC) тобто

$$C_2: = MAC(C_1, MK); \qquad (14)$$

6) на останок відправник передає отримувачу

$$C\overline{c}\ ,\ C_1, C_2\ . \qquad (15)$$

Відмітимо, що кодування c у рядок $\overline{c}$ є ще одним примітивом удосконаленого NTRU Prime Ukraine, що дозволяє за необхідності скоротити довжину до 20%.

6. КРИПТОГРАФІЧНИЙ ПРОТОКОЛ ДЕКАПСУЛЯЦІЇ КЛЮЧА В NTRU PRIME UKRAINE

Розглянемо удосконалений NTRU Prime Ukraine механізм у частині декапсуляції ключа. Отримувач отримує відкритий ключ інкапсуляції $C\overline{c}$ та захищене на сеансових ключах повідомлення C_1, C_2, тобто

$$C\overline{c}\ ,\ C_1, C_2\ . \qquad (16)$$

Безпосередньо декапсуляція шифртексту $C\overline{c}$ здійснюється у такій послідовності:

1) отримувач декодує $\overline{c}$, внаслідок чого отримує $c \in R$;

2) отримувач множить отримане значення c на $3f$ в R/q;

3) отримувач розглядає кожний коефіцієнт $3fc$ у R/q як ціле у межах з $-(q-1)/2$ до $(q-1)/2$, а далі приводить за модулем 3, та отримує поліном e у $R/3$;

4) отримувач множить поліном e на $1/g$ в $R/3$;

5) знижує e/g в $R/3$ до малого поліному $r' \in R$;

6) обчислює за аналогією як і при інкапсуляції c', C', K' з r';

7) якщо r' є t-малим, $c'=c$ та $C'=C$, то виводиться та використовується ключ симетричної автентифікації та розшифрування на ключі K'. Інакше визначається помилка і від захищеного повідомлення здійснюється відмова.

ВИСНОВКИ

1. Модернізований NTRU Prime має, порівняно з вибором кільця NTRU, декілька переваг щодо реалізації та криптографічної стійкості. Наприклад, відсутня небажана вірогідність виникнення помилок розшифрування, яка з'являється у більшості криптосистем на решітках. Крім того модернізований NTRU Prime 4591^{761} насправді забезпечує великий запас стійкості, що важливо в перспективі, коли можуть з'явитись більш ефективні атаки.

2. Основним призначенням ПІК є генерування та передача відправником інкапсульованого ключа та ключових даних отримувачу в інкапсульованому (захищеному) вигляді та декапсуляцію їх отримувачем.

3. Формальний опис механізму та протоколу інкапсуляції ключів. Попередні результати досліджень з урахуванням дозволили у найбільш загальному випадку запропонувати механізм та протокол інкапсуляції ключів.

4. Термін *досконала пряма секретність* використовується для функції протоколів узгодження ключів, які дають гарантії того, що ключі останньої сесії не будуть скомпрометовані навіть, якщо секретний ключ сервера скомпрометований.

5. Удосконалений NTRU Prime Ukraine є «механізмом інкапсуляції ключа» (KEM), він ґрунтується на алгоритмах інкапсуляції та декапсуляції секретного ключа сеансу шифрування та автентифікації.

6. Відритий ключ сеансу $C\overline{c}$ (інкапсульований ключ), що обчислений відправником, має передаватися отримувачу для використання при декапсуляції ключа отримувачем та застосування його в подальшому.

7. Модернізований NTRU Prime має, порівняно з вибором кільця NTRU, декілька переваг щодо реалізації та криптографічної стійкості. Крім того модернізований NTRU Prime 4591^{761} насправді забезпечує великий запас стійкості, що важливо в перспективі, коли можуть з'явитись більш ефективні атаки.

Література

[1] American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. – 2010.

[2] ISO/IEC 18033-2:2015. Інформаційні технології. методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри.

[3] «Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime [Electronic resource]. – Access mode: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf».

[4] [Проект ДСТУ ____:201_ Інформаційні технології Криптографічний захист інформації Алгоритм асиметричного шифрування NTRU Prime Ukraine.

[5] *Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman*. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings, volume 1423 of LNCS, pages 267–288. Springer, 1998.

[6] Циркулянт. – Електронний ресурс. – Режим доступу: https://uk.wikipedia.org/wiki/Циркулянт.

[7] *Горбенко І. Д.* Прикладна криптологія: Підручник / Горбенко І. Д., Горбенко Ю. І.; видання 2-ге. – Харків: Форт, 2013. – 878 с.

[8] *I. D. Gorbenko, O. G. Kachko, M. V. Yesina* Analysis of Asymmetric NTRU Prime IIT Ukraine Encryption Algorithm with Regards to Known Attacks, Telecommunications and Radio Engineering, Volume 77, 2018, Issue 9, pp. 799–816.

[9] *Горбенко І. Д.* Методи побудування загальних параметрів та ключів для NTRU Prime Ukraine 5-7 рівнів стійкості / І. Д. Горбенко, О. Г. Качко, Ю. І. Горбенко, І. В. Стельник, С. О. Кандій, М. В. Єсіна // Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2018. – Вып. 195. – С. 5–16.

[10] *I.D. Gorbenko, A.M. Oleksiychuk, O.H. Kachko, M.V. Yesina, V.A. Bobukh, S.O. Kandyi*. Calculation of general parameters for ntru prime ukraine of 6–7 levels of stability // Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХНУРЕ. – 2018. – Вып. 195. – С. 17–26.

Надійшла до редколегії 25.12.2018

Горбенко Іван Дмитрович, д-р. техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультету комп'ютерних наук, Харківського національного університету імені В. Н. Каразіна. Галузь наукових інтересів – криптографія, криптоаналіз, постквантова криптографія, захист інформації.

Качко Олена Григорівна, канд. техн. наук, професор кафедри ПІ ХНУРЕ. Галузь наукових інтересів – криптографія, криптоаналіз, паралельні обчислення.

Пономар Володимир Андрійович, канд. техн. наук, науковий співробітник Харківського національного університету імені В. Н. Каразіна. Галузь наукових інтересів – криптографічні перетворення, безпечне програмування, методи багатофакторної автентифікації та їх застосування з метою захисту інформації, захист криптографічних засобів інформації.

Єсіна Марина Віталіївна, канд. техн. наук, старший викладач кафедри безпеки інформаційних систем і технологій, факультету комп'ютерних наук, Харківського національного університету імені В. Н. Каразіна. Галузь наукових інтересів – захист інформації, постквантова криптографія.

Акользіна Ольга Сергіївна, науковий співробітник НДЧ кафедри безпеки інформаційних систем і технологій, факультету комп'ютерних наук, Харківського національного університету імені В. Н. Каразіна. Галузь наукових інтересів – асиметричне шифрування, механізми інкапсуляції ключів, постквантова криптографія.

Кулібаба Владислав Андрійович, аспірант кафедри безпеки інформаційних систем і технологій, факультету комп'ютерних наук, Харківського національного університету імені В. Н. Каразіна. Галузь наукових інтересів – моделі безпеки, протоколи інкапсуляції ключів, постквантова криптографія.

УДК 004.056.55

Горбенко И. Д. **Анализ сущности и модели протокола инкапсуляции ключей в кольце полиномов над конечным полем** / И. Д. Горбенко, Е. Г. Качко, В. А. Пономарь, М. В. Есина, О. С. Акользина, В. А. Кулибаба // Прикладная радиоэлектроника: науч.-техн. журнал. – 2018. – Том 17. № 3, 4. – С. – 127–137.

В работе рассматривается анализ сущности и модели протокола инкапсуляции ключей в кольце полиномов над конечным полем. Приводятся основные положения относительно протоколов. Приводятся результаты сравнения механизмов инкапсуляции ключей. Приводится криптографический протокол инкапсуляции и декапсуляции ключа в NTRU Prime Ukraine.

Ключевые слова: инкапсуляция ключей, кольцо полиномов, протокол.

Табл.: 8. Библиогр.: 10 назв.

UDC 004.056.55

Gorbenko I. D. **Analysis of the essence and models of the key encapsulation protocol in a polynomial ring over a finite field** / I. D. Gorbenko, E. G. Kachko, V. A. Ponomar, M. V. Yesina, O. S Akolzina, V. A. Kulibaba // Applied Radio Electronics: Sci. Journ. – 2018. Vol. 17. – № 3, 4. – P. 127–137.

The paper considers the analysis of the essence and models of the key encapsulation protocol in a polynomials ring over a finite field. The main provisions on the protocols are given. The results of the key encapsulation mechanisms comparison are presented. A cryptographic protocol of key encapsulation and decapsulation in NTRU Prime Ukraine is given.

Keywords: key encapsulation, polynomial ring, protocol.

Tab.: 8. Ref.: 10 items.